Romanian Association for
Information Security Assurance

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume XI
eISSN 2393-0837

CyberCon Romania
2024

THE INTERNATIONAL CONFERENCE ON
CYBERSECURITY AND CYBERCRIME

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume XI

A scientific conference organized by the
Romanian Association for Information Security Assurance

CyberCon Romania
2024

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

The International Conference on Cybersecurity and Cybercrime (IC3) is an annual scientific conference, with the purpose to encourage the exchange of ideas about the evolution of cyberspace, information security challenges, and new facets of the phenomenon of cybercrime. The event provides the appropriate framework for experts to present their research in this field.

The Proceedings of the International Conference on Cybersecurity and Cybercrime includes scientific papers reviewed by the *Editorial Board* that consists of experts from the academic field, their work taking place under the guidance of the *Advisory Board*, composed of internationally recognized personalities from the academic field.

Proceedings of the International Conference on Cybersecurity and Cybercrime
Online ISSN: 2393-0837
Print ISSN: 2393-0772
DOI: 10.19107/CYBERCON
URL: proceedings.cybercon.ro

The International Conference on Cybersecurity and Cybercrime is part of the **CyberCon Romania** event, organized by the Romanian Association for Information Security Assurance.

CyberCon Romania brings together experts from public institutions, private companies, and universities, for raising the level of awareness and embodies the cybersecurity culture.

Website: www.cybercon.ro

The Romanian Association for Information Security Assurance (RAISA) is a professional, non-governmental, non-partisan political, nonprofit, and public benefit association.

Founded in 2012, the association started as an initiative with the aim of promoting and supporting information security activities in compliance with applicable laws and creating a community for the exchange of knowledge between the experts from the public, private, and academic environment. Its vision is to encourage the cybersecurity research and education, and to contribute to the creation and dissemination of knowledge and technology in this domain.

Website: www.raisa.org

CONFERENCE COMMITTEES

CONFERENCE CHAIRMAN

Professor **Ioan C. BACIVAROV**, PhD
National University of Science and Technology POLITEHNICA Bucharest, Romania
Faculty of Electronics, Telecommunications and Information Technology

INTERNATIONAL SCIENTIFIC COMMITTEE

Professor Emeritus **Alessandro BIROLINI**, PhD
ETH Zurich, Switzerland

Professor **Angelica BACIVAROV**, PhD
POLITEHNICA Bucharest, Romania

Irina BAKHAYA, PhD
“Al. I. Cuza” Police Academy, Romania

Natalia BELL, D.Sc.
Marymount University, United State of America

Professor **Răzvan BOLOGA**, PhD
University of Economic Studies, Romania

Assoc. Prof. **Darius BUFNEA**, PhD
Babeş-Bolyai University, Romania

Assoc. Prof. **Ciprian CONSTANTIN**, PhD
“Al. I. Cuza” Police Academy, Romania

Viorel GAFTEA, PhD
Romanian Academy, Romania

Alexandru GEORGESCU, PhD
National Institute for R&D in Informatics, Romania

Assist. Prof. **Cătălin GOLOP**, PhD
“Al. I. Cuza” Police Academy, Romania

Assoc. Prof. **Niculae IANCU**, PhD
Constanța Maritime University, Romania

Assoc. Prof. **Andrei IGNAT**, PhD
“Al. I. Cuza” Police Academy, Romania

Angela IONIȚĂ, PhD
Research Institute for Artificial Intelligence, Romania

Assist. Prof. **Andrei LUCHICI**, PhD
Romanian-American University, Romania

Assoc. Prof. **Dumitru-Iulian NĂSTAC**, PhD
POLITEHNICA Bucharest, Romania

Pierluigi PERRONE, PhD
LUISS University, Rome, Italy

Professor **Florin POPESCU**, PhD
"Carol I" National Defence University, Romania

Assoc. Prof. **Eduard-Cristian POPOVICI**, PhD
POLITEHNICA Bucharest, Romania

Assoc. Prof. **Ciprian PUNGILĂ**, PhD
West University of Timișoara, Romania

Assoc. Prof. **Gabriel RAICU**, PhD
Constanța Maritime University, Romania

Professor **Răzvan RUGHINIȘ**, PhD
POLITEHNICA Bucharest, Romania

Professor **Anurag SHARMA**, PhD
GNA University, India

Assoc. Prof. **Emil SIMION**, PhD
POLITEHNICA Bucharest, Romania

Professor **Pradeep Kumar SINGH**, PhD
University of Information Technology, India

Assoc. Prof. **Adrian STERCĂ**, PhD
Babeș-Bolyai University, Romania

Assoc. Prof. **Mihai SUCIU**, PhD
Babeș-Bolyai University, Romania

INTERNATIONAL SCIENTIFIC COMMITTEE (cont.)

ORGANIZING COMMITTEE

ACKNOWLEDGEMENT:

This volume was created with the support of professors from:
- The Department of Electronic Technology and Reliability, Faculty of Electronics, Telecommunications and Information Technology, National University of Science and Technology POLITEHNICA Bucharest.
- The Department of Police, Faculty of Police, “Alexandru Ioan Cuza” Police Academy.
- The Department of Information Systems and Cyber Operations, Faculty of Security and Defence, “Carol I” National Defence University.

TABLE OF CONTENTS

Celebrating 100 Years of Modern Quality

Ioan C. BACIVAROV
National University of Science and Technology POLITEHNICA Bucharest, Romania
Faculty of Electronics, Telecommunications and Information Technology
ioan.bacivarov@upb.ro

Abstract

Quality, an omnipresent characteristic, with a profound impact on the entire economic and social life, recently celebrated this year a century since it was founded as a science. In the first part of the paper, the author analyzes how quality was founded as a science and analyzes the contributions of Walter Shewhart, considered as the "father of modern quality", as well as other quality gurus in this direction. The author concludes that quality is a dynamic concept, which constantly evolved in the 100 years of its existence. The evolution of quality in this first century of existence is analyzed and the prospects for the development of this important field are highlighted. Some of the Romanian Association for Information Security Assurance (RAISA)'s contributions to the implementation of cybersecurity (an important component of quality) culture are highlighted. Finally, some workshops organized under the auspices of RAISA in May 2024 in order to celebrate a century of modern quality are briefly analyzed.

Index terms: Quality, Quality history, Quality evolution, Walter Shewhart, Cybersecurity, Future of Quality

1. *Quality*, an omnipresent characteristic, with a profound impact on the entire economic and social life, recently celebrated a century since it was founded as a science.

Historians of the field appreciate that the modern quality was born a century ago, on 16 May 1924, when the young engineer **Walter Shewhart** introduced the *first control chart*, which launched the *statistical process control* and the *quality improvement*.

According to the great quality guru Deming, Shewhart's invention of the control chart in 1924 has been considered as one of the greatest contributions to the philosophy of science [8].

Walter Shewhart was the *pioneer* and *visionary* of *modern quality control*. Consequently, he has a special place in list of the most important "*quality gurus*".

2. I have extensively presented the personality of *Walter Shewhart* and his contributions to the development of quality as a science in an extensive article that I published a decade ago [1]. This paper was based on original documents that I obtained both from companies that had an essential role in the development of quality, and from Shewart's descendants, especially from Mr. *Darin Sekulic*, Shewhart's great-grandson, to whom I renew my thanks on this occasion.

Next, I will briefly present the main contributions of Shewhart, as well as the way in which they were received by the caliticians of the era.

Shewhart attended the University of Illinois receiving an A.B. in 1913, then an A.M. degree in 1914. He was awarded his doctorate from the University of California in 1917.

In 1918, Walter Shewhart joined the *Western Electric Company*, a manufacturer of telephony hardware for *Bell Telephone*. Bell Telephone's engineers had been working to improve quality and reliability of their transmission systems. Bell Telephone had already realized the importance of reducing variation in a manufacturing process, the basis of all *lean* production. Moreover, they had realized that continual process-adjustment in reaction to non-conformance actually increased variation and degraded quality [4], [5], [10].

In 1924, the young engineer Shewhart framed the problem in terms of "*assignable-cause*" and "*chance-cause*" variation and introduced the "*control chart*" as a tool for distinguishing between the two. Shewhart stressed that bringing a production process into a state of "statistical control", where there is only chance-cause variation, and keeping it in control, is necessary to predict future output and to manage a process economically.

Walter Shewhart and the revolutionary control chart he proposed in May 1924

Shewhart worked at Bell Telephone Labs on *statistical tools* to examine when a corrective action must be applied to a process. His writings were on statistical control of industrial processes and applications to measurement processes in science. The control chart techniques which he developed have been widely adopted [6], [7].

3. As I have already mentioned, in May 1924 Walter Shewhart introduced the *first control chart,* as a method to determine when a process was in a state of statistical control. Shewhart's methods were the basis for *statistical process control* (SPC) - the use of statistically based tools and techniques for the management and improvement of processes.

Walter Andrew Shewhart (1891 - 1967) - the “father” of modern quality

When Shewhart joined the Inspection Engineering Department at Hawthorne in 1918, industrial quality was limited to inspecting finished products and removing defective items; but that all changed in May 1924. The chief of Walter Shewhart, *George Edwards*, described this event:

"*Dr. Shewhart prepared a little memorandum only about a page in length. About a third of that page was given over to a simple diagram which we would all recognize today as a schematic control chart. That diagram, and the short text which preceded and followed it, set forth all of the essential principles and considerations which are involved in what we know today as process quality control*" [5].

Dr. George Edwards had observed the birth of the modem scientific study of process control. That same year, Dr. Shewhart created the first statistical control charts of manufacturing processes, which involved statistical sampling procedures. Shewhart published his findings in a 1931 book*, Economic Control of Quality of Manufactured Product* [9].

Shewhart worked to advance the thinking at Bell Telephone Laboratories from their foundation in 1925 until his retirement in 1956, publishing a series of papers in the *Bell System Technical Journal*.

During the 1930s, *Shewhart*'s work led him to fundamental scientific and philosophical issues, particularly those concerned with *operationalism* [10].

While Shewhart's ideas on control charts were adopted at Western Electric, they had limited impact outside the company until the late 1930s when he started working with *W. Edwards Deming* at the War Department of the United States. Deming and other engineers and statisticians worked with the War Department, creating a series of sampling inspection plans in quality field, that were published as the MIL-STD (military standard) series.

In 1939 Shewhart published the important book *Statistical Method from the* Viewpoint *of Quality Control.* The publishers of this book mentioned that: *In this classic volume (...) Dr. Shewhart illuminates the fundamental principles and techniques basic to the efficient use of statistical method in attaining statistical control, establishing tolerance limits, presenting data, and specifying accuracy and precision.* [8].

In order to aid a manager in making scientific, efficient, economical decisions, he developed *Statistical Process Control methods*. Many of the modern ideas regarding quality owe their inspiration to Dr. Shewhart.

He also developed the *Shewhart Cycle Learning and Improvement Cycle*, combining both creative management thinking with statistical analysis.

Walter Shewhart was the pioneer and visionary of modern quality control. Shewhart's name opens the select gallery of the great names in the history of modern quality. This gallery contains the names of the great "gurus" of quality, among which we could mention: *Edwards Deming, Joseph M. Juran, Kaoru Ishikawa, Philip Crosby and Armand V. Feigenbaum* a.o.

During the 1990s, *Shewhart*'s genius was re-discovered by another generation of managers, through intermedium of the "*Six Sigma*" approach [14].

4. As mention in [11] in the first part of the last century, *quality* was defined as "*conforming to the standards and specifications of a product*". Thus, the commonly adopted quality practices by industries were the standardization of quality, inspection, and rework. Deming emphasized that "quality is to fulfill the requirements of customers and satisfy them" [8]. Hence, the meaning of quality was gradually changed to a "customer-focused" perspective. Enterprises, therefore, committed themselves to satisfy customers' needs and expectations. Their aim was to pursue customer's satisfaction and loyalty . Companies also developed a number of methods to find out customers' needs and expectations. But, when some important companies announced several innovative products, and their sales were increasing, it became apparent that only satisfying customers' requirements are not enough. As a matter thereof the identification and fulfillment of customers' unsatisfied latent needs was gauged in conjunction with their emotional responses [11].

Concerning the *future of quality*, some authors consider that *Quality 4.0* is the next natural step in the evolution of this field. It is based on a new paradigm that enables smart decisions through empirical learning, empirical knowledge discovery, and real-time data generation, collection, and analysis [12]. As Quality 4.0 matures and different initiatives unfold across manufacturing companies, intractable engineering problems will be solved using the new technologies. Advancing the frontiers of manufacturing science, enabling manufacturing processes to move to the next sigma level, and achieving new levels of productivity is possible. Quality 4.0 is still in a definition phase where different authors have different perspectives on how to apply the new technologies.

An interesting new concept - learning quality control (LQC) - was introduced in [12]; this is a process monitoring system based on machine learning and deep learning; LQC focuses on real-time defect prediction or detection. The task is formulated as a binary classification problem, where historical samples *(X, l)* are used to train the algorithms to automatically detect patterns of concern associated to defects (e.g., anomalies, deviations, non-conformances).

5. In the hundred years of its existence, *quality* was a dynamic concept, which constantly evolved: in the first decades of its existence, the focus was on the issue of *inspection* and *statistical control* of product quality (the corresponding procedures being developed); in the 1960s ... 1970s, the focus began to shift towards the quality *assurance* of products and services.

In the 80s, the *Total Quality Management (TQM)* concept was founded, and starting with the 90s, an increasing importance was given to the *certification* of management systems: the appearance of standards aimed at the certification of quality management systems from the ISO 9000 series and those that followed them (ISO 14000, IS0 45000, ISO 27000 etc.) is considered a real revolution in the field.

In the current view, *quality* is considered a *vector quantity*, having a static component (*conformity*) and several dynamic components *(reliability, maintainability, security, survivability*, a.o.) whose importance has varied over time. *Reliability* began to be substantiated as science starting with the 50s, *maintainability* - starting with the 60s, and *security/safety* starting with the 70s.

Currently, the importance of security has increased, especially that of *cyber-security*, but also that of *resilience*.

6. Of course, along with the development of new disciplines in the domain of quality and dependability, there was also the problem of training specialists in these emerging fields through the development of appropriate undergraduate and post-graduate educational programs.

The first *educational programs* in the field of *quality* were held in the fifth and sixth decades of the previous century at the company level by quality "gurus" and by their consulting teams.

After 1965, several *reliability* education programs were developed at various American universities, including the Air Force Institute of Technology Dayton, Ohio, U.S. Naval Post-Graduate School Monterey, California, University of Phoenix, Arizona, Princetown University, New Jersey and Columbus University, New York.

In this context, it is noted that in Romania, especially within the Polytechnic Institute / University POLITEHNICA of Bucharest (PIB / UPB)[1] - the largest technical university in Romania - there have been valuable educational initiatives in the field quality and dependability, which places it at the forefront at European and even global level.

An essential role in the development of educational and research programs in the field of quality and reliability in the field of electronics, telecommunications and information technology was played

[1] Starting with 1992, the Polytechnic Institute of Bucharest (PIB) became the University "POLITEHNICA" of Bucharest (UPB). Since 2023, UPB becomes the National University of Science and Technology (NUST) "POLITEHNICA" Bucharest.

by the Department (Chair) of *Electronic Technology and Reliability (ETR*) of the Faculty of Electronics and Telecommunications (ElTc - PIB), founded in 1971, at the initiative of Professor *Vasile Cătuneanu* [2].

As a founding member of the ETR Department, I am proud that in the more than five decades of professional activity that I have dedicated to the development of the department and the field of quality and reliability, I have contributed to the development of numerous graduate and postgraduate programs in this domain.

The most important postgraduate programs that I have initiated and coordinated are **the Postgraduate Academic Program "Quality, Reliability, and Maintainability of Complex Systems" (1980 - 2008)** and the master's programs. *"Quality and Reliability Engineering" - ICF (1996-2006) and "Quality and Dependability in Electronics and Telecommunications" - ICSFET (starting with 2006).* A detailed presentation of these programs is done in [2].

7. The new political and social context in Romania after 1989 led to the emergence of several foundations and non-governmental organizations, in the broad field of quality, among which we would like to especially mention the activity of the *Romanian Association for Information Security Assurance (RAISA).*

Indeed, in November 2012 - when the concepts related to this field were not yet sufficiently well implemented (at least, at the level of Romania), at the initiative of a group of enthusiastic and dedicated professionals to the IT security field from the EUROQUALROM Laboratory of the Faculty of Electronics, Telecommunications and Information Technology (FETIT) of the University "POLITEHNICA" of Bucharest (including two university professors with experience, pioneers of the dependability field in Romania) and from the Police Academy "Alexandru Ioan Cuza" Bucharest has founded the *Romanian Association for Information Security Assurance* **-** *RAISA*, a professional, non-governmental, non-partisan political, non-profit and public benefit association [3].

During the years since then, other experts from academia, research, the corporate environment, and public administration - mainly PhD graduates in the field - have joined RAISA's efforts to promote cybersecurity at the national level.

All those involved in the development of RAISA understood the importance of the domain, the unique perspectives of the development of the field and the fact that only the implementation of a vast culture of cybersecurity can contribute to its success.

8. As mentioned in a press release from the AGERPRES National Press Agency [13] "to mark the centenary of quality, the *Romanian Association for Information Security Assurance (RAISA)* organized in the middle of May 2024 - together with partners from the academic environment - several events, in physical and hybrid format. they were attended by specialists in the field from different generations, students, masters and doctoral students in the field".

A first workshop dedicated to this event. was organized on May 13, 2024, under the auspices of the EUROQUALROM Laboratory from the Faculty of Electronics, Telecommunications and Information Technology (ETTI) - National University of Science and Technology "POLITEHNICA" (NUSTPB) Bucharest and RAISA.

In its opening, Professor Emeritus *Ioan C. Bacivarov,* Ph.D, Director of EUROQUALROM-ETTI emphasized the significance of this event and presented the significant developments in the field of quality in this century of continuous evolution. The speaker emphasized that in this century of existence, concerns in the field have evolved permanently, from aspects related to quality control and assurance to those related to its management and certification. Likewise, the weight of quality components has changed, evolving from compliance control to reliability and maintainability, in the second half of the last century and reaching security, especially cyber security in the last two decades.

Participants at the Workshop from 13 May 2024

Next, Professor *Angelica Bacivarov*, PhD, Vice-President of ARASEC for educational programs, evoked the significant postgraduate educational projects and programs developed within the Electronic Technology and Reliability department ETTI - NUSTPB) in the more than five decades of its existence and especially the European educational project TEMPUS S_JEP 11300 "EUROQUALROM".

For his part, Professor *Gabriela Nicolescu*, Director of the Computer Engineering and Software Department at Polytechnique Montréal presented the educational programs from her university in this field, in the wider context of educational programs in the field of quality and informational security developed in Canada.

In the final part of this workshop, the master students from the Quality and Dependability Engineering in Electronics and Telecommunications (ICSFET) master's program, developed within ETTI-UPB, discussed various aspects related to the technical, managerial and educational aspects of quality and dependability, as they are reflected in the curricula of the mentioned program.

Another workshop from the series of those dedicated to the centenary of modern quality was organized on the anniversary day (May 16th, 2024) and was dedicated to aspects related to the dependability of IT systems and especially IT security issues.

Doctoral students in the field of cyber-security, members of the guidance commissions and other specialists in the field participated in the debates, which analysed current aspects and perspectives in this important field.

Since there is an acute lack of specialists in these key fields, at universities with a technical profile - and especially at the profile faculties of NUST "POLITEHNICA" Bucharest - they have been implemented in the last decade and will be implemented in the coming years many master's and doctorate programs in this priority field, Prof. Ioan Bacivarov mentioned at the end of the workshop.

9. To conclude, we can say that the celebration of the anniversary of a century since modern quality was implemented as a science was - for RAISA members as well as for ETTI-NUST POLITEHNICA Bucharest master's and doctoral students alike - an opportunity to evoke the birth and evolution of an important domain for the economic-social life of a country as well as the prospects for the development of this field, especially through the prism of the *cyber-security* component.

References

[1]. I.C. Bacivarov, Nine Decades of Modern Quality. Walter A. Shewhart - A Pioneer and Visionary of Quality, International Journal of Information Security and Cybercrime, Vol. 3(2014), no.1, pp. 9-16.

[2]. I.C. Bacivarov, The Department of Electronic Technology and Reliability from the University Politehnica of Bucharest - 50 Years. Five Decades in the Service of Education and Scientific Research in the Field of Quality and Dependability, International Journal of Information Security and Cybercrime, vol.10 (2022), pp. 91-109.

[3]. I.C. Bacivarov, The Romanian Association for Information Security Assurance (RAISA): Ten Years in the Service of Cybersecurity - Editorial, International Journal of Information Security and Cybercrime, vol.11 (2022), pp. 7-18.

[4]. I.C. Bacivarov, “Monștrii sacri ai calității: Walter A. Shewhart”, Calitatea - Acces la success/ Quality- Access to Success, no. 2, 2001.

[5]. Walter Andrew Shewhart: http://www-groups.dcs.st-and.ac.uk (accessed March 20, 2024).

[6]. M.D. Fagen (ed.), A History of Engineering and Science in the Bell System: The Early Years (1875-1925), 1975.

[7]. D. Bayart, W.A. Shewhart, C.C. Heyde and E. Seneta, Statisticians of the Centuries, Springer Verlag, New York, 2000, pp. 398-401.

[8]. Deming, W., E. Out of Crisis. 1986; Cambridge, MA: MIT Press.

[9]. W. Shewhart, Economic control of quality of manufactured product, New York: D. Van Nostrand Company, 1931.

[10]. Western Electric History: https://memorial.bellsystem.com/westernelectric_history.html (accessed May 10, 2024).

[11]. Ching-Chow Yang, The Evolution of Quality Concepts and the Related Quality Management, in https://www.intechopen.com/chapters/53946 (accessed May 5, 2024)

[12]. Escobar, C. A., Morales-Menendez, R., Machine Learning in Manufacturing: Quality 4.0 and the Zero Defects Vision. To appear in Elsevier (2024).

[13]. AGERPRES Press release (16 May 2024): Modern quality celebrates a century of existence.

[14]. I.C. Bacivarov, A Century of Modern Quality, International Journal of Information Security and Cybercrime, Vol. 13(2024), no.1, pp. 9-14.

[15]. G. Petrica, RAISA Workshops that Marked A Century of Modern Quality, International Journal of Information Security and Cybercrime, Vol. 13(2024), no.1, pp. 76-77.

The Effect of the KiberPajzs Initiative on Fraud Detected in Electronic Payments in Hungary

Gabriella BIRÓ
Ludovika University of Public Service, Budapest, Hungary
biro.gabriella@uni-nke.hu

Abstract

The paper examines what effect the KiberPajzs initiative has on fraud detected in electronic payments in Hungary for the 2023-2024 period. First the current electronic payment fraud landscape of Hungary is described through cybercrime tendencies, the impact of digitalization on banking, and the regulatory background of electronic payments. Then the KiberPajzs initiative is introduced together with its related communicational, regulatory and law enforcement projects. Finally, the recent quarterly payment fraud data published by the Central Bank of Hungary is examined and the effects of KiberPajzs are evaluated. The author argues that the decrease in the number and value of fraudulent electronic transactions and the increase in identified failed fraud attempts coincide with the activities of the KiberPajzs initiative.

Index terms: cybercrime, electronic payments, financial education, fraud prevention, payment fraud

1. Introduction

With the increasing use of digital banking channels and the growing sophistication of tools available for cybercriminals to target their victims, the number and value of fraudulent electronic payments is on the rise worldwide. In Hungary, authorities, banks and other stakeholders have joint forces to counter this tendency and started the KiberPajzs (CyberShiled in English) initiative in 2022 as a coordinated effort to address the issue [1]. This paper seeks to describe the various aspects of the KiberPajzs initiative and show the effect it has been having on the number and value of fraudulent payments.

The question of what effect the KiberPajzs initiative has had on fraudulent electronic transactions in Hungary will be examined through the analysis of the quarterly payment reports regularly published by the Central Bank of Hungary (Magyar Nemzeti Bank - hereinafter referred to as MNB) [2]. These datasets are based on the quarterly regulatory reporting of payment service providers and commercial banks in Hungary and contain data on fraud and attempted fraud observed in card payments and the electronic payments systems. The scope of this paper is limited to electronic payments (credit transfers) and does not include card payment related data. Other sources of data are also available such as the 2024 Report on Payment Fraud by the European Central Bank [3] and the annual report of the Hungarian Financial Arbitration Board [4], but even though these confirm the identified trends, both reports have a different data frequency (half-yearly or annual) and larger time lag compared to the MNB data.

2. The Current Landscape of Electronic Payment Fraud in Hungary

Fraudulent transactions identified in electronic payments may fall into two basic categories: fraud cases conducted via the payment system - such as traditional scams utilizing electronic payments -, and payment fraud cases that are made possible because of the electronic channels such as phishing for electronic banking credentials. Both categories rely to some extent on the communication with potential victims and until recent years the Hungarian language provided a barrier to criminals that was difficult to overcome, because the majority (51.3% in 2022) of the adult Hungarian population does not speak any foreign language [5]. With the development of artificial intelligence and Large Language Models, fraudsters are now able to create credible messages in Hungarian [6],[7]. Vishing (voice phishing, usually phone calls) is also becoming very common, especially coupled with phone number spoofing, where the calling number displayed for the target is that of a commercial bank or other trusted party such as the Central Bank of Hungary [8].

2.1. Payments Related Cybercrime in Hungary

The annual Payment Systems Report published by the MNB contains a section on the fraud cases "observed through electronic payments", meaning both electronic payment fraud that is made possible by the electronic channel and other types of fraudulent payments via electronic channels. Card payment related and non-card (credit transfer) data is published separately, as the governing rules and IT systems involved in the transactions are different for card and non-card payments. A sharp rise in both the number and value of non-card fraudulent transactions, but Hungary is still among the less affected countries [9].

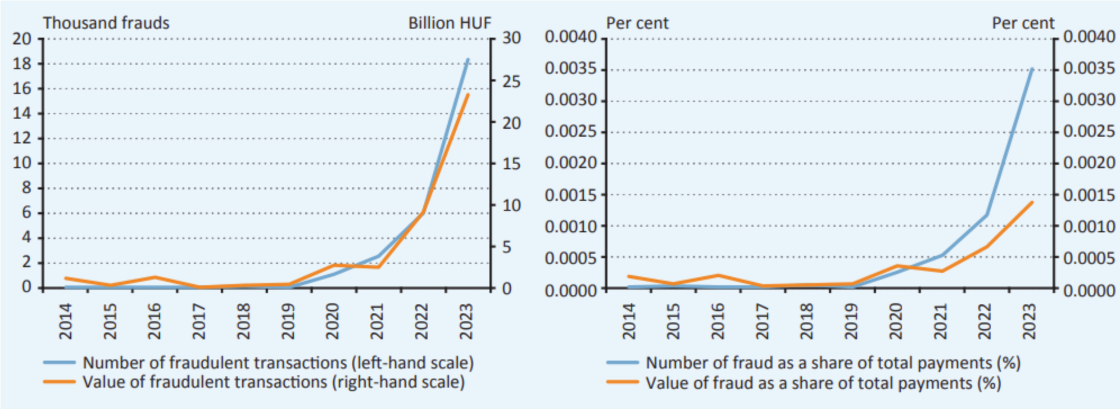


Fig. 1. Volume and value of non-card fraud published by MNB [9]

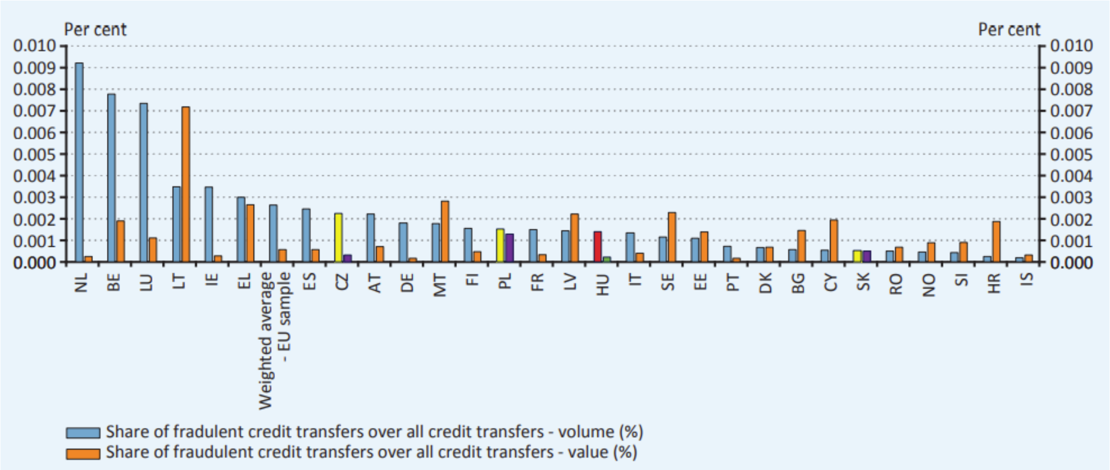


Fig. 2. Volume and value share of successful fraudulent credit transfers over all credit transfers (EBA, 2022) [9]

2.2. The Effects of Digitalization on Electronic Payments

In addition to the language factor, another major contributor to the rising fraud trends may be the rapid digitalization of the payment service providers and the COVID-19 induced transfer of consumers/clients to the digital channels (as opposed to visiting the brick-and-mortar bank branches). Some of these clients are not comfortable with the use of electronic channels and their lack of computer literacy makes them vulnerable to online fraud. On the other hand, now all Hungarian banks offer online current account opening and personal loan applications [10], thus serving their increasingly digitalized clients, but also providing a bigger attack surface for fraudsters.

2.3. Regulatory Background

The legal framework for cybercrimes in Hungary is in line with the Budapest Convention on Cybercrime [11], covering basically all cases of electronic payment fraud that are not covered by the fraud related article (§ 373, “csalás”) of the Hungarian Criminal Code [12], which is favoured by judicial practice. However, the Budapest Convention is considered by some to be outdated and in need of a review [13].

Hungary has implemented the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2, [14]) in its payment regulations, therefore the regulatory environment is very similar to all other EU countries. The PSD2 basically mandates the use of strong authentication (two-factor authentication) for online transactions [15]. The original purpose of the regulation was to increase the security of the payment systems and protect the consumers by defining strict liability rules for fraudulent transactions. According to the European Central Bank, “observed fraud rates for credit transfers remained consistently at 0.002% or below across all categories analysed” in 2022 and 2023 [3]. However, the unexpected result of the PSD2 implementation was that criminals found new ways to target consumers and trick them into handing over their e-banking credentials, resulting in increasingly large losses on the client side with 98.3% of the financial liabilities falling to consumers [9]. This resulted in a strong perception that banks do not do enough to protect their customers and has begun to undermine the trust in the banking system, spurring MNB to take action.

3. The KiberPajzs Initiative

The founding members of the KiberPajzs initiative were the Central Bank of Hungary (MNB) both in its capacities of financial supervisor and consumer protection authority, the Hungarian Banking Association, the National Media and Infocommunications Authority (NMHH), the National Cyber Security Center of Hungary (NBSZ-NKI) and the Hungarian Police. The five original founding organizations signed a cooperation agreement on 7th November 2022 and the website https://www.kiberpajzs.hu was launched at the same time. The founders were later joined by the Hungarian Financial Arbitration Board, the Ministry of Justice (also including the network of victim support centres), the Hungarian State Treasury, the Supervisory Authority for Regulated Activities (SZTFH), the Ministry of Economics and the National Protective Service (NVSZ) [1]. These powerful participants launched a comprehensive educational programme to improve customers' digital financial awareness through a unified, ongoing communication campaign and to help consumers to detect and prevent fraud at an early stage. In addition to the communication campaign, another very important benefit of the initiative is the sharing of knowledge between experts on fraud scenarios, analysis of fraud scripts, modus operandi, characteristics and trends, and more efficient prevention and protection processes.

The outcomes of the initiative have been manyfold:

- the awareness campaign is ongoing, with various platforms and messages to a wide variety of target audiences from billboards to television spots, TikTok videos and paper handout at pensioners' club events by local police officers;
- smoother and more efficient interaction between law enforcement agencies, banks and other authorities, resulting in faster interventions and successful cases of asset recovery;
- streamlined journey for fraud victims, with guidance for banks on how to communicate sympathetically to fraud victims [1], improved police reporting, unified messages for consumer protection and redressal procedures and easier access to victim support;
- improved legal framework for cooperation, information sharing and fraud prevention thanks to the participation of major regulators.

4. Other Initiatives Related to KiberPajzs

Some participants of the KiberPajzs initiative also added their own spinoffs to the project and enhanced the actions of KiberPajzs. Particularly the MNB, the Hungarian Banking Association (together with MédiaUnió) and the Hungarian Police launched successful actions.

4.1. MNB action

MNB issued a comprehensive Fraud Recommendation in 2023 for supervised payment service providers (mainly banks) that covers the prevention, detection and management of fraud observed through payment services and comes into force in three stages: 1st January 2024 for "quick wins", 1st September 2024 for requirements that need a larger implementation effort, 1st March 2025 for real-time fraud monitoring systems [16]. The Fraud Recommendation introduced new requirements on contracting, on the delivery of new payment instrument to the customers (such as new payment cards or mobile banking activation), on the lines of defence preventing external and internal fraud, the design and operation of the IT environment and process controls, analysis and lessons learnt of fraud cases, improving customers' security awareness, transaction limits and restrictions, strong customer authentication by third party service providers, mitigation of the risks attached to the multifunctional instrument providing any element of strong customer authentication, transaction monitoring mechanisms related to fraud, and the requests for rectification related to unauthorised payment transactions. It is worth noting that though the recommendations of MNB are not legally binding, MNB evaluates the compliance to the recommendations during its supervisory activities, meaning that noncompliance can result in supervisory actions.

In addition to the Fraud Recommendation, the MNB has also issued several circulars detailing expectations about the use of KiberPajzs communication materials by banks of drawing the attention of banks to specific modus operandi for electronic payment fraud [17]. Some of these circulars are not public, so they are not published but only shared with the intended recipients.

The most resource intensive action by MNB is the initiation of a central fraud monitoring and prevention solution that will be developed and operated by GIRO, the MNB owned Hungarian clearing house that processes all domestic transactions [18]. The development is expected to go live in 2025, so it is not relevant for the current payment trends.

4.2. The Mátrix Project

The Hungarian Police announced the Mátrix project in October 2023 with the intent to tackle online fraud [19]. They established a new strategic unit specialized in cybercrime, with a provisional headcount of 300 officers and a mandate to cooperate across the law enforcement organization countrywide. They have ever since encountered some serious success stories such as dismantling a complete call centre of 41 individuals specialized in Hungarian language vishing and AnyDesk fraud in cooperation with the Ukrainian police [20], [21]. These actions have resulted in a perceivable drop of criminal activity.

The new unit is also very active in communicating both the fraud prevention messages and the success stories and organizing online and offline educational event for various target audiences.

4.3. The MédiaUnió Campaign

MédiaUn[22]association of media content providers, who donate their free spots for social purposes and select a topic each year. In 2023 and 2024 they decided to address online fraud and cooperated with the Hungarian Banking Association and the KiberPajzs subject matter experts to create messages that are consistent with the KiberPajzs campaign but have a distinct design. The MédiaUnió campaign significantly amplified the fraud prevention and security awareness messages and provided new channels of communication.

4.4. Pénz7

Pénz7 [22] is the Hungarian equivalent of the European Money Week organized by the European Banking Federation in order to provide financial education and raise awareness about money and personal finances. Throughout one week in March, many financial education events are organized across Europe by national banking associations and the European Banking Federation. [23]. In Hungary, the main targets of the educational campaign are schools, with different materials for all ages of children. In 2023, the special focus of the campaign was the security of digital finance, with professional volunteers touring the country and delivering lectures and classes and various educational institutions [24].

5. Fraud Data Published by the Central Bank of Hungary

In accordance with Article 96(6) of PSD2 [14], payment service providers (mostly banks) are required to report statistical data on fraud relating to different means of payment to their competent authorities, that is the MNB in case of Hungary. These data are collected for every quarter of the year and published by the MNB regularly. The changes in reporting methodology sometimes make comparisons difficult, but the reporting regime under PSD2 is consistent enough for 2020-2024 to allow for analysis. Major changes are expected in the reporting framework for 2025 due to regulatory changes.

The data reported to MNB is collected through the official reporting platform of MNB and payment service providers failing to submit reports are subject to supervisory actions such as fines, but the different reporting practices of the payment service providers (mainly banks) make the data somewhat less reliable, even though MNB publishes a detailed guidance on how and what to report [25]. Payment fraud related data is reported currently in form P12. This data is more relevant and timely than other data sources such as the complaints handled at the financial consumer protection authority, the Financial Arbitrage Board of police data, because the fraudulent transactions are reported for the time period when they took place (as opposed to when the client decides to complain or file a police report, which may be typically weeks later in case of complaints) and the latency (not reporting) is much smaller than in case of the police or other sources.

Figure 3. demonstrates the rise of the number and value of fraudulent transactions, as described in the MNB Payment Report for 2023 [9], but we see a significant drop in both the amount and the number of successful fraud in the fourth quarter of 2023, when we would expect to see a rise because of the increase in online shopping (and related fraud) due to the Christmas holidays. In 2023 Q4 the KiberPajzs initiative already took momentum, while the MNB Fraud Recommendations were not yet in force and the Mátrix project had just been announced, so the most likely explanation is that the communication campaign and other KiberPajzs efforts were successful.

In 2024 Q1 we see a spike in the numbers, but the increase in value was caused by a one-off event, a large retail store loosing 6 billion Forints (€15.5 million) to fraud [26]. In 2024 Q2 the trend is declining again.

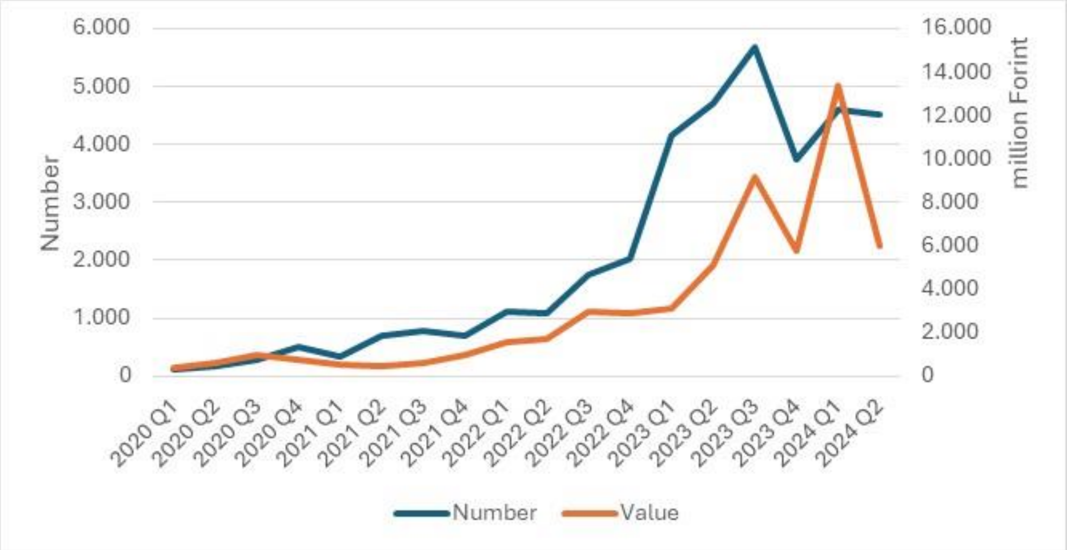


Fig. 3. The number and value of fraudulent transactions in electronic payments (edited by the author based on the dataset published by MNB [2])

Figure 4. shows the number and value of unsuccessful fraudulent transaction attempts, as reported by payment service providers to MNB. The criteria for reporting are the following: "*[...]any case in which the loss incurred by the payment service provider or the customer does not occur (typically the payment order is not executed or the fraudulent customer's claim for reimbursement is rejected by the reporting party). These include cases where the payer's payment service provider intervenes before the payment order is approved, typically as a result of the fraud filtering mechanisms in place, regardless of the origin or main motive of the fraud.*"[25] In case the value of the attempted fraud is not known, the case if reported with a value of 0, so the increase the value seen in 2023-2024 means that more exact data is available, rather than an increase in actual fraud attempts. The drop in the number of attempts can also indicate that fewer frauds attempts are blocked by the banks, because clients are more likely to recognize fraud attempts at an earlier stage.

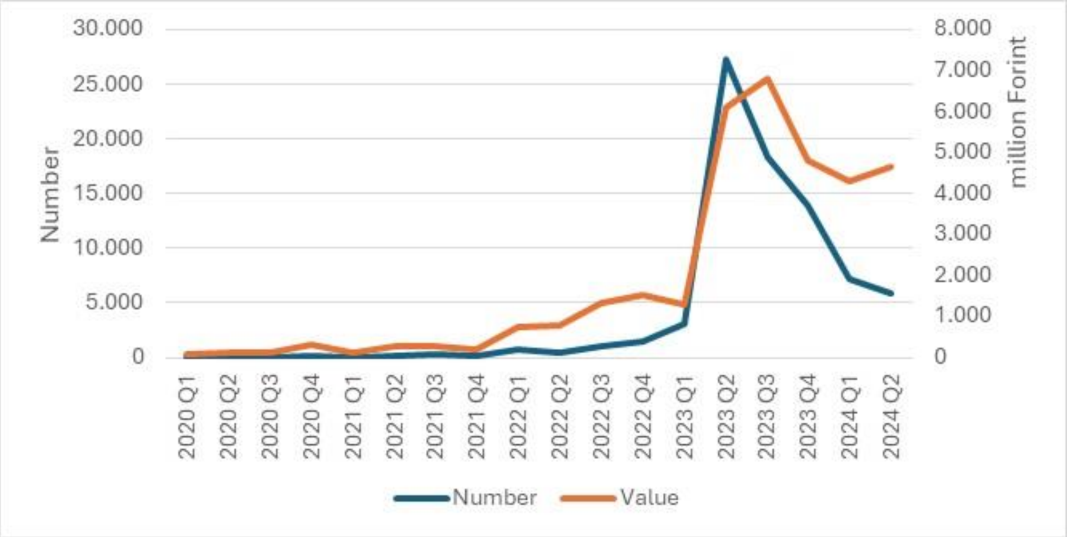


Fig. 4. The number and value of unsuccessful fraudulent transaction attempts in electronic payments (edited by the author based on the dataset published by MNB [2])

6. Conclusion

The data on fraudulent transactions and unsuccessful fraud attempts in electronic payments published by MNB suggests that the KiberPajzs initiative had a positive effect on fraud prevention. Other initiatives that might have had an impact were not mature enough during the reporting period to significantly influence the numbers. MNB itself also made a moderately optimistic announcement about the success of KiberPajzs in 2024, after the release of the 2023 Q3 data [27]. The fight against fraud is never over and we have yet to see what effect the central fraud prevention system will have on payment fraud or is cyber criminals come up with new modus operandi, but for now it seems that KiberPajzs is effective in decreasing electronic payment fraud.

References

[1]. Magyar Nemzeti Bank, ‘Kiberpajzs’. Accessed: Oct. 27, 2024. [Online]. Available: https://kiberpajzs.hu/

[2]. Magyar Nemzeti Bank, ‘Pénzforgalmi visszaélések’. Sep. 16, 2024. Accessed: Oct. 17, 2024. [Online]. Available: https://statisztika.mnb.hu/idosor-3644

[3]. European Central Bank, ‘ECB and EBA publish joint report on payment fraud’. Aug. 01, 2024. Accessed: Oct. 27, 2024. [Online]. Available: https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240801~f21cc4a009.en.html

[4]. Magyar Nemzeti Bank, ‘Jelentés a Pénzügyi Békéltető Testület éves tevékenységéről 2023.’ Accessed: Oct. 27, 2024. [Online]. Available: https://www.mnb.hu/bekeltetes/bemutatkozas/eves-jelenteseink/jelentes-a-penzugyi-bekelteto-testulet-eves-tevekenysegerol-2023

[5]. Eurostat, ‘Number of foreign languages known (self-reported) by sex’. Eurostat, 2022. doi: 10.2908/EDAT_AES_L21.

[6]. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024, European Union Agency for Law Enforcement Cooperation. LU: Publications Office, 2024. Accessed: Jul. 28, 2024. [Online]. Available: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

[7]. Europol, Facing reality?: law enforcement and the challenge of deepfakes : an observatory report from the Europol innovation lab. LU: Publications Office, 2024. Accessed: Oct. 17, 2024. [Online]. Available: https://data.europa.eu/doi/10.2813/158794

[8]. ‘Ismét csalók próbálnak visszaélni az MNB nevével’. Accessed: Oct. 27, 2024. [Online]. Available: https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2023-evi-sajtokozlemenyek/ismet-csalok-probalnak-visszaelni-az-mnb-nevevel

[9]. Magyar Nemzeti Bank, ‘Payment Systems Report’. Accessed: Oct. 27, 2024. [Online]. Available: https://www.mnb.hu/en/publications/reports/payment-systems-report

[10]. Magyar Nemzeti Bank, ‘FinTech and Digitalisation Report, July 2024’. Jul. 2024. Accessed: Oct. 27, 2024. [Online]. Available: https://www.mnb.hu/en/publications/reports/fintech-and-digitalisation-report/fintech-and-digitalisation-report-july-2024

[11]. Convention on cybercrime | EUR-Lex. Accessed: Oct. 27, 2024. [Online]. Available: https://eur-lex.europa.eu/EN/legal-content/summary/convention-on-cybercrime.html

[12]. Btk. (új) - 2012. évi C. törvény a Büntető Törvénykönyvről - Hatályos Jogszabályok Gyűjteménye. Accessed: Oct. 27, 2024. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1200100.tv

[13]. C. Krasznay, ‘Húsz év a globális kiberbűnözés elleni küzdelemben : A Budapesti Egyezmény értékelése’, Külügyi Szemle, vol. 20, no. Különszám, pp. 191-214, 2021, doi: 10.47707/Kulugyi_Szemle.2021.2.09.

[14]. DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on Payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Accessed: Oct. 27, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32015L2366

[15]. COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication. Accessed: Oct. 27, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32018R0389

[16]. Magyar Nemzeti Bank, Recommendation No 5/2023 (VI.23.) of the Magyar Nemzeti Bank on the prevention, detection and management of abuses observed through payment services.

[17]. Magyar Nemzeti Bank, 'Vezetői körlevelek'. Accessed: Oct. 27, 2024. [Online]. Available: https://www.mnb.hu/felugyelet/szabalyozas/felugyeleti-szabalyozo-eszkozok/vezetoi-korlevelek

[18]. GIRO, 'Összefogással a biztonságos banki tranzakciókért'. 2024. Accessed: Jul. 21, 2024. [Online]. Available: https://www.giro.hu/news/biztonsagos-banki-tranzakciok

[19]. ORFK, 'Mátrix Projekt a kiberbiztonságért', A Rendőrség hivatalos honlapja. Accessed: Oct. 27, 2024. [Online]. Available: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/zsaru-magazin/matrix-projekt-a-kiberbiztonsagert

[20]. 'Mátrix Projekt - közös nemzetközi akcióban számolták fel a rendőrök az eddigi legnagyobb illegális call center hálózatot', A Rendőrség hivatalos honlapja. Accessed: Oct. 27, 2024. [Online]. Available: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/matrix-projekt-kozos-nemzetkozi-akcioban

[21]. 'Поліція Закарпаття ліквідувала масштабну мережу шахрайських кол-центрів - затримано лідера та 18 членів злочинної організації | Національна поліція України'. Accessed: Oct. 27, 2024. [Online]. Available: https://www.npu.gov.ua/news/politsiia-zakarpattia-likviduvala-masshtabnu-merezhu-shakhraiskykh-kol-tsentriv-zatrymano-lidera-ta-18-chleniv-zlochynnoi-orhanizatsii

[22]. 'PÉNZ7 - Pénzügyi és Vállalkozói Témahét', PÉNZ7 - Pénzügyi és Vállalkozói Témahét. Accessed: Oct. 27, 2024. [Online]. Available: https://www.penz7.hu/

[23]. 'EUROPEAN MONEY WEEK', EBF. Accessed: Oct. 27, 2024. [Online]. Available: https://www.ebf.eu/europeanmoneyweek/

[24]. E. Terták and L. Kovács, 'Fókuszban a pénzügyi biztonság kibertérben is - PÉNZ7', G.É.P., vol. 10, no. 1, pp. 5-20, 2023, doi: 10.33926/GP.2023.1.1.

[25]. Magyar Nemzeti Bank, 'Kapcsolódó előírások, technikai segédletek'. Accessed: Oct. 27, 2024. [Online]. Available: https://aszp.mnb.hu//eloirasok-technikai-segedletek

[26]. J. Kwak, 'Pepco Group N.V. - Notice regarding Hungarian business', Pepco Group. Accessed: Oct. 27, 2024. [Online]. Available: https://www.pepcogroup.eu/media-news/pepco-group-n-v-notice-regarding-hungarian-business/

[27]. Magyar Nemzeti Bank, 'Tavaly év végén csökkentek az átutalásos kibercsalások, de továbbra is fokozott figyelem kell'.

A National Security Perspective on Strengthening E.U. Civilian-Defence Cybersecurity Synergy: A Systemic Approach

Niculae IANCU
Constanta Maritime University; West University of Timisoara, Romania
nicu.iancu@marcyscoe.org, Niculae.iancu@e-uvt.ro

Abstract

The integration of civilian and defence sectors within the European Union's cybersecurity framework has become a strategic priority, driven by the increasingly complex nature of digital threats to both national and collective security. This paper examines the need for a systematic approach to enhance civilian-defence cybersecurity synergy, emphasising the importance of coordinated efforts to address a range of challenges, including ransomware, state-sponsored attacks, and hybrid warfare. The study highlights the strategic importance of this integration for national and E.U.-wide interests, identifying key obstacles such as fragmented policy frameworks, operational cultural differences, and resource allocation disparities. To bridge these gaps, the paper proposes strategic solutions, including regulatory harmonisation, joint training programmes, and investment in dual-use technologies. The research underscores the critical role of a unified policy approach in facilitating efficient resource allocation, streamlined communication, and faster incident response. Additionally, it explores the potential of emerging technologies, such as AI and quantum computing, to strengthen cybersecurity capabilities across sectors. Ultimately, the integration of civilian and defence efforts within the E.U.'s cybersecurity ecosystem is essential for building a resilient, cohesive, and adaptive framework, ensuring the protection of digital infrastructure, enhancing national security, and reinforcing the E.U.'s global leadership in cybersecurity.

Index terms: cybersecurity civilian-defence integration, E.U. cybersecurity framework, cyber threats, national security, E.U. sovereignty in cyberspace

1. Introduction

In this era defined by rapid technological advancements and increasing digitalisation, the European Union faces a growing array of cyber threats that pose significant risks to both national and collective security. Cyber incidents have evolved in complexity and scope, ranging from ransomware attacks and data breaches to sophisticated state-sponsored operations and hybrid warfare tactics. These threats can disrupt critical infrastructures, undermine public trust, and weaken the resilience of national economies. The integration of digital systems across civilian sectors—such as finance, healthcare, energy, and transportation—has made these infrastructures particularly vulnerable, heightening the urgency for a robust and coordinated cybersecurity strategy.

Traditionally, the responsibility for national security, including the defence against external threats, has been vested in the defence sector. However, the nature of cyber threats transcends traditional boundaries, often targeting civilian infrastructures and leveraging vulnerabilities in interconnected digital networks. This convergence of civilian and national security concerns necessitates a new approach that integrates the strengths of both sectors. The E.U. has recognised this need, prompting efforts to enhance synergy between civilian and defence entities within its cybersecurity framework. Effective collaboration between these sectors is critical to developing a coordinated response capable of addressing both conventional and emerging threats, ensuring the security and resilience of national and collective E.U. interests.

Despite the strategic importance of this integration, several challenges hinder the development of a cohesive cybersecurity ecosystem across the E.U. Fragmented and ambiguous policy frameworks, differences in operational cultures, and disparities in resource allocation are among the key obstacles that need to be addressed. The lack of harmonised regulations and inconsistent information-sharing protocols can create gaps in defence measures, making it easier for adversaries to exploit vulnerabilities. Additionally, the civilian sector often faces budget constraints that limit the adoption of advanced cybersecurity technologies, while the defence sector, although well-resourced, may lack the flexibility and innovation-driven approach that characterises civilian tech industries.

This paper explores a systematic approach to strengthening the synergy between civilian and defence sectors within the E.U.'s cybersecurity framework. It examines the strategic importance of this integration, identifies key challenges, and proposes solutions to bridge existing gaps. By focusing on regulatory harmonisation, joint training programmes, and investment in dual-use technologies, this study aims to highlight effective strategies for building a cohesive and resilient cybersecurity ecosystem. Additionally, the paper discusses the potential of emerging technologies, such as artificial intelligence (AI) and quantum computing, to enhance cybersecurity capabilities across sectors. Ultimately, this research advocates for a unified policy approach that facilitates efficient resource allocation, streamlined communication, and faster incident response, reinforcing the E.U.'s position as a global leader in cybersecurity while ensuring the protection of its digital infrastructure and national security.

2. Rising Importance of Cybersecurity in National Security

In the contemporary security landscape, the increasing reliance on digital technologies across all sectors of society has dramatically elevated the significance of cybersecurity as a core element of national security. Traditionally, national security was defined through the lens of military strength, state sovereignty, and territorial integrity [1]-[3]. The post-Cold War era expanded the traditional approach to security by introducing non-military dimensions such as economic, societal, and environmental concerns [4]. More recently, the digital revolution has further extended the scope of what constitutes a security threat, incorporating new dimensions that transcend physical borders and include cyberattacks on critical infrastructure, cybercrime, cyber espionage, and the disruption of political processes using digital tools [5].

Cybersecurity has become an essential pillar of national security as states and non-state actors recognise the potential of cyberattacks to cause widespread disruption and damage to a nation’s critical infrastructure, as well as its citizens and society as a whole. The vulnerabilities in sectors such as finance, healthcare, energy, and telecommunications make them prime targets for cyberattacks, which can wipeout essential services and erode public trust. The cyber domain has introduced a new form of power—cyber power—which encompasses both the capacity to defend critical digital assets and the ability to disrupt adversaries' systems [6]. This shift has necessitated a redefinition of what constitutes a national security threat, elevating cyber threats to the top of the security agenda and placing cybersecurity at the centre of state defence mechanisms.

For example, in line with global trends, since 2016, Romania’s National Security Strategies have encapsulated the growing prominence of cybersecurity as a national security priority. In its 2010 edition, Romanian policymakers moved ‘beyond regional instability and terrorism’ to also examine ‘new risks and threats, such as pandemics, natural disasters, and cyber or energy security’. Although at the time they assumed that ‘such threats do not directly affect the state’, they recognised that many of these new factors, ‘radicalised as a result of the current evolution of globalisation, can seriously affect the quality of life and call into question the citizen's safety’ [7]. The 2015 National Security Strategy addressed cyber issues in its security threats assessment, highlighting the growing concern of ‘cyber threats initiated by hostile entities, both state and non-state’. These threats target ‘informational infrastructures of strategic interest to public institutions and companies’. The strategy specifically highlighted the threat of ‘cyberattacks carried out by cybercrime groups or extremist hackers, which directly undermine Romania's national security,’ advancing the cyber domain to a major national security concern. This focus on cybersecurity marks a notable evolution compared with previous National Security Strategies, demonstrating an increased recognition of the critical and expanding nature of cyber threats to national security.

The current 2020 National Security Strategy further develops the concept of cybersecurity by unequivocally integrating it into the ‘extended national security concept’, positioning it on the same level with traditional security domains such as ‘defence, foreign policy, public order, intelligence, counterintelligence, and security’. [8] This demonstrates a ‘multi-dimensional approach to security’ [8], tailored to meet the increasingly complex security challenges of the modern world, while also reflecting Romania’s alignment with Euro-Atlantic strategic thinking. Such a vision ensures the ‘resilience’ of vital sectors, including energy, finance, and critical infrastructure [8], reflecting a broader understanding that cybersecurity is now an integral component of national defence systems which can no longer be neglected or underfunded.

The militarisation of cyberspace further underscores the growing importance of cybersecurity in national and alliance settings. States have increasingly recognised cyberspace as the fifth domain of warfare, alongside land, sea, air, and space. This strategic shift is reflected in the strategies and doctrines of national governments and international security organisations, which now include dedicated cyber defence units within their military and intelligence agencies. For instance, NATO officially recognised cyberspace as a domain of operations in 2016, indicating the strategic importance of securing digital infrastructure to maintain national and international security [9]. Similarly, several ‘great power competitors’ [10], including the United States, China, and Russia, have established cyber commands responsible for both defensive and offensive cyber operations [11]. The pursuit of strategic advantage and dominance now extends well beyond conventional warfare, with cyberspace emerging as a critical arena for geopolitical competition. This has led these and many other nations to invest heavily in developing advanced cyber capabilities, both for executing cyberattacks and for defending against potential threats, thereby establishing cyberspace as a critical domain of future warfare [12]. This demonstrates a growing recognition that cyber threats have the potential to cause significant harm comparable to traditional military attacks, if not greater, because of the interconnectedness of global systems.

One of the most critical developments in the global nexus between cybersecurity and national security is the concept of hybrid warfare [13]. Hybrid warfare combines conventional military tactics with irregular tactics, such as cyberattacks, disinformation campaigns, and economic coercion, to destabilise adversaries [14]. The cyber dimension of hybrid warfare allows adversaries to conduct asymmetric operations that are difficult to trace and even harder to attribute. This is particularly concerning for national security and allied defence because it complicates the conventional understanding of conflict, making it more difficult for states to respond effectively to these threats.

For example, Russia’s cyber operations against Ukraine in 2014, which accompanied its annexation of Crimea, are a prime example of hybrid warfare. These operations included targeted attacks on Ukraine’s critical infrastructure, including energy grids, and extensive disinformation campaigns to destabilise the political environment [15]. Since the full-scale Russian invasion of Ukraine in 2022, cyber warfare has complemented the conventional forces engaged in conflict, further demonstrating how cyberattacks have been integrated into broader military strategies. Cyberattacks were used not only to undermine state functions and disturb adversary military technologies but also to erode public confidence and create confusion, thereby weakening the state's ability to respond to more traditional military threats. This demonstrates the intricate role cybersecurity now plays in the broader national security calculus, especially in the context of hybrid threats.

Moreover, non-state actors have also recognised the potential of cyberattacks to influence national security. Terrorist organisations have attempted to develop cyber capabilities that could be used to disrupt government functions or critical infrastructure, though their success has been limited thus far [16]. However, the increasing availability of cyber tools on the black market and the proliferation of sophisticated hacking techniques raise concerns about the future capabilities of such groups. Cyber warfare, therefore, poses a multilayered threat, not just from state actors but from a diverse array of non-state actors who could leverage these tools to undermine national security.

The rapid advancement of technology, particularly in fields like artificial intelligence (AI), the Internet of Things (IoT), and quantum computing, is reshaping the nature of cybersecurity challenges. As these technologies become more integrated into the fabric of society, they create new vulnerabilities that can be exploited by cyber adversaries. For example, the proliferation of IoT devices in critical infrastructure has expanded the attack surface for cyberattacks, making it easier for malicious actors to gain access to sensitive systems, including those vital to national security [17].

Especially, AI poses a significant dual-use dilemma in cybersecurity. On one hand, it offers the potential to enhance defensive capabilities by improving threat detection and automating responses to cyber incidents [18]. AI-driven systems analyse network traffic and user behaviour, identifying anomalies that may indicate a breach. These systems can autonomously respond by isolating compromised systems, preventing further damage, and acting as autonomous response tools without requiring human intervention [19]. In the defence sector, AI has been applied to detect malware more effectively by analysing large datasets and recognising patterns indicative of cyber threats. NATO, for example, has made significant investments in AI-powered cybersecurity systems, enabling them to predict and block cyber intrusions pre-emptively, especially in the face of zero-day attacks that exploit previously unknown vulnerabilities [20].

However, while AI has enhanced cybersecurity defences, it has also been weaponised by adversaries to launch more sophisticated attacks that evade traditional defence mechanisms [18]. AI-powered malware hides malicious code within legitimate applications and only triggers when certain conditions, such as facial recognition, are met. This targeted and highly evasive nature makes it difficult to detect using conventional defences, posing a significant challenge for cybersecurity professionals [21]. Moreover, AI is increasingly being utilised by cybercriminals to orchestrate more sophisticated phishing attacks. By analysing data from social media, emails, and other online activities, AI can generate highly personalised phishing messages that are much harder to distinguish from legitimate communication.

In addition to these AI threats, the emergence of quantum computing presents another significant challenge to cybersecurity. Quantum computing promises to exponentially increase computational power, potentially rendering current cryptographic systems obsolete. While still in its developmental stages, the race to achieve quantum supremacy is raising concerns about the future security of data and communications. Many nations are now investing heavily in quantum-resistant cryptography to mitigate these risks, recognising that cybersecurity will become even more crucial as we enter the quantum era [22].

The dual-use nature of emerging technologies complicates efforts to secure national digital infrastructures. As adversaries continue to adapt and exploit these new capabilities, both civilian and military sectors must remain vigilant and invest in advanced defence technologies to stay ahead in the cybersecurity arms race.

Consequently, the rising importance of cybersecurity within national security frameworks reflects broader trends in global politics and technology. As the digitalisation of critical infrastructure and state functions continues, the cyber domain will increasingly define the contours of national security threats. State and non-state actors alike are capitalising on the vulnerabilities inherent in digital systems, and the militarisation of cyberspace further heightens the urgency of establishing robust cybersecurity measures.

Ultimately, cybersecurity is no longer a peripheral concern; it is central to the protection of national sovereignty, the integrity of critical infrastructure, and the stability of political systems. Governments must, therefore, prioritise the development of integrated cybersecurity strategies that involve, at their core, international cooperation, to navigate the complex threat landscape of the 21st century. The increasing importance of cybersecurity within national security frameworks has not only reshaped national strategies, as seen in Romania's evolving approach, but has also demanded greater coordination at the supranational level. The European Union, recognising the interconnectedness of digital infrastructure and the complexity of modern cyber threats, has taken steps to harmonise civilian and defence cybersecurity efforts across member states. As cyber threats grow in scope and sophistication, the need for an integrated approach that leverages both civilian and defence capabilities becomes ever more pressing.

3. The E.U.'s Strategic Imperative for Cyber Resilience and Sovereignty

The European Union has emerged as a global leader in developing comprehensive cybersecurity frameworks, recognising the increasing complexity and scale of digital threats in the modern era. At the core of the E.U.'s cybersecurity policy lies the strategic imperative to safeguard critical infrastructures and ensure the stability of its interconnected digital economies. This policy framework not only seeks to defend against cyber threats posed by both state and non-state actors but also actively fosters technological innovation and leadership within the digital domain, thereby enhancing the E.U.'s global competitiveness. By promoting resilience across member states, the E.U. aims to mitigate vulnerabilities that adversaries might exploit. Furthermore, the framework is forward-looking, focusing not only on defensive measures but also on cultivating innovation, which is vital for maintaining leadership in the digital sphere and ensuring stability and security in the rapidly evolving cyber landscape.

The complexity of modern cyber threats, which includes espionage, ransomware, and hybrid warfare tactics, necessitates a coordinated response across member states. Promoting stability through cybersecurity measures is essential for safeguarding critical services like transport, energy, health, and finance, all of which are highly interconnected and increasingly dependent on network and information systems. As the number of connected devices is expected to grow exponentially, with a significant portion located in Europe, vulnerabilities to cyberattacks are set to increase dramatically in the near future [23].

Defending against a broad spectrum of cyber threats is vital for the E.U. Cyberattacks have the potential to destabilise economies, disrupt governance, and erode public trust. The malicious targeting of critical infrastructure, such as energy grids and communication networks, represents a major global risk. The internet's decentralised nature, which has allowed it to support exponential increases in traffic, has also left it vulnerable to geopolitical tensions. These tensions, combined with the concentration of essential internet services in the hands of a few private companies, expose the European economy and society to disruptive events that could impact millions. In 2023, approximately 70% of the incidents responded to by cybersecurity teams involved critical infrastructure sectors [24]. This marks a sharp increase in both the scale and frequency of attacks compared to previous years, likely exacerbated by the ongoing geopolitical tensions and digital transformation efforts across Europe.

In this intricate security context, the E.U.'s cybersecurity strategy has been shaped by the increasing frequency of cyberattacks on critical sectors and growing geopolitical tensions, which have emphasised the urgent need for a robust and coordinated cybersecurity policy across the Union. The European Commission has recognised that cyber threats transcend national borders, making cooperation among member states essential for safeguarding interconnected digital infrastructures [23]. To address these threats, the E.U. has developed a comprehensive cybersecurity strategy that integrates both civilian and defence sectors, but without clearly delineating their roles. This lack of distinction introduces significant challenges, particularly concerning governance, resource allocation, and the differing priorities of each sector. The absence of clear boundaries raises critical questions about coordination, especially regarding the prevention of overlaps in technology development and the avoidance of operational redundancies. These challenges must be managed effectively to ensure that both sectors function efficiently and complement each other in addressing modern cyber threats.

Fostering innovation in cybersecurity is also critical to maintaining the EU's competitiveness. Cybersecurity innovation, driven by cross-border collaboration and investment in research and development, ensures that Europe remains resilient in the face of emerging threats. However, the increasing sophistication of cyberattacks, often combining disinformation campaigns with infrastructure attacks, highlights the need for stronger EU-wide cybersecurity mechanisms.

The shortage of cybersecurity skills within the EU presents another major challenge. Despite the critical nature of cybersecurity, around 291,000 posts for cybersecurity professionals remained unfilled across Europe in 2022, leaving organisations vulnerable to attacks. Additionally, over two-thirds of European companies, particularly SMEs, are considered 'novices' in cybersecurity preparedness, compared to their counterparts in Asia and America. The impact of these shortcomings is significant, with cybersecurity incidents often triggering chain reactions that affect the wider economy and society. Trust in digital tools and services is paramount, and concerns over security continue to deter many Europeans from fully engaging with online services. Reports indicate that nearly two-fifths of EU citizens have experienced security-related problems, and three-fifths feel unequipped to protect themselves against cybercrime [25].

Improving cybersecurity is essential for building trust in digital services, safeguarding privacy, and ensuring the security of personal data. It also underpins the digital transformation of Europe's economy and society, driving benefits such as more flexible workplaces, smarter transport systems, and cleaner energy grids. The EU's new Cybersecurity Strategy for the Digital Decade addresses these concerns and lays out a framework for protecting its people, businesses, and institutions from cyber threats. By fostering a secure and open cyberspace, the EU aims to enhance international cooperation, protect democratic values, and ensure the long-term stability and prosperity of its member states [23].

Moreover, a central objective of the overarching E.U.'s cybersecurity policy is the attainment of digital sovereignty. This concept refers to the E.U.'s capacity to assert control over and safeguard its digital infrastructure, minimising reliance on external actors. By doing so, the E.U. seeks to demonstrate its 'leadership and strategic autonomy in the digital domain'. [36]. Achieving digital sovereignty not only enhances the Union's resilience to external threats but also positions it as a global leader in shaping the future of cybersecurity and technological governance, ensuring that critical infrastructures and data remain under European control. This is crucial for securing critical technologies, data, and infrastructures from third-party interference. Cybersecurity is fundamental in this regard, as it enables the E.U. to safeguard its digital assets while promoting the development of indigenous technological capabilities [26].

The Cybersecurity Act of 2019 is a pivotal step towards achieving digital sovereignty. While strengthening the role of the E.U. Agency for Cybersecurity (ENISA), the Act established a cybersecurity certification framework for ICT products and services, ensuring high standards of security across the Union. This certification framework plays a vital role in ensuring that E.U. member states and businesses adhere to uniform cybersecurity protocols, thus reducing the risk of cyberattacks on critical infrastructures [27].

4. Bridging the Cyber Divide by Integrating Civilian and Defence Sectors in the EU Cybersecurity Strategy

In the European Union’s cybersecurity landscape, the roles of the civilian and defence sectors are distinct yet highly complementary, ensuring a comprehensive approach to tackling both civilian and national security cyber threats. The civilian sector, composed of private companies, public institutions, and critical infrastructure operators, is largely responsible for securing economic and public service infrastructures. Their focus is on ensuring resilience, business continuity, and safeguarding consumer data and privacy. This includes protection against common cyber threats like ransomware, phishing, and data breaches, which are often directed at large businesses and public services, such as hospitals, energy grids, and financial systems. Civilian cybersecurity efforts are typically centred around passive defences, such as firewalls, encryption, and regular vulnerability assessments, aimed at mitigating risks and improving incident response capabilities [27][28].

On the other hand, the defence sector is tasked with protecting national and collective security interests, often involving more advanced and proactive cyber defence measures. This sector not only focuses on defending military infrastructures but also conducts intelligence operations, counters cyber espionage from state actors, and employs offensive cyber capabilities when necessary. As hybrid threats, such as disinformation campaigns and attacks on critical infrastructure, become more prevalent, military cyber defence teams must stay ahead of emerging threats by leveraging cutting-edge technologies like AI and quantum cryptography [23].

Despite the distinct roles of the civilian and defence sectors, there is a growing recognition that synergies between the two are essential for creating a comprehensive cybersecurity framework in the E.U. Threats to critical infrastructure, for instance, have both civilian and national security implications, which require joint efforts for incident response and resilience planning. However, defence remains primarily a national responsibility, closely tied to national sovereignty. This contrasts with the broader vision of a European Defence Union, first championed by the E.U.'s founding figures, remarkably Jean Monnet and Robert Schuman. While their early aspirations included integrating defence policies as part of a politically unified Europe - illustrated by the European Defence Community proposal in 1952 - such a union has yet to fully materialise. Defence continues to be governed predominantly at the national level, with initiatives under the Common Security and Defence Policy (CSDP) representing incremental steps toward, but not fully realising, the collective defence envisioned by these early architects of European unity.

This tension between national sovereignty and collective defence has structurally influenced the relationship between the defence and civilian sectors in the E.U.’s cybersecurity efforts. While the defence sector prioritises the protection of classified information and operates within a framework of secrecy, civilian agencies focus on transparency and broad information-sharing, driven by economic and ethical considerations. These differing approaches present challenges to fostering effective cooperation. Bridging these differences is crucial to developing a more integrated cybersecurity strategy, one that can leverage the strengths of both sectors while addressing the growing complexities of modern cyber threats.

As E.U. policymakers envision a more integrated and resilient security framework, particularly with the guidance of the 2022 E.U. Strategic Compass, which acts as a de facto E.U. Grand Strategy, the need for enhanced cooperation between civilian and defence sectors becomes increasingly vital. The Strategic Compass emphasises the growing necessity to protect the E.U.'s most critical processes, assets, and information, particularly as its institutions are subject to an increasing number of cyberattacks and system intrusion attempts. Strengthening the intelligence picture, ensuring trustworthy communication systems, and streamlining security rules across the Union are central to this vision [29].

A common approach by Member States, E.U. institutions, bodies, and agencies, including CSDP missions and operations, is required to protect information, infrastructure, and communication systems. This will necessitate significant investments in state-of-the-art European technical equipment, infrastructure, and expertise. Building on the E.U. Cybersecurity Strategy, the Strategic Compass calls for the adoption of additional standards and rules on information and cyber security, as well as the protection of both classified and sensitive non-classified information within E.U. institutions. [29] These efforts aim to facilitate more secure exchanges between Member States, while bolstering the common approach to cybersecurity across the Union.

Particularly, the Digital Europe Programme, launched in 2021, aims to strengthen the E.U.'s digital capacities by investing in cybersecurity, artificial intelligence, and high-performance computing. This programme fosters synergy between the civilian and defence sectors by encouraging collaboration on research, development, and innovation in cybersecurity technologies [28]. Notably, it marks the first time in E.U. history that the European Commission has utilised a common budget to finance civil-defence synergy in cybersecurity. For example, the 'Strengthening Synergies in Defence and Civilian Cybersecurity-ECYBRIDGE' project is an ambitious initiative of 17 organisations funded by the E.U. to unify the cybersecurity capabilities of civilian and defence sectors across the E.U. [30].

To build on these synergies, it is essential to extend collaborative efforts to other E.U.-funded programmes such as the Permanent Structured Cooperation (PESCO), the European Defence Fund (EDF), and Horizon Europe. Each of these initiatives offers unique opportunities to strengthen the integration between the civilian and defence sectors. PESCO, for instance, encourages deeper defence cooperation among E.U. member states, facilitating joint projects and the development of shared capabilities. By aligning PESCO projects with cybersecurity initiatives, the E.U. can enhance its collective defence posture while addressing cyber threats that may compromise military operations and infrastructures [31]. Similarly, EDF focuses on fostering innovation and collaboration in defence research and development. By integrating cybersecurity advancements into EDF projects, the E.U. can ensure that both civilian and military domains benefit from cutting-edge technologies, reinforcing overall cyber resilience [32].

Additionally, Horizon Europe, the E.U.'s flagship research and innovation programme, supports the development of new technologies and solutions across multiple sectors. Leveraging Horizon Europe's resources for cybersecurity research can drive innovation and the creation of robust cybersecurity tools, enabling the civilian and defence sectors to adapt to evolving threats [33].

By strategically combining the strengths of these programmes, the E.U. can create a more cohesive and comprehensive approach to cybersecurity, ensuring that its digital infrastructure, economic interests, and national security are well protected against a wide range of cyber threats.

5. A Systematic Approach for Strengthening Civilian-Defence Cybersecurity Synergy

A systematic approach to strengthening the synergy between civilian and defence sectors within the E.U.'s cybersecurity framework has become a strategic necessity in the face of evolving digital threats. For member states, this integration is critical to address the complex and multifaceted nature of modern cyber threats, ranging from ransomware and data breaches to state-sponsored attacks and hybrid warfare tactics. Effective collaboration between civilian and defence entities is essential for a robust, coordinated response capable of addressing both conventional and emerging threats, ensuring the security and resilience of national and collective E.U. interests.

The rationale for greater integration is rooted in the interconnected nature of modern society's digital infrastructure, where disruptions can have cascading effects across vital sectors. Civilian entities, such as private companies and critical infrastructure operators, typically act as the first line of defence against these threats. However, their efforts could be significantly enhanced by the technological capabilities, strategic intelligence, and resources that defence sectors bring to the table. Research has shown that such integration leads to more cohesive and adaptable defences, reducing the chances of system vulnerabilities being exploited by adversaries.

Traditionally, the defence sector has borne the responsibility of safeguarding national security, focusing on preventing hostile actions against the state, including cyber espionage and cyberattacks from state actors. In contrast, civilian agencies have concentrated on protecting data privacy, ensuring business continuity, and maintaining public trust. However, the lines between these domains have blurred significantly, as evidenced by incidents where state-sponsored attacks have targeted civilian infrastructure, creating widespread disruption and undermining public confidence [34]. This convergence underscores the need for a comprehensive approach that integrates the strengths of both sectors, fortifying the E.U.'s overall cybersecurity posture.

One of the primary obstacles to achieving effective integration between the civilian and defence sectors is the difference in operational cultures. The defence sector traditionally operates under strict protocols of secrecy, which often restricts information-sharing and can hinder collaboration with civilian entities that prioritise open communication and cooperation. Additionally, the regulatory and legal frameworks governing the civilian and defence sectors vary significantly, complicating efforts to establish cohesive guidelines for technological and operational cooperation without compromising national security imperatives. Creating a regulatory environment that fosters cooperation between these sectors requires nuanced policy development that acknowledges their distinct yet complementary roles.

From a political perspective within the E.U., coordinated policy efforts are essential to bridge these divides. Member states must work towards creating a regulatory framework that facilitates cooperation between civilian and defence sectors while respecting their distinct responsibilities. According to the European Commission, harmonised strategies can lead to better risk management and incident response, reducing vulnerabilities across the Union's digital landscape [24]. Furthermore, shared policy frameworks enable faster information-sharing and joint operations, which are essential for responding to cross-border cyber incidents. A unified policy approach allows for more efficient resource allocation and streamlined communication channels, thereby enhancing collective security. Improved coordination among E.U. member states can significantly reduce response times during incidents, ensuring a quicker and more effective counter to cyberattacks. A fragmented policy landscape, however, can lead to disjointed efforts, ultimately weakening collective defence measures across the E.U. [35].

Resource allocation remains a critical challenge in bridging the gap between civilian and defence cybersecurity capabilities. Civilian agencies frequently struggle with budget constraints that limit their ability to invest in advanced cybersecurity technologies and maintain robust defences against sophisticated threats. Conversely, the defence sector, while generally well-resourced, may lack the agility and innovation-driven culture typical of the civilian tech industry. Strategic investment and funding mechanisms, such as the European Defence Fund and Horizon Europe, are crucial in addressing these disparities by supporting joint projects that leverage dual-use technologies applicable to both civilian and military contexts. Pooling resources and adopting shared funding initiatives can lead to more efficient use of technology and expertise, thereby enhancing the E.U.’s overall resilience against cyber threats. Furthermore, sustainable funding models are vital for the success of long-term cybersecurity projects; reliance on short-term funding can create vulnerabilities, leading to gaps in capability and preparedness that adversaries may exploit. Consistent and strategic financial backing is essential for developing enduring cybersecurity frameworks that can adapt to evolving threats.

Table 1. Detailed Key Challenges and Strategic Solutions for E.U. Civilian-Defence Cybersecurity Integration

Key Challenges	**Strategic Approach**	**Implementation Mechanism**	**Necessary Resources**
Fragmented civilian - defence policy frameworks	Develop cohesive E.U.-wide policy frameworks	Introduce civilian-defence synergistic policy initiatives under the E.U. Cybersecurity Strategy and Strategic Compass	Policy expertise, coordination across member states, funding for policy integration
Differences in operational cultures	Foster cross-sectoral collaboration through training and joint exercises	Create joint training programmes funded by Horizon Europe	Funding for joint exercises, trainers, facilities for simulation-based training
Resource allocation disparities	Implement strategic funding allocation for joint projects	Leverage European Defence Fund and Horizon Europe to support innovation	Financial backing from E.U. funds, investment in R&D, public-private partnerships
Regulatory inconsistencies	Harmonise regulations across civilian and defence sectors	Adopt E.U.-level directives and guidelines to standardise legal frameworks	Legal expertise, regulatory bodies, E.U. legislative support
Information-sharing barriers	Establish secure and standardised information-sharing protocols	Develop interoperable platforms and secure channels for data exchange	Secure communication technologies, cybersecurity standards, monitoring tools
Skills gap in cybersecurity workforce	Enhance education and training to build a versatile workforce	Collaborate with academic institutions for skill development programmes	Partnerships with universities, funding for scholarships and training, access to experts
Integration of emerging technologies	Promote ethical investment in dual-use technologies	Establish research partnerships to explore and deploy emerging tech solutions	Research grants, ethical guidelines, collaboration with tech firms and labs

To address these challenges (see the Table 1) member states should prioritise the establishment of unified command structures that bring together representatives from both civilian and defence sectors. Such entities could oversee the coordination of joint exercises, the sharing of intelligence, and the development of integrated response strategies to cyber incidents. This approach requires national and E.U.-level commitment to ensure consistency and avoid jurisdictional conflicts. Moreover, addressing the skills gap across the E.U. is imperative. Member states should implement cross-sectoral training programmes that include both civilian and military cybersecurity experts, building a workforce capable of handling complex cyber threats. Simulation-based exercises, for example, would prepare both sectors to manage hybrid threats, enhancing situational awareness and response capabilities.

A systematic approach to information-sharing must also be developed. Standardised protocols for sharing information between civilian and defence entities are essential to ensure a swift and coordinated response to cyber incidents. The NIS Directive has laid an important foundation in this regard, mandating cooperation among national cybersecurity agencies. However, further efforts are needed to streamline these protocols across sectors and member states, reducing response times and mitigating the impact of attacks.

Emerging technologies such as AI, machine learning, and quantum computing are reshaping the cybersecurity landscape, offering advanced tools for threat detection, prediction, and mitigation that can benefit both civilian and defence sectors. For example, AI-powered algorithms can process large datasets to identify patterns indicative of a cyber threat, enabling proactive measures before an attack is executed. Similarly, quantum cryptography promises unprecedented encryption capabilities, crucial for securing military and civilian communications. By investing in the development and deployment of these technologies, member states can strengthen their cybersecurity capabilities across sectors. However, it is crucial that these investments are underpinned by policies that ensure the ethical use of emerging technologies and prevent their misuse for malicious purposes.

6. Conclusions

In the contemporary intricate security environment, the integration of civilian and defence sectors within the E.U.'s cybersecurity framework has emerged as a strategic imperative due to the increasingly complex and evolving nature of digital threats. This paper has argued that a systematic approach to strengthening civilian-defence cybersecurity synergy is crucial for effectively addressing both conventional and emerging threats, thereby ensuring the security and resilience of national and collective E.U. interests. The rationale for this integration is grounded in the interconnectedness of modern digital infrastructures, where disruptions can trigger cascading effects across multiple sectors, affecting both civilian and national security dimensions.

One of the primary findings of this research is the necessity for coordinated policy efforts across E.U. member states. Fragmented national policies and regulatory inconsistencies can lead to inefficiencies, creating exploitable gaps in defence measures. Harmonising policy frameworks, as exemplified by initiatives such as the E.U. Cybersecurity Strategy and the E.U. Strategic Compass, is critical to fostering cooperation between civilian and defence entities. Such coordinated efforts allow for more efficient resource allocation, streamlined communication, and improved incident response, thereby enhancing the overall security posture of the E.U.

This paper has also highlighted the significant challenges posed by differences in operational cultures between civilian and defence sectors. While the defence sector often operates under strict protocols of secrecy, the civilian sector prioritises transparency and open communication. Bridging this divide requires not only regulatory harmonisation but also the establishment of joint training programmes and unified command structures. These mechanisms can facilitate better cooperation, information-sharing, and the development of integrated response strategies that leverage the strengths of both sectors.

Resource allocation remains a critical challenge. Civilian agencies often face budget constraints that limit their ability to adopt cutting-edge technologies, while the defence sector, despite having more resources, may lack the innovation-driven approach typical of civilian tech industries. Strategic funding through mechanisms such as the European Defence Fund and Horizon Europe can address these disparities by supporting joint projects that utilise dual-use technologies. Effective investment strategies, coupled with sustainable funding models, are essential for building enduring cybersecurity frameworks capable of adapting to the dynamic threat landscape.

Additionally, the importance of addressing the skills gap within the E.U.'s cybersecurity workforce cannot be understated. The development of cross-sectoral training programmes, in collaboration with academic institutions, will help build a versatile workforce equipped to handle complex cyber threats. Moreover, the integration of emerging technologies, including AI, machine learning, and quantum computing, offers new opportunities for enhancing cybersecurity capabilities across both civilian and defence domains. However, ethical considerations must guide the investment and deployment of these technologies to prevent misuse.

Overall, this paper underscores that achieving a robust and integrated cybersecurity framework requires a holistic approach that considers policy, regulatory, financial, and technological dimensions. Member states must work collectively to address these challenges, drawing on both national and E.U.-level initiatives to create a cohesive and resilient cybersecurity ecosystem. Strengthening civilian-defence synergy will not only bolster the E.U.'s defensive capabilities but also reinforce its position as a global leader in cybersecurity innovation, safeguarding digital infrastructure, economic interests, and national security against a broad spectrum of cyber threats.

Future research could explore more in-depth case studies of successful civilian-defence integration within the E.U. and assess the long-term effectiveness of current policy frameworks. Such studies would contribute to understanding the practical implications of the strategic approaches discussed in this paper and provide further insights into optimising the E.U.'s cybersecurity resilience.

References

[1]. S. Walt, "The Origins of Alliances," Cornell University Press, 1987.

[2]. A. Wolfers, "National Security as an Ambiguous Symbol," Political Science Quarterly, vol. 67, no. 4, 1952, pp. 481-502

[3]. J. Mearsheimer, The Tragedy of Great Power Politics, New York: W.W. Norton, 2001.

[4]. B. Buzan, People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era, 2nd ed., Hertfordshire: Harvester Wheatsheaf, 1991.

[5]. L. Kello, The Virtual Weapon and International Order, New Haven: Yale University Press, 2017.

[6]. J. Nye, "Cyber Power," Harvard Kennedy School Belfer Center for Science and International Affairs, 2011.

[7]. Romania National Security Strategy, 2010.

[8]. Romania National Defence Strategy, 2020-2024.

[9]. NATO, "NATO Recognizes Cyberspace as a Domain of Operations," 2016.

[10]. DiCicco, Jonathan M., and Tudor A. Onea. "Great-Power Competition." *Oxford Research Encyclopedia of International Studies.* 31 Jan. 2023; Accessed 14 Oct. 2024.

[11]. P.W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford: Oxford University Press, 2014.

[12]. Thomas F. Lynch III, Introduction, In National Defense University, "Strategic Assessment 2020: Into a New Era of Great Power Competition," National Defense University Press, Washington, D.C., 2020. [Online]. Available: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2404286/1-introduction/. [Accessed: 13-Oct-2024].

[13]. F. G. Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars," Potomac Institute for Policy Studies, Arlington, VA, USA, 2007.

[14]. S. Reeves, "Hybrid Warfare: The Changing Character of Conflict and the Implications for International Humanitarian Law," *International Law Studies*, vol. 95, 2019, pp. 323-358.

[15]. R. Connolly, *Russia's Response to Sanctions: How Western Economic Sanctions Reshape Domestic Politics in Russia*, Cambridge: Cambridge University Press, 2018.

[16]. J.A. Lewis, "The Islamic State and Information Technology," in *Cybersecurity and Cyberwarfare: What Everyone Needs to Know*, 2020, pp. 141-155.

[17]. D. Wright, *Cybersecurity in the Internet of Things*, Cham: Springer International Publishing, 2019.

[18]. M. Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," 2018.

[19]. *Darktrace*, "Autonomous Response: AI Cyber Defense for Real-Time Threat Mitigation," Darktrace, 2023. [Online]. Available: https://www.darktrace.com. [Accessed: 14-Oct-2024].

[20]. *NATO CCDCOE*, "Locked Shields: NATO's Annual Cyber Defence Exercise," Cooperative Cyber Defence Centre of Excellence, 2023. [Online]. Available: https://ccdcoe.org. [Accessed: 14-Oct-2024].

[21]. *IBM*, “DeepLocker: How AI Can Power a Stealthy New Breed of Malware,” IBM Research Blog, Aug. 2018. [Online]. Available: https://www.ibm.com/blogs/research/2018/08/deeplocker/. [Accessed: 14-Oct-2024].

[22]. *National Institute of Standards and Technology*, “Post-Quantum Cryptography: NIST's Efforts to Secure the Future,” NIST, 2022. [Online]. Available: https://www.nist.gov/news-events/news/2022/post-quantum-cryptography. [Accessed: 14-Oct-2024].

[23]. *European Commission*, "The EU’s Cybersecurity Strategy for the Digital Decade," 2020.

[24]. *European Union Agency for Cybersecurity (ENISA)*, "ENISA Threat Landscape 2023," 2023.

[25]. *Eurostat*, "Cybersecurity and Trust in the Digital Economy," 2021.

[26]. A. Kaspersen, "Digital Sovereignty and Europe’s Role in Global Cybersecurity," *J. Eur. Cybersecurity Stud.*, vol. 5, no. 2, pp. 23-34, 2020.

[27]. *European Union Agency for Cybersecurity (ENISA)*, "The Cybersecurity Act", 2019.

[28]. *European Commission*, "Digital Europe Programme: A New Era of Cybersecurity", 2021.

[29]. *European Commission*, "A Strategic Compass for Security and Defence", 2022.

[30]. *Maritime Cybersecurity Centre of Excellence*, "ECYBRIDGE Project," [Online]. Available: https://ecybridge.eu/. [Accessed: 14-Oct-2024].

[31]. *European Commission,* "Permanent Structured Cooperation (PESCO)," [Online]. Available: https://www.pesco.europa.eu/. [Accessed: 20-Oct-2024].

[32]. *European Commission,* "European Defence Fund (EDF)," [Online]. Available: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en. [Accessed: 20-Oct-2024].

[33]. *European Research Executive Agency,* "Increased cybersecurity," [Online]. Available: https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/increased-cybersecurity_en. [Accessed: 20-Oct-2024].

[34]. R. Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies*, vol. 35, no. 1, pp. 5-32, 2012.

[35]. J. F. Dunn Cavelty and M. Wenger, "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics," *Contemporary Security Policy*, vol. 41, no. 1, pp. 5-32, 2020.

[36]. *European Parliament*, “Digital sovereignty for Europe,” 2020.

Enhancing Cybersecurity for UAV Systems: Implementing NIS2 Provisions for Safe Drone Deployment in Albania

Vilma TOMCO[1], Klorenta PASHAJ[2]
[1] State Authority for Geospatial Information, Tirana, Albania
vimatster@gmail.com
[2] National Cyber Security Authority, Tirana, Albania
klorenta.pashaj@gmail.com

Abstract

Unmanned Aerial Vehicles (UAVs) have become essential tools in both military and civilian applications, from surveillance to infrastructure monitoring. However, their increased use has raised significant cybersecurity concerns, particularly regarding vulnerabilities to cyberattacks such as GPS spoofing, signal jamming, and data link interception. This paper reviews the key cybersecurity challenges facing UAVs and explores mitigation strategies to enhance UAV security, with a focus on potential applications in Albania. Drawing on recent studies, we examine common attack vectors, including man-in-the-middle (MITM) attacks, denial-of-service (DoS) attacks, and unauthorized data interception. These vulnerabilities pose risks not only to the safe operation of UAVs but also to the integrity of the critical infrastructure they monitor. To address these issues, the paper proposes robust encryption protocols, real-time monitoring systems, and the integration of machine learning-based intrusion detection techniques to safeguard UAV communications and operations. Furthermore, this research highlights the importance of aligning UAV security measures with the EU's NIS2 Directive, offering recommendations on regulatory frameworks tailored to the Albanian context. The findings emphasize the need for a comprehensive approach to UAV cybersecurity, combining technological innovation with stringent regulatory oversight to ensure safe and secure UAV deployment in Albania's rapidly evolving digital landscape.

Index terms: Cybersecurity, GPS spoofing, Intrusion detection, NIS2 Directive, Unmanned Aerial Vehicles (UAVs)

1. Introduction

Unmanned Aerial Vehicles (UAVs), or drones, are gaining widespread use in Albania across sectors such as border surveillance, infrastructure monitoring, and agriculture. Originally developed for military purposes, UAVs are now essential in civilian domains due to their flexibility and cost-effectiveness. However, as UAV deployment grows, so do the associated cybersecurity risks, particularly in critical areas like energy infrastructure inspection and disaster management.

UAVs are vulnerable to a range of cyber threats, including GPS spoofing, signal jamming, and man-in-the-middle attacks, which can compromise their operations. A cyberattack on a UAV system could lead to unauthorized control, service disruption, or data breaches, posing significant risks to national security. Given these challenges, ensuring the security of UAV communication networks and data exchange is crucial for maintaining their integrity and functionality.

The European Union's NIS2 Directive offers a regulatory framework that Albania can align with to strengthen its cybersecurity measures. Although not an EU member, Albania is adapting its cybersecurity policies to meet EU standards, particularly in sectors involving UAV technology. This paper explores how the NIS2 Directive can be applied to enhance UAV cybersecurity in Albania, proposing strategies to safeguard these systems from evolving threats and ensuring their secure deployment in critical sectors.

2. Literature Review

2.1. Overview of Existing Cybersecurity Vulnerabilities in UAVs

The rapid proliferation of Unmanned Aerial Vehicles (UAVs) has created new cybersecurity concerns due to the increasing complexity and connectivity of these systems. UAVs, being cyber-physical systems, operate through interconnected components such as flight controllers, communication links, ground control stations (GCS), and various sensors [1][2]. These systems are prone to cybersecurity vulnerabilities that could be exploited by adversaries. Vulnerabilities in UAV systems can result from weak encryption protocols, unsecured data transmission, and inadequate protection of communication channels (Hartmann & Giles, 2016). These issues are especially problematic in civilian and commercial drones, where security mechanisms are often less robust than in military-grade UAVs [2].

One critical vulnerability lies in the GPS systems that most UAVs rely on for navigation. GPS signals are inherently weak and unencrypted, making them susceptible to spoofing and jamming attacks, which can cause UAVs to lose their way or be redirected by malicious actors [2][3]. Additionally, unencrypted communication links between the UAV and the GCS can expose UAVs to man-in-the-middle (MITM) attacks, where adversaries intercept and manipulate data [2].

Several studies have classified the common cyberattack vectors targeting UAV systems. The most prevalent among these include GPS spoofing, signal jamming, and man-in-the-middle attacks.

2.2. Cybersecurity Threats to UAVs

UAVs, being cyber-physical systems, are highly vulnerable to a variety of cybersecurity threats due to their reliance on real-time communication, navigation systems, and data exchange protocols. These threats can be categorized into several types, each targeting a different component of UAV operations.

GPS Attacks: One of the most common threats to UAVs is GPS-based attacks, which can include GPS spoofing and jamming. In a GPS spoofing attack, the UAV’s navigation system is deceived by broadcasting fake GPS signals, causing the drone to follow incorrect coordinates, potentially leading to crashes or unauthorized redirection. GPS jamming disrupts the communication between the UAV and GPS satellites by overwhelming the signal with noise, making it difficult or impossible for the UAV to navigate properly [2][1]. Since many UAVs rely on GPS for autonomous flight, attacks on these systems pose a significant risk to their operations.

Signal Jamming: UAVs depend on continuous communication with ground control stations (GCS) for command-and-control functions. Signal jamming involves the intentional disruption of these communication links, rendering the UAV unable to receive commands or transmit data back to the control station [3]. This type of attack can lead to loss of control, forcing the UAV into an unplanned landing or causing it to crash. In critical missions, such as search and rescue operations or infrastructure inspections, signal jamming could result in mission failure with potentially life-threatening consequences [2].

Data Interception and Man-in-the-Middle (MITM) Attacks: UAVs frequently transmit sensitive data, including real-time video feeds and telemetry information. In a data interception attack, adversaries capture these data transmissions, potentially gaining access to critical information such as live video feeds or flight paths [2]. MITM attacks occur when an attacker intercepts and manipulates the communication between the UAV and its ground station [2][3]. These attacks can result in the unauthorized control of the UAV, allowing the attacker to issue commands, steal data, or even crash the drone.

Firmware Exploits: Firmware is responsible for the core functions of UAVs, including navigation, communication, and sensor data processing. Exploiting vulnerabilities in UAV firmware can allow an attacker to take full control of the drone's operations [2]. This type of attack is particularly dangerous because it can be difficult to detect and can be performed remotely if the firmware is not adequately secured.

3. Risks Posed to UAVs Used in Critical Infrastructure

The use of UAVs in critical infrastructure, such as energy grids, telecommunications networks, and border surveillance, has increased in recent years due to their efficiency in performing tasks like real-time monitoring, inspection, and data collection. However, the integration of UAVs into these vital sectors introduces substantial cybersecurity risks.

In critical infrastructure, UAVs perform missions where the reliability and security of their operations are paramount. For instance, UAVs are used to inspect power lines, monitor oil pipelines, and survey large areas of land for environmental protection. Any disruption caused by a cyberattack on these UAVs could lead to severe consequences. GPS spoofing or jamming during an infrastructure inspection could cause the UAV to fail in detecting faults in power grids or pipelines, resulting in undetected malfunctions that could escalate into widespread service outages [3]. Similarly, signal jamming during border surveillance could prevent UAVs from transmitting critical data on illegal activities, thereby compromising national security [2].

Moreover, data interception in UAVs used for infrastructure monitoring could lead to unauthorized access to sensitive information, such as energy usage patterns or vulnerabilities in physical infrastructure. This could give adversaries the information needed to carry out further attacks, such as targeting power stations or other key facilities [3]. The hijacking of UAVs used for critical infrastructure monitoring could also allow attackers to steal or destroy equipment, further disrupting services.

3.1. Real-World Incidents and Case Studies Relevant to These Threats

Several real-world incidents demonstrate the severity of cybersecurity threats to UAVs. One notable case occurred in 2011, when Iranian forces reportedly used GPS spoofing to capture a U.S. military UAV, the RQ-170 Sentinel, by tricking it into landing in hostile territory [2]. This incident highlights the vulnerability of even military-grade UAVs to GPS-based attacks and underscores the importance of securing navigation systems.

Another incident occurred in the United Kingdom, where signal jamming disrupted the operations of commercial UAVs used for surveying during the construction of a railway. The jamming not only caused delays in the project but also posed safety risks, as the UAVs lost communication with their operators and became uncontrollable [3]. This case illustrates how jamming attacks can affect UAV operations in civilian contexts, leading to both operational and safety concerns.

In a more recent example, researchers demonstrated the possibility of MITM attacks on civilian UAVs by intercepting and manipulating the communication between a drone and its controller [2]. The attackers were able to take control of the drone, alter its flight path, and access the video feed without the operator's knowledge. This case study exemplifies the growing threat of data interception and manipulation in the civilian UAV market, where encryption and secure communication protocols are often not as robust as in military applications.

These incidents highlight the pressing need for stronger cybersecurity measures in UAV systems, particularly in critical infrastructure and sensitive operations. The vulnerabilities exposed by these real-world attacks emphasize that UAV cybersecurity should be a top priority for both regulatory bodies and UAV operators. As Albania and neighboring countries increase their reliance on UAV technology in critical sectors, addressing these threats through effective mitigation strategies becomes essential to ensure the security and resilience of UAV operations.

3.2. Mitigation Strategies

To address these vulnerabilities, researchers have proposed several mitigation strategies aimed at strengthening UAV cybersecurity. Some of the key measures include:

Encryption Protocols: One of the most widely recommended solutions for enhancing UAV security is the implementation of strong encryption protocols for both GPS signals and communication links. By encrypting these data streams, attackers are less likely to intercept and manipulate critical information [1][2]. For instance, military-grade UAVs often use encrypted GPS signals to protect against spoofing, a practice that could be extended to civilian UAVs operating in sensitive areas.

Real-Time Monitoring and Intrusion Detection Systems (IDS): Advanced real-time monitoring systems combined with machine learning-based intrusion detection systems (IDS) have been proposed as effective ways to detect abnormal activities in UAV operations. These systems can monitor UAV behavior in real-time, flagging any deviations from expected patterns that may indicate an ongoing attack [2][3]. Implementing IDS in critical sectors where UAVs are used, such as border surveillance and infrastructure monitoring, can provide an early warning against cyber threats.

Resilient Communication Protocols: Some researchers have explored the use of resilient communication protocols, such as Frequency Hopping Spread Spectrum (FHSS), to defend against jamming and MITM attacks. FHSS changes the communication frequency rapidly, making it difficult for adversaries to jam the signal or intercept data [2][3]. Additionally, fail-safe mechanisms such as autonomous return-to-home functions can mitigate the impact of communication loss [1].

Authentication and Access Control: Strengthening authentication mechanisms for UAV systems, particularly for civilian and commercial drones, has been highlighted as a key strategy in the literature. Multifactor authentication, as well as cryptographic keys for UAV operators, can significantly reduce the likelihood of unauthorized access [3].

As UAVs become integral to critical infrastructure and civilian applications, the need for robust cybersecurity measures grows exponentially. The complexities of UAV systems, combined with their vulnerability to cyberattacks, have prompted the development of multiple mitigation strategies aimed at securing their operation. This section outlines key strategies, including encryption protocols, real-time monitoring, machine learning-based threat detection, incident response mechanisms, and UAV-specific cybersecurity frameworks and best practices.

Encryption Protocols and Secure Communication Techniques

One of the most critical defense mechanisms against cyberattacks on UAVs is the implementation of strong encryption protocols. These protocols ensure that communication between UAVs and their ground control stations (GCS) is secure, protecting data from interception and unauthorized access. End-to-end encryption of data transmission is vital in preventing man-in-the-middle (MITM) attacks, where attackers intercept and manipulate communication between UAVs and operators [1][2]. Encryption ensures that even if an attacker intercepts the communication, the data remains unreadable without the appropriate decryption key.

For GPS systems, which are prone to spoofing attacks, the use of cryptographically secure GPS signals can provide additional protection. While such encryption is more commonly used in military applications, extending its use to civilian and commercial UAVs operating in critical sectors could significantly reduce the risk of GPS spoofing [2]. Additionally, secure communication techniques such as Frequency Hopping Spread Spectrum (FHSS) can help mitigate signal jamming by changing the communication frequency at rapid intervals, making it difficult for attackers to jam the signal [3].

The integration of Public Key Infrastructure (PKI) in UAV communication channels can further strengthen authentication mechanisms. PKI ensures that only authorized operators can access and control UAV systems, using cryptographic keys to verify the identity of both the UAV and the operator [3].

Real-Time Monitoring and Machine Learning for Threat Detection

The dynamic nature of UAV operations requires continuous monitoring to detect potential security breaches in real time. Advanced Intrusion Detection Systems (IDS), when integrated with UAV systems, can provide real-time threat detection by monitoring communication patterns, flight data, and system behavior for anomalies. IDS systems are particularly effective when combined with machine learning (ML) algorithms, which can learn from historical data and improve their ability to detect suspicious activities over time [2].

Machine learning-based threat detection has the advantage of being adaptive and responsive to evolving attack methods. ML algorithms can analyze vast amounts of data generated by UAV operations, identifying deviations from expected behavior that may signal a cyberattack. For instance, if a UAV's flight path is suddenly altered without input from the operator, or if communication latency increases unexpectedly, the IDS can flag these events as potential threats [2][3]. Such systems can also predict future vulnerabilities by analyzing patterns from previous attacks, allowing for preemptive countermeasures to be implemented.

Moreover, UAV systems equipped with real-time monitoring can automate certain security responses, such as switching communication channels in case of jamming or initiating a return-to-home sequence if a security breach is detected [4]. These proactive defense mechanisms minimize the time between detecting an attack and responding to it, reducing the potential damage.

Incident Response Strategies for Compromised UAVs

Given the critical functions that UAVs perform, especially in sectors like energy, telecommunications, and border security, having a well-structured incident response strategy is essential. Incident response for UAVs involves not only addressing immediate threats but also ensuring the continuity of operations with minimal disruption.

In the event of a cyberattack, such as a signal jamming or a MITM attack, the UAV must be equipped with predefined fail-safe mechanisms. For example, many UAVs are designed with an autonomous return-to-home function that activates when communication with the ground station is lost [1]. This mechanism ensures that the UAV returns to a designated safe location rather than being lost or hijacked. Furthermore, UAVs should have redundant communication channels, allowing operators to regain control if the primary communication link is compromised [3].

In the case of a more severe compromise, such as a successful MITM attack where the UAV has been hijacked, it is essential to have an immediate shutdown protocol. This would involve remotely disabling the UAV to prevent the attacker from using it for malicious purposes. Additionally, a robust forensic analysis should be carried out post-incident to determine the nature of the attack, assess damage, and implement corrective measures to prevent future breaches [2].

Incident recovery should also include a comprehensive review of the security protocols and systems in place, ensuring that any vulnerabilities are patched before the UAV is redeployed. Continuous updates to the UAV’s firmware and software are crucial in mitigating known vulnerabilities [2].

4. UAV-Specific Cybersecurity Frameworks and Best Practices

The increasing reliance on UAVs in critical infrastructure necessitates the development of UAV-specific cybersecurity frameworks. These frameworks provide a structured approach to UAV security, covering all aspects of their operation, from pre-flight to post-flight procedures. A comprehensive UAV cybersecurity framework should include guidelines on secure system design, regular maintenance, and operational best practices.

One of the primary components of such a framework is the enforcement of cyber hygiene practices for UAV operators. This includes ensuring that UAVs operate on updated software, that encryption keys are regularly rotated, and that strict access control measures are implemented [3]. Security audits should also be a routine part of UAV operations, with periodic checks to ensure compliance with security standards and regulations.

In line with the European Union's NIS2 Directive, the framework should include specific requirements for cyber resilience, ensuring that UAVs used in critical infrastructure can withstand and recover from cyberattacks. NIS2 provisions advocate for risk assessments, incident reporting mechanisms, and cross-border collaboration in cybersecurity [3]. By aligning with these standards, Albania and neighboring regions can ensure that UAV operations are secure and resilient against evolving threats.

The NIS2 Directive (Network and Information Systems Directive 2), introduced by the European Union, is a regulatory framework aimed at strengthening cybersecurity across critical sectors, including energy, transport, healthcare, and digital infrastructure. It builds on the original NIS Directive, placing greater emphasis on risk management, incident reporting, and cross-border cooperation. NIS2 requires entities in critical sectors to adopt stringent cybersecurity measures, conduct regular risk assessments, and ensure robust incident response mechanisms [3].

Finally, collaborative efforts between government agencies, private industry, and international bodies are critical in developing and enforcing these cybersecurity standards. Sharing threat intelligence, best practices, and new technologies can enhance the overall security of UAV operations across borders [3]. As UAV usage grows, especially in sensitive sectors, the implementation of these frameworks and best practices will be crucial in safeguarding operations and ensuring the security of critical infrastructure.

Current Adoption of UAVs in Albania and Neighboring Regions

In Albania, the adoption of UAVs has increased significantly, particularly in areas such as environmental monitoring, border security, and critical infrastructure inspections [2][1]. These UAVs are often used by government agencies, private companies, and research institutions to monitor large areas that would otherwise be difficult to reach. For instance, UAVs play an important role in surveillance missions along Albania's extensive coastal borders, aiding law enforcement in detecting illegal activities such as smuggling [2].

However, the increasing reliance on UAV technology brings with it the growing concern of cybersecurity threats, especially in sectors such as energy infrastructure and border control, where drones play a critical role [3]. Neighboring regions, such as Kosovo and North Macedonia, have similarly adopted UAV technologies in various sectors. As a result, Albania and its neighbors face shared challenges in securing UAV operations, especially given the regional focus on enhancing critical infrastructure protection under EU directives such as NIS2[3]. Albania's increasing integration with EU cybersecurity frameworks, including NIS2 provisions, presents an opportunity to build a robust cybersecurity posture for UAV systems, ensuring their secure deployment across key sectors.

After 50 years of communism, Albania has made substantial strides in building a multi-party democracy, establishing a market economy, and strengthening the rule of law. From 1990 to 2022, the country has seen steady economic growth, with an average annual growth rate of 3.8%. Under the 2021-2025 Governing Program, the Albanian Government has committed to accelerating the country's EU integration process. A key development area in the 2021-2024 program is the creation of a "Digital Society" aimed at modernizing electronic systems in various sectors, including geospatial information, to enhance services for citizens and businesses. The Albanian Government has identified ICT infrastructure modernization as a priority over the last 12 years, and one of the steps taken in this direction was the establishment of the National Spatial Data Infrastructure (NSDI) under Law 72/2012. This law established the State Authority for Geospatial Information (ASIG) as the NSDI Administrator and National Mapping Authority for Albania. In 2020, the Government approved the "Geospatial Information Governance Policy for Albania, 2020-2030," recognizing ASIG's central role in managing the geoinformation system in Albania.

4.1. Remote Sensing Project

One of the core measures in this policy document is the increased use of Remote Sensing technology by government agencies to monitor and accurately plan territorial development. ASIG has been designated as the authority responsible for establishing the Remote Sensing Monitoring Center, which will handle processing, analyzing, and disseminating geospatial data generated by national remote sensing projects. Currently, two important projects are underway:

1. Satellite Service for Territorial Monitoring

This project uses advanced satellite technology to monitor Albania and is expected to continue until 2025. The Government of Albania has contracted Satellogic, an American company, to provide exclusive operational satellite services for three years. These satellites will capture multispectral stereoscopic imagery at 70 cm resolution and hyperspectral imagery at 25 m resolution. ASIG's Remote Sensing Monitoring Center will process this data into geospatial products such as orthoimagery, digital elevation models, and thematic maps, which will support local and central government authorities in:

- Emergency response to natural disasters
- Urban development and monitoring
- Environmental protection
- Tourism development
- Agriculture

2. Purchase of UAV Drones

Albania has also acquired a fleet of UAVs (Unmanned Aerial Vehicles) through a strategic partnership with Turkey, as part of the modernization efforts of Albania's Armed Forces within NATO. Besides national security applications, the UAV project will also serve civilian monitoring needs. ASIG contributed to the technical specifications and will receive an aerial photogrammetric camera with a resolution of 4 cm/pixel, mounted on the UAV, to capture high-resolution imagery. Like the satellite data, these UAV images will be processed by ASIG to produce high-accuracy geospatial data, such as orthoimagery and digital terrain models. This data can also be used for producing topographical base maps, thanks to expertise gained from a previous JICA-supported project, "Geospatial Information for Sustainable Land Development in the Tirana-Durres Zone" (2017-2019). Combined with satellite data, this imagery will support:

- Detailed urban planning
- Engineering projects
- Enhancing the Land Information System

Albania is also focusing on strategic satellite services, including the Albania 1 and Albania 2 satellites, for monitoring, geospatial data processing, and informed decision-making. ASIG, a part of the Copernicus Relay network, actively promotes Copernicus Open Data, highlighting its benefits for local communities and businesses. ASIG is also running campaigns to raise awareness and improve public institutions' capabilities in utilizing satellite services.

Albania's comprehensive geospatial framework, established under Law No. 72/2012 [5], was recently updated by the Parliament on September 19, 2024, to fully align with the EU's INSPIRE Directive (2007/2/EC) [6]. This legislation regulates the creation, management, and use of geospatial data to facilitate effective data sharing among public authorities. The 2020-2030 National Policy on Geospatial Information sets strategic goals to improve access to, use of, and governance of geospatial information across Albania

4.2. How the NIS2 Directive Can Guide UAV Cybersecurity in Albania

Although Albania is not an EU member, it has demonstrated efforts to align with EU cybersecurity frameworks, including the NIS2 Directive [7], as it aspires to join the Union. The NIS2 provisions can serve as a valuable guide for establishing UAV cybersecurity standards in Albania, particularly for UAVs used in critical sectors such as border surveillance and energy infrastructure monitoring [3]. By adopting NIS2's risk management approach, Albania can enforce stricter controls on UAV operations, ensuring that vulnerabilities are addressed proactively, and incidents are reported promptly.

To align with EU standards, Albania should prioritize updating its cybersecurity legislation to incorporate NIS2's key provisions. This includes implementing mandatory risk assessments for UAV operators, requiring incident reporting within specified timeframes, and enforcing penalties for non-compliance. Additionally, Albania should foster cross-border collaboration with neighboring EU countries, sharing best practices and threat intelligence to enhance the resilience of its UAV cybersecurity posture [3].

A secure UAV cybersecurity framework for Albania should include several critical elements:

- Encryption protocols for secure communication between UAVs and ground control systems.
- Intrusion detection systems (IDS) and machine learning-based threat detection for real-time monitoring.
- Incident response strategies, including fail-safe mechanisms like return-to-home and automatic shutdown protocols in case of security breaches [2].
- Periodic security audits to ensure compliance with cybersecurity regulations.

Recommendations for Policy-Makers and Regulatory Bodies

Albanian policy-makers should:

- Mandate risk assessments for UAV operators in critical sectors.
- Establish penalties for non-compliance with cybersecurity standards.
- Encourage the adoption of best practices for UAV cybersecurity, such as strong encryption and secure communication protocols [3].
- Foster public-private partnerships to share threat intelligence and develop industry-specific guidelines.
- Integration of Best Practices and Alignment with the NIS2 Directive

By integrating best practices from the NIS2 Directive, Albania can ensure its UAV operations are secure and resilient. This includes adopting multi-factor authentication for UAV systems, ensuring that UAV operators are adequately trained in cybersecurity protocols, and requiring regular updates to software and firmware to address known vulnerabilities [2] [3].

5. Conclusion and Future Directions

This paper has highlighted the key cybersecurity challenges faced by UAVs, including GPS spoofing, signal jamming, and data interception. Effective mitigation strategies, such as encryption, real-time monitoring, and incident response mechanisms, are critical to ensuring the secure operation of UAVs in Albania. The NIS2 Directive offers a robust framework for guiding UAV cybersecurity, which Albania can leverage as it aligns with EU standards [2][3].

Future challenges for UAV cybersecurity in Albania include keeping pace with evolving threats and integrating emerging technologies like artificial intelligence for autonomous threat detection. Additionally, there is a need for increased investment in cybersecurity infrastructure to support UAV operations in critical sectors. As UAV usage expands, maintaining regulatory compliance and incident reporting will become more complex [3].

International cooperation will play a crucial role in securing UAV systems, as threats are often transnational. Albania should continue to collaborate with EU member states and regional partners to share intelligence, harmonize regulations, and strengthen its cybersecurity ecosystem. Evolving regulatory frameworks, such as the NIS2 Directive, will provide valuable guidance as Albania works to enhance its UAV cybersecurity measures and ensure safe and secure UAV deployment in critical sectors [3].

References

[1]. Costa, D. G., Bittencourt, J. C. N., Oliveira, F., Peixoto, J. P. J., & Jesus, T. C. (2024). Achieving sustainable smart cities through geospatial data-driven approaches. Sustainability, 16(640).

[2]. Dahlman, E., & Lagrelius, K. (2019). A game of drones: Cyber security in UAVs (KTH Bachelor Thesis Report). KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science.

[3]. Hartmann, K., & Giles, K. (2016). UAV exploitation: A new domain for cyber power. In N. Pissanidis, H. Rõigas, & M. Veenendaal (Eds.), 2016 8th International Conference on Cyber Conflict (pp. 205-215). NATO CCD COE Publications

[4]. Sanghavi, P., & Kaur, H. (2023). *A comprehensive study on cyber security in unmanned aerial vehicles*. 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom).

[5]. “Law No. 72 of 28.6.2012.” Accessed: Oct. 21, 2024. [Online]. Available: https://sane27.com/wp-content/uploads/Law-no.72-of-28.6.2012.pdf

[6]. “INSPIRE Directive.” Accessed: Oct. 21, 2024. [Online]. Available: https://knowledge-base.inspire.ec.europa.eu/legislation/inspire-directive_en

[7]. “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).” Accessed: Oct. 21, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

AR-in-a-Box: A Structured 8-Step Framework for Cybersecurity Awareness

Ioan-Cosmin MIHAI
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
cosmin.mihai@academiadepolitie.ro

Abstract

AR-in-a-Box, developed by the European Union Agency for Cybersecurity (ENISA), offers a comprehensive framework to guide organisations in creating effective cybersecurity awareness programs. Through a structured 8-step process, this toolkit helps organisations set objectives, secure resources, manage human capital, segment audiences, select communication tools, plan timelines, implement programs, and evaluate outcomes. This paper explores each step in detail, incorporating state-of-the-art research and real-world case studies to demonstrate AR-in-a-Box's effectiveness in fostering a cybersecurity-conscious culture. Through targeted communication, interactive elements, and performance metrics, AR-in-a-Box enables organisations to embed cybersecurity awareness and improve resilience against evolving cyber threats.

Index terms: AR-in-a-Box, cybersecurity awareness, cybersecurity education, program evaluation, performance metrics

1. Introduction

As cyber threats grow more sophisticated, the human factor in cybersecurity has become a focal point for organisations. Statistics indicate that human error remains a leading cause of security breaches, with issues like phishing and weak passwords contributing significantly to organisational vulnerabilities. ENISA has developed AR-in-a-Box, a structured toolkit designed to help organisations build effective cybersecurity awareness programs tailored to their specific needs.

This paper provides a comprehensive overview of AR-in-a-Box's 8-step framework, encompassing every stage from initial objective setting to program evaluation. By integrating theory and practical application, we illustrate how AR-in-a-Box can enhance security awareness across organisations of varying sizes and sectors. The paper also includes case studies highlighting the framework's flexibility and effectiveness in different contexts.

2. State-of-the-art in cybersecurity awareness

Cybersecurity awareness initiatives are increasingly focused on behavioural change rather than simple knowledge dissemination. Research shows that traditional training models often rely on periodic lectures or policy-based sessions and need more engagement to instil long-term behavioural change. Contemporary approaches incorporate interactive elements such as gamification and personalised messaging, which are proven to enhance user engagement and retention.

Models like the Protection Motivation Theory (PMT) and the Elaboration Likelihood Model (ELM) provide theoretical foundations for effective awareness programs [1]. PMT emphasises that individuals are more likely to adopt protective behaviours if they perceive the threat as severe and believe they can counter it effectively. ELM supports the idea that tailored messaging can lead to deeper processing and acceptance of cybersecurity behaviours [2]. AR-in-a-Box leverages these models by offering a segmented and interactive approach that encourages users to internalise security best practices.

Several frameworks guide cybersecurity awareness. The SANS Security Awareness Maturity Model and ISO/IEC 27001 provide guidelines on cybersecurity training, but they often lack more practical tools for engaging employees or measuring program effectiveness [3, 4]. In contrast, AR-in-a-Box integrates best practices from behavioural science, offering tools like communication strategies, quizzes, and gamified learning modules. Including key performance indicators (KPIs) also makes it a data-driven solution that facilitates continuous improvement.

3. AR-in-a-Box 8-Step Framework

Step 1: Identify Objectives

The first step in AR-in-a-Box is setting clear, SMART objectives that align with the organisation’s cybersecurity goals. This foundational step is essential for defining the program’s direction and measuring its success. Typical objectives include reducing phishing incidents, increasing password hygiene, and fostering cybersecurity awareness. Setting these goals ensures that the program targets specific areas of improvement [5].

Step 2: Secure Financial Resources

Adequate funding is crucial for an effective awareness program. AR-in-a-Box recommends justifying budget requests by highlighting potential financial savings from preventing cyber incidents. Organisations are encouraged to explore cost-effective strategies, such as reusing content or leveraging open-source materials. This approach emphasises that organisations can build impactful awareness programs even with limited budgets by being resourceful [5].

Step 3: Ensure Human Resources

AR-in-a-Box emphasises the importance of a dedicated team to implement and sustain the program. Key roles include cybersecurity officers, PR and communication experts, and IT staff. Each member brings a unique skill set that contributes to the program’s success, from developing content to ensuring technical support and effective message dissemination. This multidisciplinary approach ensures that all aspects of the program, from educational content to technical implementation, are handled effectively [5].

Step 4: Split Employees into Target Groups

Segmenting the audience allows for tailored messaging, ensuring each group receives relevant and understandable information. Employees can be categorised based on job functions, risk levels, and technological familiarity. For example, technical staff may require advanced training on specific security protocols, while general employees benefit from basic cybersecurity hygiene practices. Targeted training is more likely to resonate with employees and foster compliance [5].

Step 5: Choose the Right Means

AR-in-a-Box provides various tools, such as infographics, videos, quizzes, and games, to communicate cybersecurity concepts effectively. The right tools depend on the audience and the message’s complexity. Gamification, for example, has proven effective for engaging users and reinforcing learning. By choosing appropriate means of communication, organisations can create a multifaceted program that caters to diverse learning preferences and maximises engagement [5].

Step 6: Create a Time Plan

A well-defined timeline is essential for maintaining momentum and ensuring program consistency. AR-in-a-Box advises organisations to plan awareness activities in phases, allowing for regular reinforcement and adaptation as new threats emerge. The timeline should include initial training, refresher courses, and periodic assessments. Spacing out learning sessions aligns with educational theories like spaced repetition, which enhances long-term retention [5].

Step 7: Implement the Program

The implementation phase involves launching the program, monitoring initial engagement, and addressing immediate challenges. AR-in-a-Box suggests gathering feedback to make necessary adjustments and improve the program's relevance. This step is critical for translating the planned objectives into actionable awareness activities. Effective implementation requires clear communication and ongoing support to foster a security-conscious environment [5].

Step 8: Evaluate the Program

Evaluating the program's effectiveness is essential for continuous improvement. AR-in-a-Box includes KPIs such as incident reduction rates, quiz scores, and user feedback. Regular evaluations enable organisations to measure progress against objectives, identify areas for improvement, and adjust strategies as needed. By systematically evaluating the program, organisations demonstrate their commitment to cybersecurity and reinforce its importance to employees [5].

4. Implementations of Cybersecurity Awareness Initiatives

The following case studies illustrate how real organisations across different sectors have implemented cybersecurity awareness programs similar in structure and objectives to ENISA's AR-in-a-Box framework. These examples showcase how these organisations have improved cybersecurity awareness and resilience through structured, data-driven approaches.

4.1. UK Healthcare Sector

The UK's National Health Service (NHS) is one of the largest healthcare systems in the world. It has faced significant cybersecurity challenges, especially after the 2017 WannaCry ransomware attack, which affected many NHS facilities. This event prompted NHS Digital, the central organisation responsible for NHS IT services, to implement a comprehensive awareness and training program to strengthen cybersecurity practices across the healthcare system [6].

Following the attack, NHS Digital rolled out a nationwide cybersecurity awareness campaign targeting all levels of healthcare workers, from administrative staff to medical professionals. The initiative included e-learning modules, periodic phishing simulations, and workshops on data protection and secure information handling. Additionally, NHS Digital introduced the "CareCERT" service, which provides cybersecurity alerts, guidance, and resources to NHS organisations.

The NHS saw a marked improvement in cybersecurity awareness, with staff showing increased vigilance in identifying phishing emails and safeguarding patient data. Regular assessments indicated a significant reduction in employees' susceptibility to phishing attempts [7]. This case illustrates how a large, complex healthcare organisation can leverage structured training and real-time updates to foster a security-conscious culture.

While the NHS has made significant strides, sustaining engagement remains challenging in an environment with high staff turnover and varying levels of digital literacy. Continuous refresher training and adaptive content tailored to different professional roles would likely improve long-term results.

4.2. US National Cybersecurity Awareness Month

The US Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA) jointly run the annual "Cybersecurity Awareness Month" every October [8]. Launched in 2004, this initiative aims to raise cybersecurity awareness among American citizens, businesses, and public agencies through a month-long campaign each year.

Cybersecurity Awareness Month promotes various weekly themes, such as phishing prevention, software updates, and multifactor authentication, to engage audiences on critical cybersecurity topics. The campaign employs social media outreach, webinars, educational toolkits, and partnerships with corporations, academic institutions, and non-profit organisations. DHS also collaborates with the Cybersecurity and Infrastructure Security Agency (CISA) to provide updated guidance and resources to individuals and organisations.

Cybersecurity Awareness Month has become widely recognised, with extensive participation from private sector partners and a solid social media presence. Surveys after the campaign show increased public awareness of basic cybersecurity practices, such as using strong passwords and recognising phishing attempts [8] [9]. This case underscores how a targeted, recurring campaign can reinforce cybersecurity behaviours and increase public engagement.

While Cybersecurity Awareness Month has successfully raised awareness, maintaining momentum throughout the year remains challenging. Expanding the campaign’s reach through year-round initiatives and continuous engagement with partners could strengthen its long-term impact.

4.3. Cybersecurity Awareness Initiatives for EU Organisations

ENISA, the European Union Agency for Cybersecurity, has developed cybersecurity awareness initiatives to support EU member states and organisations. ENISA’s "Cybersecurity Awareness Month" and other year-round activities target a broad audience across Europe and aim to instil good cybersecurity practices in both the public and private sectors [10].

ENISA’s awareness initiatives include online training modules, infographics, and interactive quizzes distributed across EU institutions and businesses. Each October, ENISA coordinates cybersecurity awareness activities across member states, including developing a centralised website with resources, guides, and promotional materials available to all EU citizens. The campaign themes are consistent across Europe, ensuring a unified message on cyber hygiene and secure data handling.

ENISA’s initiatives have effectively promoted cybersecurity awareness on a continental scale. Member states report increased participation in training programs and positive feedback from awareness campaigns. ENISA’s centralised approach facilitates a consistent message across diverse cultures, making cybersecurity education accessible throughout Europe [11].

A challenge for ENISA’s awareness initiatives is adapting content to the EU's varying levels of digital literacy and cultural differences. Future improvements could involve more localised content tailored to specific member states’ needs, allowing for greater customisation while maintaining core cybersecurity principles.

Comparative Analysis

These examples demonstrate how structured cybersecurity awareness campaigns across different sectors and regions can improve cybersecurity readiness and resilience. These organisations have successfully promoted cybersecurity best practices tailored to their audiences by employing targeted messaging, interactive training, and strategic partnerships. Each segment, healthcare employees, the public, or specific industry groups receive relevant and actionable information through targeted messaging, enhancing engagement and encouraging positive behavioural change. Furthermore, these initiatives foster a culture of security that extends beyond immediate participants, influencing broader organisational practices and public awareness.

Table 1. Comparative view

Organization	Sector	Key Objectives	Primary Tools Used	Outcomes Achieved	Limitations
NHS Digital (UK)	Healthcare	Improve resilience against cyber threats	E-learning, phishing simulations, CareCERT alerts	Significant reduction in phishing incidents	Sustaining engagement with high turnover
DHS and NCSA (US)	Government	National Cybersecurity Awareness	Social media, toolkits, partnerships	High public engagement and awareness	Sustaining awareness beyond campaign month
ENISA (EU)	Pan-European	Unified cybersecurity awareness	Training modules, centralized resources, campaigns	Broad EU-wide participation and awareness	Localization across diverse EU cultures

Interactive training, such as phishing simulations, gamified learning, and hands-on workshops, has proven valuable in reinforcing cybersecurity knowledge. These methods help individuals retain and apply information in real-world contexts, fostering a deeper understanding of cybersecurity risks and responses. Strategic partnerships with industry stakeholders, educational institutions, and public agencies amplify the reach and impact of these campaigns, leveraging resources and expertise to engage a wider audience and enhance the credibility of the messaging.

Despite these successes, challenges remain, particularly in sustaining engagement over time. Cybersecurity is not a "one-and-done" topic; threats evolve continuously, requiring ongoing awareness and adaptability. Maintaining long-term engagement demands creative approaches, such as periodic refreshers, updated content, and engaging formats that prevent "awareness fatigue" [12]. Without sustained engagement, initial improvements in cybersecurity behaviour may diminish over time, exposing organisations to potential risks.

Another critical challenge is addressing cultural diversity, especially for initiatives that span multiple regions or countries. Differences in language, digital literacy, and cultural attitudes toward cybersecurity can impact how messages are perceived and acted upon. For instance, what resonates with one demographic group may be less effective for another. Tailoring content to fit cultural and regional contexts is essential for achieving a truly inclusive and effective awareness campaign. This may involve translating materials, adjusting messaging to align with local values, or using culturally relevant examples that increase relatability and comprehension.

In conclusion, while these cases demonstrate the substantial benefits of structured cybersecurity awareness programs, they also highlight areas where future improvements could enhance impact. Developing adaptive strategies that address the need for sustained engagement and the nuances of cultural diversity will be essential for organisations looking to build a more resilient, security-conscious culture across all levels of their workforce and communities.

5. Conclusion

AR-in-a-Box provides a robust, adaptable framework for cybersecurity awareness. Its eight-step process encompasses all aspects of program development and execution. Each step, from Defining objectives and evaluating outcomes fosters a cybersecurity-conscious culture by addressing security's technical and behavioural dimensions. The toolkit's modular structure and data-driven approach make it accessible to organisations of varying sizes, enabling them to implement tailored and effective awareness programs.

The case studies demonstrate AR-in-a-Box's flexibility and impact across different organisational contexts, from small businesses to large public sector campaigns. By focusing on behavioural change and continuous improvement, AR-in-a-Box offers a comprehensive solution that prepares organisations to adapt to an ever-evolving cyber threat landscape.

References

[1]. T. Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organizations," *European Journal of Information Systems*, vol. 18, no. 2, pp. 106-125, Apr. 2009.

[2]. J. A. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, R. Warkentin, and M. Baskerville, "Future directions for behavioral information security research," *Computers & Security*, vol. 32, pp. 90-101, 2013.

[3]. SANS Institute, Security Awareness Maturity Model, [Online]. Available: https://www.sans.org/mlp/ssa-ebook-maturity-model/

[4]. International Organization for Standardization, *ISO/IEC 27001:2013 - Information Security Management*, ISO/IEC, 2013.

[5]. European Union Agency for Cybersecurity (ENISA). *AR-in-a-Box* [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-raising-in-a-box

[6]. UK Department of Health*, Your Data: Better Security, Better Choice, Better Care,* 2018: https://assets.publishing.service.gov.uk/media/5a823ac6ed915d74e62367b0/Your_data_better_security_better_choice_better_care_government_response.pdf

[7]. NHS Digital. "Data Security Centre: Cyber and Data Security Services." Available: https://digital.nhs.uk/cyber-and-data-security

[8]. Cybersecurity and Infrastructure Security Agency (CISA), "Cybersecurity Awareness Month," 2023. Available: https://www.cisa.gov/cybersecurity-awareness-month

[9]. National Cybersecurity Alliance (NCSA), "Cybersecurity Awareness Month," 2023. Available: https://staysafeonline.org/cybersecurity-awareness-month/

[10]. European Union Agency for Cybersecurity (ENISA), "European Cybersecurity Month,". Available: https://cybersecuritymonth.eu/

[11]. European Union Agency for Cybersecurity (ENISA), *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, Nov. 2018. Available: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

[12]. N. S. Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Computers & Security*, vol. 56, pp. 70-82, Feb. 2016. Available: https://doi.org/10.1016/j.cose.2015.10.006

Security of Digital Files: Audio Tampering Detection

Sebastian-Alexandru ARGHIRESCU
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
sarghirescu@upb.ro

Abstract

In an age where most of the data we interact with daily is stored digitally, methods of checking its authenticity become more and more essential. This is especially true for sound, as the increasing public availability of AI models makes tampering with audio files easier than ever. In this paper, we will be investigating the current landscape of audio forensics as well as our new hardware-based solution for double encoding detection.

Index terms: audio, automation, security, spectrum, tampering

1. Introduction and state of the art

There are two main types of approaches in classical audio tampering detection: active approaches based on embedding a watermark inside the file during or after recording and passive approaches which do not require any additional embedding.

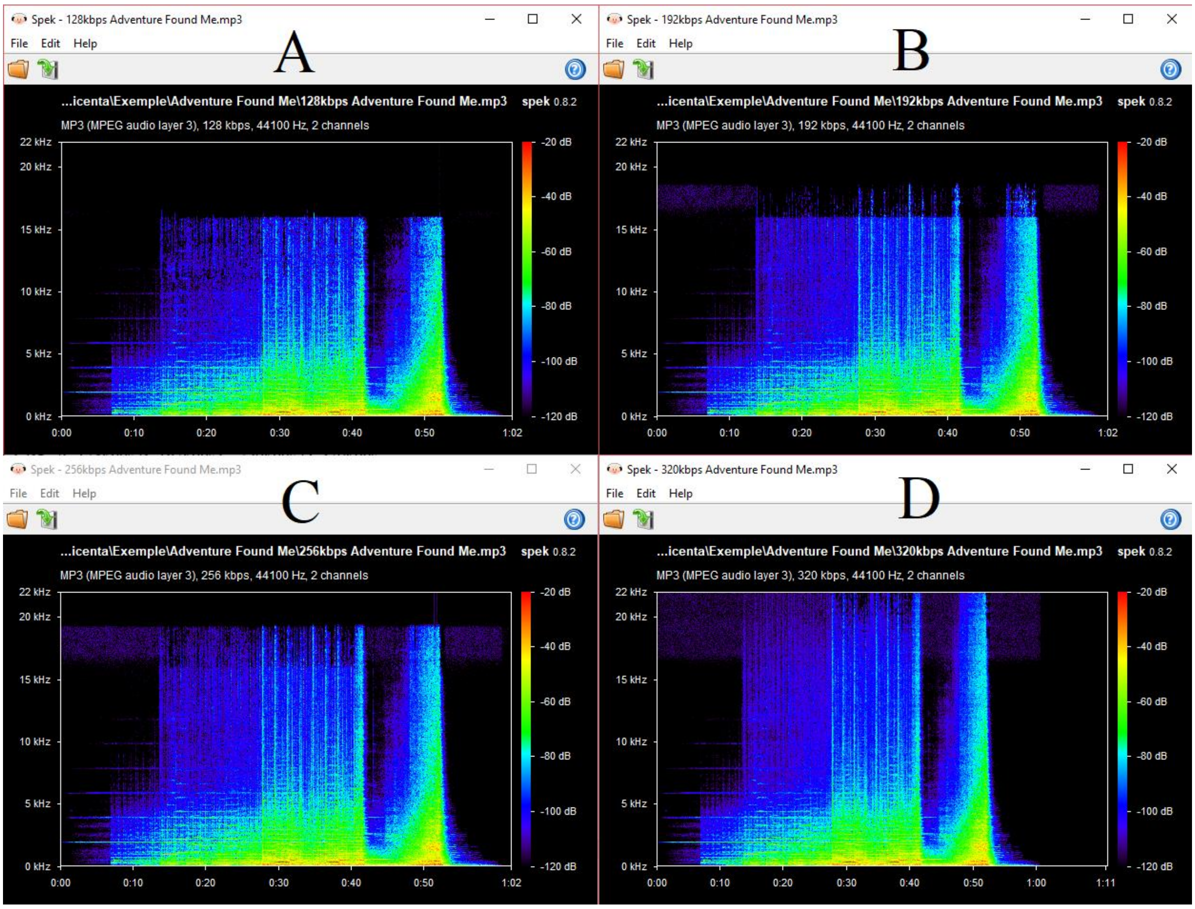
A passive approach for determining if an audio file has been tampered with is by doing an Electric Network Frequency (ENF) analysis on the recording in question. This is based on the finding that we can extract the mains hum from the recording and compare it with a database to detect tampering. The mains hum fundamental frequency should be at 50 Hz or 60 Hz depending on the location where the audio recording was taken. Due to the loading of national electric grind in various countries, the harmonics of the mains hum also differ by city and by time of day, so it is possible to also get an estimate of the time of the recording [1]. One instance of such ENF analysis is presented in [2] where the authors use FFT (Fast Fourier Transform) and machine learning algorithms to classify extracted ENF signals from signals of different lengths. The detection accuracy found varied by the algorithm used, signal duration (5, 15, 25, 35, 45 s) and type of tampering (copy, deletion) but ultimately fell in the 81-99% detection range. Another approach for ENF analysis is presented in [3] in which the authors use DFT (Discrete Fourier Transform) and a parallel RDTCN-CNN (Residual Dense Temporal Convolutional Network - Convolutional Neural Network) approach to obtain higher accuracy at 97-98%. As shown in [3], the main disadvantage of such methods is that they are highly dependent on the choice of training data set as well as requiring adequate hardware for the models to run on. A model that works in a country with over 90% accuracy could fall to below 60% in another country and would have to be tested and retrained every time on deployment.

Looking at active approaches, these are usually based on some form of embedding a DWT (Discrete Wavelet Transform) watermark into the source recording which can then be used to detect tampering or to reconstruct the original signal from various integrity fractions. One such example is [4] where the authors use a compressed version of the original audio signal to generate the watermark. This method showed a higher signal-to-noise ratio for the watermark than other active approaches, over 93% tampering detection rate and 80-98% recovery of the original recording with a destruction rate between 50-20%. The main disadvantage of this method is that it is in itself altering the original signal. If a passive approach is used on a watermarked recording, then it will output a false positive. In this case, we would need to know that a watermark was previously applied to the recording for an accurate tampering detection. The accuracy of active approaches also does not seem to be superior to that of their passive counterparts described above.

Another important subject in audio tampering detection is that of double encoding. This concept is less relevant in voice recording, where the classical methods discussed above are used, and more relevant in music. We will be measuring the compression level of a musical recording using Equation 1, where $\mathrm{F_S}$ is the sampling frequency of the recording and $\mathrm{N_{bps}}$ is the number of bits per sample.

$$\mathrm{F_S} * \mathrm{N_{bps}} = \mathrm{Bitrate} \tag{1}$$

Looking at the example in Figure 1, we see the spectrogram for the same song (Adventure Found Me by Jason Graves) four times at different bitrates: 128, 192, 256, and 320 kbps encoded using LAME [5] in a .MP3 container. The spectrograms were drawn using Spek [6].



...icenta\Exemple\Adventure Found Me\128kbps Adventure Found Me.mp3
MP3 (MPEG audio layer 3), 128 kbps, 44100 Hz, 2 channels

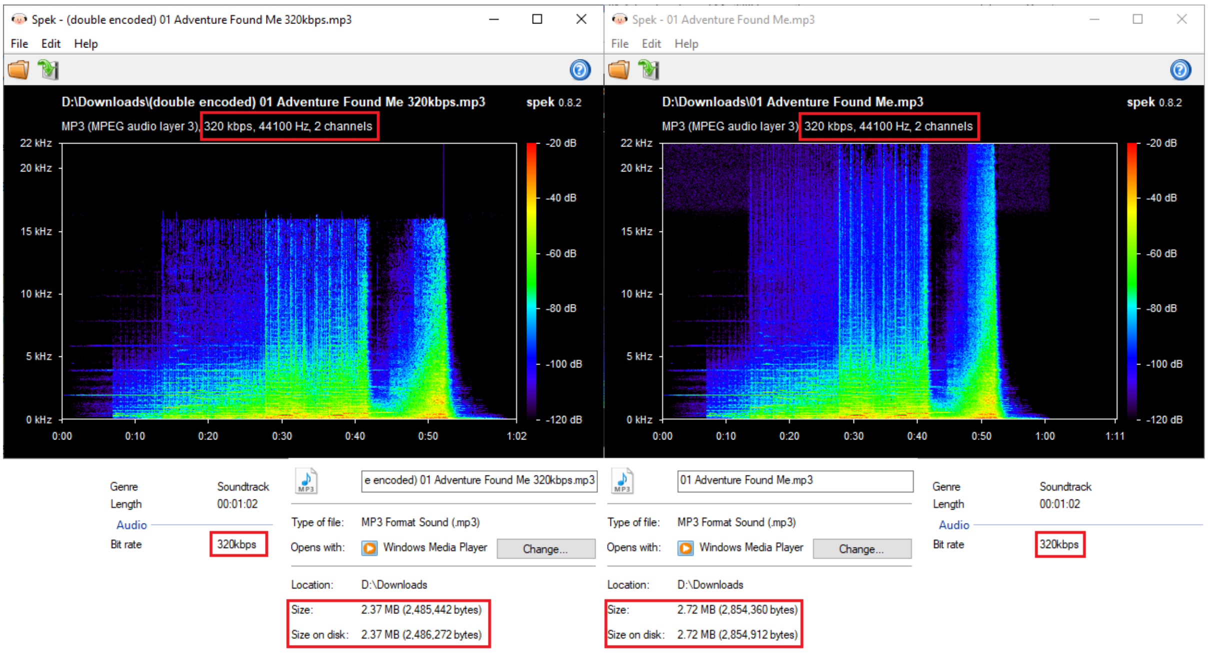
...icenta\Exemple\Adventure Found Me\192kbps Adventure Found Me.mp3
MP3 (MPEG audio layer 3), 192 kbps, 44100 Hz, 2 channels

...icenta\Exemple\Adventure Found Me\256kbps Adventure Found Me.mp3
MP3 (MPEG audio layer 3), 256 kbps, 44100 Hz, 2 channels

...icenta\Exemple\Adventure Found Me\320kbps Adventure Found Me.mp3
MP3 (MPEG audio layer 3), 320 kbps, 44100 Hz, 2 channels

Fig. 1. Spectrogram for the song Adventure Found Me - Jason Graves, 44.1 kHz, MP3, CBR, A. 128 kbps, B. 192 kbps, C. 256 kbps, D. 320 kbps

It was observed in [7] that we can use a spectrogram to determine the compression level of an audio file. We can see that for each jump in compression, the high-frequency content of the recording is visibly cut. This is normal as it reduces the size of the file, but the 128 kbps file could be re-encoded at 320 kbps increasing back the size without regaining any of the lost information. This is called double-encoding. In Figure 2 we can see that the double-encoded file on the left is almost the same size as the original file on the right, but its compression level is much higher. We can also see that the metadata of the file is the same which means the only way to distinguish the two is by looking at their spectrum. It is worth noting that depending on the file and the compression algorithm used the double encoded file may be larger than the original. The file size and reported bitrates in Spek and in Windows File Explorer are marked in red.



Spek - (double encoded) 01 Adventure Found Me 320kbps.mp3

D:\Downloads\(double encoded) 01 Adventure Found Me 320kbps.mp3

MP3 (MPEG audio layer 3), 320 kbps, 44100 Hz, 2 channels

Spek - 01 Adventure Found Me.mp3

D:\Downloads\01 Adventure Found Me.mp3

MP3 (MPEG audio layer 3), 320 kbps, 44100 Hz, 2 channels

Genre: Soundtrack
Length: 00:01:02
Bit rate: 320kbps

e encoded) 01 Adventure Found Me 320kbps.mp3
Type of file: MP3 Format Sound (.mp3)
Opens with: Windows Media Player
Location: D:\Downloads
Size: 2.37 MB (2,485,442 bytes)
Size on disk: 2.37 MB (2,486,272 bytes)

01 Adventure Found Me.mp3
Type of file: MP3 Format Sound (.mp3)
Opens with: Windows Media Player
Location: D:\Downloads
Size: 2.72 MB (2,854,360 bytes)
Size on disk: 2.72 MB (2,854,912 bytes)

Genre: Soundtrack
Length: 00:01:02
Bit rate: 320kbps

Fig. 2. File properties and spectrogram of the double encoded recording of Adventure Found Me - Jason Graves (left) and the original version (right)

Looking at the state of the art for this type of audio tampering we find that most solutions are using various machine learning algorithms. One example of this is [8] in which the authors use transformer networks to look at the compression history of audio files. The detection accuracy they obtained was between 84 and 94%. Another example of this is [9] which is more focused on codec classification rather than tampering detection but is using similar methods. Even though some of these methods such as [8] are less susceptible to the dataset used for training a big disadvantage of them is that they cannot be used to look at encrypted data streams such as the music used by streaming services. Other solutions for double encoding detection that do not use machine learning techniques usually use Modified Discrete Cosine Transform (MDCT) coefficients. Example of this are [10] and [11]. The accuracy of these methods in seems to be higher but the datasets used for testing were smaller and they seem to be very sensitive to the codec used for testing, working best with MP3 files. There is also the manual looking-at-the-spectrogram approach we have presented above but it is very slow and very dependent on the tester's experience.

2. Materials and methods

Our proposed solution uses a development board with additional signal acquisition circuitry in order to calculate the FFT and detect the presence of a specific predetermined audio band in the recording. In case of the double-encoding detection this interest band would be [17-20] kHz. A block diagram for the board cand be found in Figure 3. The red connections in Figure 3 represent power lines while the black connections represent data lines. An Arduino equipped with an ATmega2560 was used as a microcontroller for testing due to the larger memory requirement for the display buffer. The board was powered from a 9V battery in order to avoid as much interference as possible on the audio signal acquisition path. A 3.5mm male-to-male cable was used to inject the signal into the board form a signal generator. The same cable was used when testing the audio file from Figure 1, but instead of a signal generator, it was connected to the audio output of a computer using Windows 10.

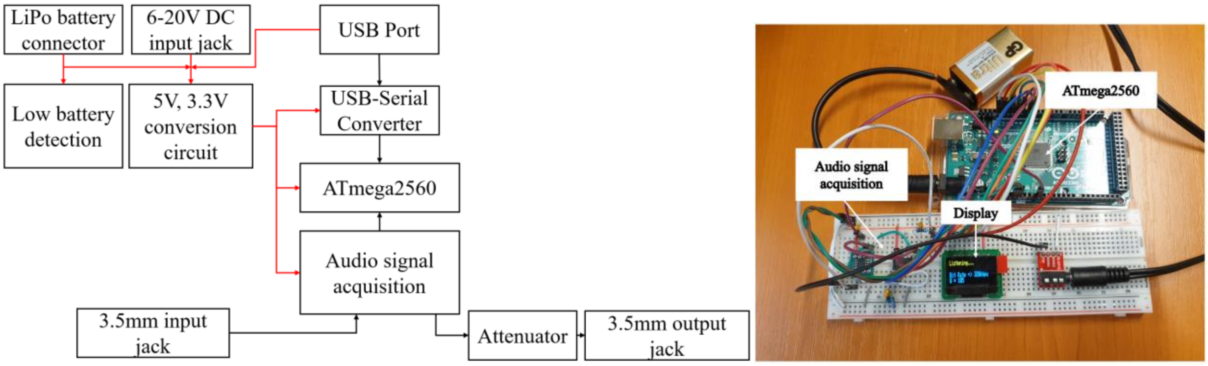


Fig. 3. Board diagram for the development board (left) and a picture of the board prototype (right)

The board samples the input signal at a frequency of 76.9 kHz, storing each sample in an 8-bit variable. The board then calculates the FFT and filters out all the frequency data that is not in the [17-20] kHz interval. It then calculates the spectral power distribution on smaller bands of 1 kHz inside the interest interval and estimates a quality factor Q. Based on this Q, the original bitrate of the song is estimated. The formulas used for these estimations are based on experimental observations. In order to test the performance of our solution we have used a signal generator to generate sine, square and triangle waves at different frequencies and amplitudes. The result of this testing can be seen in Figure 4 below.

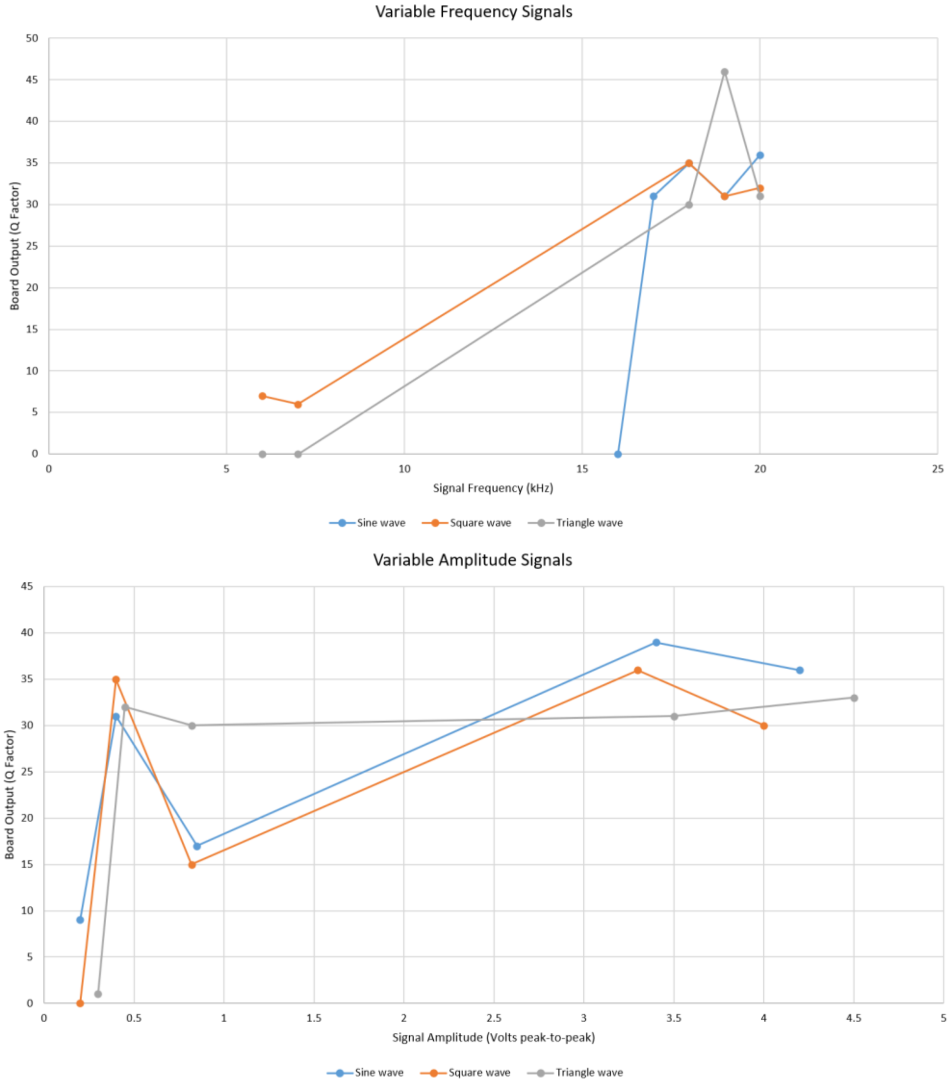
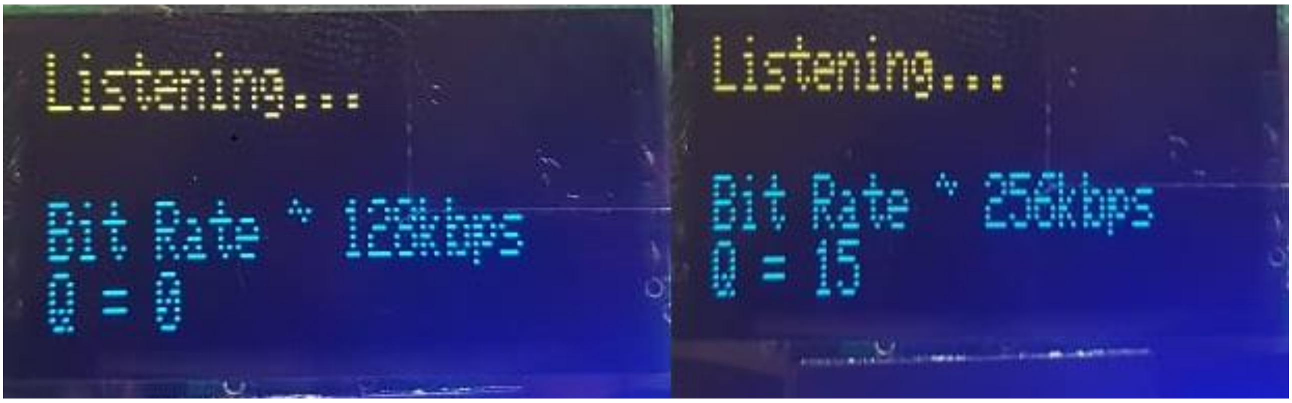


Fig. 4. Board output Q factor on the y-axis and signal frequency (up) or signal amplitude (down) on the x-axis for sine, square and triangle waves used for testing

If we consider the double encoding correctly detected for a Q-factor of 20 or over, then we can calculate a detection accuracy of 1 for the variable frequency signals and 0.8 for the variable amplitude signals for a mean accuracy of 0.9 or 90% for this very small dataset. We have also tested the songs present in Figure 1.A and Figure 1.D and the results can be seen in Figure 5 below.



```
Listening...

Bit Rate ~ 128kbps
Q = 0
```

```
Listening...

Bit Rate ~ 256kbps
Q = 15
```

Fig. 5. Detection results on the board display after the song in Figure 1.A was played (left) and after the song in Figure 1.D (right)

We see that the detection was far more difficult for signals with low amplitudes. We also have to take into account that square and triangle waves have harmonics on multiples of the fundamental frequency, and thus these harmonics could be detected causing false positives. This was not the case here probably because of the relatively low amplitudes of those harmonics in the test signals but could happen on larger datasets. The song we tested in Figure 1 was also not detected correctly, being recognized as 256 kbps instead of 320 kbps. This is likely caused by the short duration of the high frequency bursts observed in Figure 1.

3. Conclusion

There are many ways to tamper with audio recordings, from classical methods such as deleting or moving sections, to more advanced techniques like encoding lower-quality music in larger containers. There are also plenty of methods for detecting such tampering attempts. From active approaches consisting of embedding watermarks in the recording to passive ENF analysis to various machine learning algorithms trained on multiple data sets. Some approaches such as ENF analysis or watermark embedding have high accuracy rates but are unable to detect double encoding. Machine learning algorithms are also accurate but are highly dependent on the dataset used for training and require dedicated complex hardware to host the models. Other solutions using MDCT coefficients can detect encoding-based tampering but are not codec-agnostic.

Our proposed solution has lower detection rates even on pure monotonal signals but it looks at the recording in the analog domain so it can analyze encrypted data streams such as those found on streaming services in close-to-real-time. It is susceptible to low-duration pulses of high-frequency content but is less affected by the codec used in the recording than other methods. The amplitude of the signal must also be high enough (over 0.2 Vpp) for the detection of double encoding to be possible. Real-time ENF analysis may also be possible with this approach, but a lot more research on larger datasets is required.

References

[1]. R. Garg, A. L. Varna and M. Wu, "Modeling and analysis of Electric Network Frequency signal for timestamp verification," 2012 IEEE International Workshop on Information Forensics and Security (WIFS), Costa Adeje, Spain, 2012, pp. 67-72, doi: 10.1109/WIFS.2012.6412627.

[2]. Hsu, H.-P.; Jiang, Z.-R.; Li, L.-Y.; Tsai, T.-C.; Hung, C.-H.; Chang, S.-C.; Wang, S.-S.; Fang, S.-H. Detection of Audio Tampering Based on Electric Network Frequency Signal. Sensors 2023, 23, 7029. https://doi.org/10.3390/s23167029.

[3]. Zeng, C.; Kong, S.; Wang, Z.; Li, K.; Zhao, Y. Digital Audio Tampering Detection Based on Deep Temporal-Spatial Features of Electrical Network Frequency. Information 2023, 14, 253. https://doi.org/10.3390/info14050253.

[4]. Hu, Y., Lu, W., Ma, M. et al. A semi fragile watermarking algorithm based on compressed sensing applied for audio tampering detection and recovery. Multimed Tools Appl 81, 17729-17746 (2022). https://doi.org/10.1007/s11042-022-12719-0.

[5]. LAME MP3 Encoder, available online: https://lame.sourceforge.io/, last accessed on 30.10.2024.

[6]. Spek, available online: https://github.com/alexkay/spek, last accessed on 30.10.2024.

[7]. Alessandro, Brian & Shi, Y.Q. (2009). Mp3 bit rate quality detection through frequency spectrum analysis. 10.1145/1597817.1597828.

[8]. Z. Xiang, P. Bestagini, S. Tubaro and E. J. Delp, "Forensic Analysis and Localization of Multiply Compressed MP3 Audio Using Transformers," ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Singapore, Singapore, 2022, pp. 2929-2933, doi: 10.1109/ICASSP43922.2022.9747639.

[9]. Atieh Khodadadi, Soheila Molaei, Mehdi Teimouri, Hadi Zare, Classification of audio codecs with variable bit-rates using deep-learning methods, Digital Signal Processing, Volume 110, 2021, 102952, ISSN 1051-2004, https://doi.org/10.1016/j.dsp.2020.102952.

[10]. Yang, R., Shi, Y.-Q., & Huang, J. (2009). Defeating fake-quality MP3. Proceedings of the 11th ACM Workshop on Multimedia and Security - MM&Sec ’09. doi:10.1145/1597817.1597838.

[11]. Bianchi, T., Rosa, A.D., Fontani, M. et al. Detection and localization of double compression in MP3 audio tracks. EURASIP J. on Info. Security 2014, 10 (2014). doi:10.1186/1687-417X-2014-10.

Fake News

Dan-Ion CĂLIN, Alexandru BARCAN, Ciprian CONSTANTIN, PhD
“Alexandru Ioan Cuza” Police Academy, Bucharest, Romania
dancalin228@gmail.com, alexbarcan23@gmail.com, ciprianconstantin07@yahoo.com

Abstract

The terms "fake news" and "falsehood" have become ubiquitous in contemporary society. They influence or alter the way in which people perceive reality. The challenge of combating fake news lies in its ability to evade detection and capture the attention of a growing number of individuals. It has the potential to alter the way reality is perceived, impact the reputation of institutions and organisations, and even pose a threat to national security by influencing perceptions of values and risks. In today's context, fake news has emerged as a significant vulnerability, with the potential to be exploited as part of hybrid warfare strategies. One proposed method for combating the spread of fake news is the development of critical thinking skills that are specifically designed to identify such information and mitigate its influence on personal beliefs and values.

Index terms: disinformation, deep fake, fake news, information war, psychological warfare

1. Introduction

This article intends to provide an analysis of the fake news phenomenon and its effects on society, democracy, and the individuals who seek to propagate it. To accomplish this, it is crucial to understand the social context and how this phenomenon has gained substantial traction and influence. Historically, human societies have encountered and managed misinformation. However, the distinction today lies in the fact that fake news is increasingly utilized as a tool to achieve social and political objectives.

2. What is fake news?

In the absence of a clear definition, fake news is understood to be news that is either completely false or contains incomplete or partially true information. It is published with the intention of forming false opinions among those who access it. The content is fabricated, distorted, exaggerated, taken out of context and presented in a different image. Alternatively, it is a self-serving opinion that has been transformed into valid news with biased argumentation [1].

In 2018, as part of a series of measures to secure the digital information space, the European Commission started work on an EU-wide Code of Good Practice on Combating Online Misinformation, which defines misinformation as "a set of demonstrably false or misleading information created, presented and disseminated for economic gain or to deliberately mislead the public and which may cause public harm" [1].

3. What is the relationship between fake news, propaganda and disinformation?

The term 'dezinformatsiya', derived from the Russian language, has its roots in the actions of Soviet strategists during the 20th century. These actions were designed to disseminate false information with the intention of influencing public opinion. The subjects of disinformation were primarily selected from topics of broad public interest, and the content of the messages was based on a combination of true and false information. These messages were sent in a sustained and persistent manner [2] [3] [4].

The term 'propaganda' has its roots in the late 19th and early 20th centuries. It is defined as any information that is manipulated or distorted with the intention of promoting a political or other cause. This manipulation or distortion is typically carried out by governments or media institutions with the aim of influencing public opinion in a way that is favourable to the propagandist [5] [6].

4. What does fake news aim to achieve?

The act of distorting the public's perception or creating a new trend with the intention of misinforming or creating confusion and destabilising the sense of collective or national security.

The adverse effects of fake news are predominantly experienced by citizens, who are an integral component of the concept of national security as both beneficiaries and as a value to be protected.

The visibility gained as a result of the circulation of messages (issuing, receiving, absorbing, distributing, quoting, redistributing) increases the potential danger to national security, particularly in the context of fostering mistrust in democratic systems. Furthermore, fake news messages tend to appeal to prejudices or exploit issues that are particularly sensitive to the population, such as ethnic tensions, racial, ethnic, or religious differences. This is done in order to divert attention from issues that are more relevant to the state and its citizens [7].

With today's technological capabilities, it is very easy to create, edit, publish and distribute content. National interests can be compromised by the power of fake news published with the aim of influencing a state's strategic decisions by exploiting mistrust or doubt [1].

It is possible for a variety of domestic and foreign actors to utilise mass online disinformation campaigns on a large scale with the intention of sowing mistrust and creating societal tensions, which could have serious consequences for our collective security. Furthermore, disinformation campaigns initiated by third countries can constitute a hybrid threat to internal security, including electoral processes, particularly when combined with cyber-attacks. For instance, Russian military doctrine explicitly recognises information warfare as one of its domains. Furthermore, the dissemination of disinformation can also impact political processes by distorting public opinion. Domestic and foreign actors may utilise disinformation to influence policy, public discourse and behaviour in areas such as climate change, migration, public security, health and finance. Additionally, misinformation can also contribute to the erosion of trust in science and empirical evidence.

5. How fake news is used in war: hybrid war

Fake news has become a powerful tool in modern conflicts, used to manipulate public opinion, destabilize adversaries, and influence the course of events on the battlefield. Here are some of the most common ways fake news:

Propaganda and disinformation are used in war:

1. Fabrication of an enemy image: Dissemination of false information regarding the enemy's intentions, capabilities, or cruelty can serve to justify one's own actions and mobilise the population for the war effort.
2. The sowing of discord among the enemy is achieved through the creation and dissemination of false rumours pertaining to political or social divisions within the enemy country. This can result in the undermining of national unity and the weakening of resistance.

3. Manipulating international public opinion: The dissemination of false information has the potential to influence international public opinion and garner political or economic support for one's own interests.

Psychological Operations:

1. Demoralizing the enemy: The dissemination of misinformation regarding significant losses, military setbacks, or internal issues has the potential to dispirit enemy forces and diminish civilian morale.
2. Creating panic: The dissemination of false information regarding the occurrence of chemical, biological, or nuclear attacks has the potential to incite panic and chaos among the civilian population.
3. Influencing strategic decisions: The dissemination of inaccurate information regarding the disposition of enemy forces has the potential to mislead military commanders and exert undue influence on strategic decision-making.

Censorship and control of information:

1. Blocking access to truthful information: In an effort to control the narrative and maintain power, authoritarian regimes may resort to censoring the media and blocking internet access, thereby limiting the population's ability to access information about the conflict.
2. Promoting alternative narratives: The creation and promotion of alternative narratives can serve to justify the actions of the regime and distort the reality of the situation.

Amplifying social divisions:

1. Exploiting fear and hatred: The dissemination of misinformation can be employed to exacerbate existing anxieties and prejudices, thereby intensifying social polarisation and fostering further social divisions.
2. Preventing dialogue and peaceful resolution of conflicts: The proliferation of fake news can create an atmosphere of distrust and hostility, impeding constructive dialogue and negotiation, and prolonging the conflict.

6. Fake news and COVID-19

COVID-19 (Corona Virus Disease, 19 indicates the year the first case was reported) is a disease caused by SARS-CoV-2 that began in December 2019 in Wuhan, China. The outbreak is thought to have started in a seafood market, and some articles claim it was created in a laboratory in Wuhan. The most common symptoms of the virus are fever, cough and tiredness. In most people, this virus presents with mild forms of symptoms, with an 80% recovery rate without the need for hospitalisation. People at high risk of developing health problems with SARS-Cov-2 are the elderly, people with heart or lung problems, diabetes or cancer. The symptoms of the virus are similar to those of seasonal flu. The psychological impact on all people is of crucial importance because of the very rapid transmission of the virus, the quarantine period, the possibility of losing loved ones, mistrust of others, infected people who do not follow the rules, guilt, anxiety, pessimism and paranoia.

A fake news during the pandemic period is represented by the fact that G5 would be the cause of the COVID-19 virus or even exacerbate the disease (Ahmed, Videl-Allabal, Downing, Segui, 2020). Ahmed and his collaborators conducted a study analysing the spread of this fake news and misinformation on the social network Twitter. They analysed this phenomenon for one week and found that out of 233 messages distributed, 34.8% of the messages belonged to people who believed in this phenomenon. The remaining 65.2% of the messages came from people who did not believe in the conspiracy theory but spread the message. This clearly shows the rapid spread of false information without prior investigation. The person who wrote this message intended to spread misinformation. The consistency of this rumour is extreme, as some people have set fire to 5G masts/towers and even a hospital phone tower in the UK [5].

7. The psychological implications of fake news

The role of emotions in how people perceive and respond to fake news is a significant one. Emotional responses, such as fear, anger, or excitement, can render individuals more vulnerable to misinformation, as emotionally charged content often captures attention more effectively than neutral information. When individuals experience intense emotions, they may be inclined to rely less on critical thinking and more on intuitive responses, increasing the likelihood of accepting misinformation without verification. Furthermore, emotionally compelling narratives are frequently shared more extensively on social media, which further amplifies the dissemination and impact of misinformation. Recognizing the role of emotions in information processing is vital for effectively addressing the challenges posed by fake news [5].

The rapid dissemination of fake news is a phenomenon that is particularly prevalent in the political sphere, where it is often employed with the intention of influencing public opinion and behaviour. This phenomenon subsequently extends into other domains, including science, technology, celebrity culture and events related to natural disasters. In these contexts, misinformation can distort perceptions of essential topics and create confusion among the general public. Those who rely more on emotions than reason tend to perceive such messages as true, even when they are misleading [5].

A classification of errors associated with the phenomenon of fake news:

1. The illusionary truth effect: describes the tendency of individuals to view a statement as more credible with increased exposure, regardless of its truthfulness. The more frequently information is repeated, the higher its perceived credibility becomes, even if the information is false. This phenomenon arises from psychological mechanisms that blur the line between familiarity and truth, leading people to accept frequently encountered information as true simply because they have heard it often. The illusionary truth effect is frequently leveraged in the context of fake news, playing a significant role in the dissemination and entrenchment of disinformation [5].
2. Partisan identity: in the context of fake news, partisan identity refers to the influence that a person's political or ideological affiliation exerts on their perception and dissemination of false information. It has been demonstrated that this identity can impact memory, resulting in individuals recalling situations or false claims that did not actually occur. One pertinent experiment demonstrated that, among participants who were exposed to a series of both authentic and fictitious news stories, approximately half reported that a specific event had occurred, while 27% of participants indicated that they had observed the event on the news, despite its actual absence [5].

Partisan identity extends beyond the boundaries of consciousness and perception of reality. When coupled with ideological beliefs, this identity can lead an individual to eschew the verification of a fake news story, instead relying on their pre-existing beliefs. This dynamic contributes to the perpetuation of misinformation and impedes efforts to counter the impact of fake news in society [5].

8. Conclusion

In conclusion, the phenomenon of fake news poses a significant challenge in today's society, requiring ongoing efforts to understand not only how it spreads but also how it evolves over time. Its effects are increasingly apparent and have the potential to profoundly influence various choices, including those related to politics, social interactions, and personal decisions.

Every day, people are inundated with a torrent of messages, and the reliability of online information sources is deteriorating, complicating the process of discernment even further. This issue is exacerbated by social media algorithms that tend to favor provocative and emotionally charged content, often at the expense of verified and trustworthy information.

The psychology behind fake news is intricate. Cognitive mechanisms, such as the illusionary truth effect and confirmation bias, make individuals more likely to accept false information as true. Consequently, distinguishing between fact and fiction is not always straightforward. Therefore, it is crucial to promote media literacy and critical thinking, enabling individuals to develop the skills needed to assess information sources and make informed decisions.

In essence, the resolution of the issue of fake news requires the collaboration of governments, media organisations, educational institutions and civil society. This must be done in order to foster a healthier information landscape that champions the truth and mitigates the effects of misinformation. It is incumbent upon each of us to play a pivotal role in this endeavour by assuming responsibility for the verification of information prior to its dissemination. In this way, we contribute to the development of a more informed society, better equipped to navigate the information challenges of our time.

References

[1]. S.R.I., "Fake News #awareness," 2020.

[2]. https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX%3A52018DC0236.

[3]. https://www.researchgate.net/profile/Ruxandra-Buluc/publication/335727273_CULTURA_DE_SECURITATE_si_FENOMENUL_FAKE_NEWS/links/5d77dc83299bf1cb809807ff/CULTURA-DE-SECURITATE-si-FENOMENUL-FAKE-NEWS.pdf.

[4]. https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/dealing-with-propaganda-misinformation-and-fake-news.

[5]. B. Cristina Maria and M. Alexandra, "Fenomenul Fake News," Institutul European, Bucharest, 2022.

[6]. Norbert Schwarz, Mariela E. Jaffé, Eryn J. Newman, Reiner Greifeneder, Psihologia Fake News: Acceptarea, distribuirea și corectarea informațiilor false, Trei SRL, 2021.

[7]. B. Oprea, "Fake News și dezinformare online: recunoaște și verifică," Polirom, Bucharest, 2022.

Operationalizing the Cyber Threat Landscape: Key Considerations and Challenges in Developing a Specific Organizational Program

Costel CIUCHI, PhD
Assoc. Prof., Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
costel.ciuchi@upb.ro

Abstract

The landscape of cyber threats is multifaceted, encompassing a wide array of attack vectors, including distributed denial of service (DDoS) attacks, phishing, man-in-the-middle attacks, password-based intrusions, remote exploitation, privilege escalation, and malware deployment. As the sophistication of cyber threats continues to advance, coupled with the development of increasingly sophisticated evasion techniques, traditional security mechanisms - such as firewalls, intrusion detection systems, antivirus software, and access control lists - are proving less effective in identifying and mitigating these complex threats. This underscores the urgent need for the development and implementation of innovative, more robust solutions to counteract the growing prevalence of cyber-attacks. The objective of this proposal is to examine the ENISA Cybersecurity Threat Landscape Methodology and explore potential advancements that integrate traditional decision-making frameworks with emerging cybersecurity technologies. As concerns over cyber warfare continue to escalate, nations must adopt adaptable cyber frameworks and methodologies capable of preventing cyber crises. Furthermore, these frameworks should foster greater international collaboration and participation in the ongoing global discourse on cybersecurity.

Index terms: risk & vulnerability management, threat landscape, cyber threat intelligence, defence strategies, incident response, intrusion detection, frameworks and methodologies

1. Introduction

The digital threat landscape constantly evolves, with malicious actors launching more sophisticated attacks daily. Organizations must keep up with the latest cybersecurity frameworks to stay ahead of this dynamic threat environment. The frequent questions from stakeholders and political level related to cybersecurity: How secure we are? What is the status of cybersecurity?

Several factors led to the development of legislation, policies and guidance, but not limited to, the growing cyber threat landscape, technological advancement, increase in emerging risks, insufficient implementation of the Directives in the national legislative framework, increased dependency on digital and supply chain risks, evolving European cybersecurity policy, and the need to strengthen the developments in domain.

Cybersecurity Threat Landscape (CTI) represent the knowledge and understanding of actual or perceived threats that conduct organizations' security decision-making. The intelligence typically relates to the threat actor's goals, intentions, strategies, capabilities, limitations, and vulnerabilities. It is used in organizational planning, analysis, situation awareness, and prediction of future events related to cybersecurity to support business operations and managerial decisions.

The practice of threat intelligence comes from the military area [1], where decision-makers and experts, collect, process, and disseminate intelligence to other upper levels of decisions and stakeholders.

CTI represent a subset of cyber intelligence (CI) that relates to threats and threat actors [2]. By implementing a CTI Program, organizations can transform generic cyber practices from being "reactive and undirected" to being "proactive, anticipatory, and dynamic" [3].

2. Threat Landscape

The **threat landscape** is the entirety of potential and identified cyber threats affecting a particular organization, sector, group of users, or time period [4].

The threat landscape is typically conceptualized as encompassing the vulnerabilities, malicious software, and distinct categories of threat actors along with their methodologies that pose risks within a particular context.

This implies that it is essential to consider the specific characteristics of an organization, sector, or even an individual, which may include, but are not limited to, the following factors [5]:

- the sensitive or valuable data targeted by attackers;
- the security state, cost and frequency of cyber-attacks;
- geopolitical influences, as certain threats focus on entities located in specific countries or regions.

The threat landscape evolves both over time and in response to events that have a substantial impact on the organization, people, or sector for which the threat landscape is defined. A recent example of this is the rise in attacks targeting remote-access tools, which have become prominent within the threat landscapes of numerous organizations.

Several factors, shape and influence the evolution of the threat landscape [6, 7], including:

- identification and disclosure of vulnerabilities that open opportunities for cybercriminal exploitation;
- release of updated software versions introducing additional functionality and potential security risks;
- development of new hardware platforms, and innovative data processing methodologies, such as cloud computing and edge computing;
- global events, such as the COVID-19 pandemic, have forced organizations to make major changes to their infrastructure, often expanding the attack surface.

Understanding the current threat landscape is crucial, as conducting a comprehensive analysis allows for the identification of potential information security risks confronting a specific entity - whether a company, individual, or entire sector.

This proactive approach enables the implementation of preventive measures, thereby enhancing the entity's ability to anticipate and mitigate emerging threats to information security.

3. Current Cyber Threat Landscape

The current cybersecurity threat landscape is marked by growing complexity and rapid evolution. Organizations are exposed to a wide spectrum of threats, ranging from simple, low-tier attacks to sophisticated, highly coordinated campaigns launched by nation-state actors.

According to the ENISA Threat Landscape 2024 report [8], which covers the period from July 2023 to June 2024 and was released in September 2024, seven primary cybersecurity threats were identified:

- Ransomware
- Malware

- Social Engineering
- Threats against data
- Threats against availability: Denial of Service
- Information manipulation and interference
- Supply chain attacks

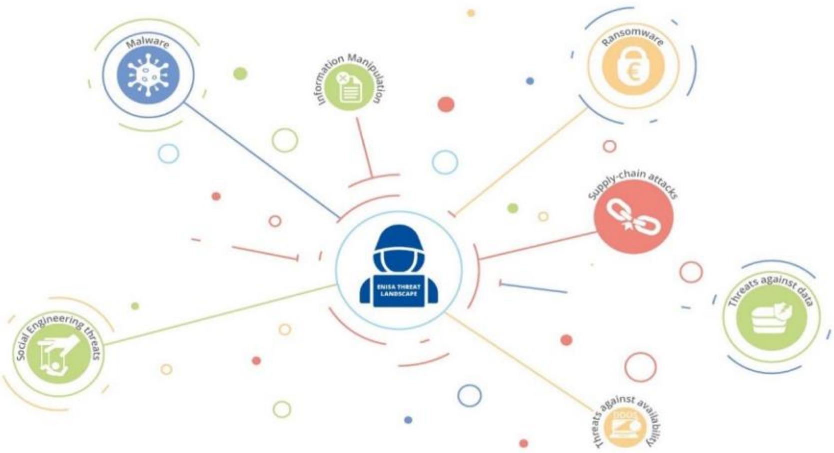


Fig. 1. ENISA Threat Landscape 2024 - Prime threats [8]

The ENISA Threat Landscape (ETL) 2024 report is derived from a combination of open-source data, primarily of a strategic nature, as well as ENISA's own Cyber Threat Intelligence (CTI) capabilities. The report follows the methodology outlined in the ENISA Cybersecurity Threat Landscape (CTL) framework [9].

According to the CrowdStrike 2024 Global Threat Report [10], several key emerging trends and evolving threats are currently shaping the cybersecurity landscape, including:

- **Ransomware -** remains a persistent and high-impact threat, with threat actors employing increasingly advanced tactics to target organizations of all sizes. The primary method of monetization for ransomware attacks continues to be the encryption of critical data, followed by extortion demands for decryption keys or the threat of public data leakage;
- **Supply Chain Attacks -** involve the compromise of third-party vendors or software providers to gain unauthorized access to a target organization's systems. These attacks are primarily aimed at data exfiltration and optimization of extortion tactics, often leveraging trusted relationships to bypass traditional security measures;
- **Business Email Compromise (BEC) -** a form of social engineering in which attackers impersonate senior executives or other trusted individuals to deceive employees into transferring funds or disclosing sensitive information. BEC attacks often result in substantial financial losses for organizations globally, exploiting human trust and organizational communication channels;
- **IoT vulnerabilities** - the growing number of Internet of Things (IoT) devices presents an attractive target for threat actors, as many of these devices are deployed with inadequate security measures. Exploiting these vulnerabilities allows attackers to gain unauthorized access to corporate networks or use compromised devices as launching points for attacks on other systems or organizations;
- **State-Sponsored Attacks -** nation-state actors remain a critical threat, conducting cyber espionage, intellectual property theft, and targeting critical infrastructure for disruption. Geopolitical tensions often escalate these activities, resulting in highly targeted intrusions and an increase in hacktivist-driven cyber operations. Such attacks are expected to persist

as key drivers of cyber conflict, with both strategic and ideological motivations shaping the threat landscape;

- **Generative Artificial Intelligence (AI) - t**hreat actors are leveraging AI technologies to enhance the sophistication and precision of cyberattacks. AI-driven attacks can automate social engineering tactics, refine malware to evade detection and optimize attack strategies, making them more adaptive and harder to mitigate. This increasing use of AI poses significant challenges for traditional defence mechanisms;
- **Malvertising and SEO Poisoning** - **Malvertising** involves the creation of malicious advertisements that serve as vectors for cybercriminal activities, often leading to malware infections or data breaches. **SEO Poisoning** involves manipulating search engine optimization (SEO) techniques to artificially elevate malicious websites in search engine results. This tactic exploits the common user perception that top-ranked search results are the most credible, increasing the likelihood of users visiting and interacting with compromised sites.

Global reports emphasize several critical trends that must be considered when assessing the current cyber threat landscape. These include:

- **Increasing Role of Artificial Intelligence (AI)**: AI technologies are increasingly being utilized in both cyberattack execution and the enhancement of cybersecurity defences. Attackers leverage AI to automate and refine attack strategies, while defenders use it to improve threat detection, response times, and overall security posture;
- **Emerging Security Regulations**: Governments and regulatory bodies are enacting new and **evolving** cybersecurity laws, compliance standards, and data protection frameworks. These regulations are significantly shaping how organizations manage data security, privacy, and risk mitigation, with a growing emphasis on compliance and accountability;
- **Critical need for cyber resilience:** as cyber threats become more persistent and sophisticated, organizations must focus on building resilience to ensure rapid recovery, business continuity, and minimal disruption in the event of a successful cyberattack, thereby maintaining operational stability even during a breach.

4. Implement a Cyber Threat Landscape Program

Based on the three pillars of cybersecurity - **people**, **process**, and **technology** [11] - an organizational cyber threat landscape program must incorporate a strategy that is tailored to the specific needs of the business and aligned with its objectives. This approach should be designed to enhance the organization’s ability to perform securely and effectively. To achieve this, all three pillars should be guided by five key directions:

- **Prevention (education, policy development, and security best practices)**
- **Protection (defence mechanisms, block malicious activity and mitigate risks).**
- **Detection (monitoring tools, anomaly detection, and behavioural analytics identifying attacks in real-time).**
- **Response (incident response planning, containment strategies, and communication protocols.**
- **Cooperation (sharing information and collaborating with internal and external sources)**

By integrating these five directions into the core pillars of people, process, and technology, organizations can develop a robust, adaptive cybersecurity program that aligns with business goals and responds effectively to the evolving threat landscape.

Developing a cyber threat landscape assessment [12] based on proposed program pillars represents a more comprehensive evaluation of an organization's digital security posture. It involves systematically identifying, analysing, and prioritizing potential new possible cyber threats that could impact the organization.

This assessment helps organizations understand the range of risks they face, the likelihood and potential impact of those threats, and the effectiveness of existing security controls. By gaining insights into current vulnerabilities and emerging threats, organizations can develop targeted strategies, policies, and procedures, to enhance their cybersecurity defences and improve overall risk management.

Conducting a ***cyber-threat landscape assessment*** provides several key benefits for organizations that are using classical cybersecurity approaches. These benefits include (Table 1):

Table 1. Benefits for organizations

Directions	***Domain***	***Benefits***
Prevention	*vulnerabilities*	• *classification of vulnerabilities based on the organization technologies, processes, and personnel;* • *identify cross-domain vulnerabilities.*
Protection	*risk mitigation*	• *helps prioritize the most significant threats and vulnerabilities based on the potential impact on the organization;* • *ensure effective risk reduction by prioritizing risk mitigation efforts.*
Detection	*enhanced threat intelligence*	• *better understanding of potential cyber threats and attackers, and associated risks;* • *develop more effective incident response plans, detect and prevent malware infections, and identify emerging attack techniques.*
Response	*improved incident response and recovery*	• *identify potential breaches and security incidents, allowing organizations to develop a proactive incident response plan;* • *effectively respond to a security incident with a plan, minimizing the impact on their operations.*
Compliance	*compliance with regulations and standards*	• *ensure an organization complies with these regulations and standards;* • *identify potential compliance gaps or factors such as insufficient access controls or inadequate security training.*
Cooperation	*collaboration and intelligence sharing*	• *collaboration with external partners, such as threat intelligence networks, industry groups, or local authorities lead to a stronger collective defence.*

5. Program actions to protect against the Threat Landscape

Organizations must establish a robust and proactive cybersecurity framework to safeguard against the dynamic and constantly evolving threat landscape. A comprehensive cyber threat landscape program should incorporate several critical components, including the four primary workflows:

- **Establish Programs - Supply Chain Security program, Threat Monitoring program, Change Management program;**
- **Implement Plans - Regular Security Assessments plan, Incident Response plans, Disaster Recovery plans;**
- **Conduct - regular Employee Training, regular Cyber Exercises, and regular Software and System Updates;**
- **Control - Implementing rigorous verification, monitoring, and control mechanisms across all the aforementioned activities (regular audits, performance tracking, and the use of automated tools)**

A critical starting point for organizations is to adopt the ENISA Cybersecurity Threat Landscape (CTL) methodology [9] as part of their organizational culture. This approach provides a structured framework for understanding and managing cyber threats. Organizations should then develop a tailored cybersecurity framework that focuses on effectively managing cybersecurity risks, mitigating vulnerabilities, and enhancing overall digital defence mechanisms. This framework should integrate threat intelligence, risk assessment, and proactive security measures to address evolving threats and safeguard the organization's assets.

Also, adopting a methodology (ENISA Cybersecurity Threat Landscape - CTL), including high management leadership and oversight, legal considerations will develop a cybersecurity governance framework that will ensure an organization's cybersecurity practices are well-coordinated, consistently applied, and capable of adapting to an ever-changing threat landscape.

By strategically investing in human resources, addressing skills gaps, leveraging advanced technologies, enhancing risk management practices, and fostering improved communication and collaboration, organizations can significantly bolster their security posture and mitigate potential cybersecurity risks.

Additionally, the continuous development and refinement of existing frameworks and methodologies will serve as critical enablers for capacity building, empowering organizations to effectively navigate the increasingly complex and dynamic cybersecurity landscape.

To strengthen their cybersecurity defences, organizations should take several specific actions. First, they must develop and implement proactive recruitment strategies to attract and retain skilled cybersecurity professionals, offering competitive salaries, benefits, and opportunities for professional development. Additionally, investing in training and development programs is essential to upskill existing staff, bridging skills gaps through online webinars, corporate training events, and mentoring initiatives.

Organizations should also explore the potential of artificial intelligence (AI) to automate routine tasks, enhance threat detection and response capabilities, and improve overall security posture. Conducting regular cyber risk assessments is critical for identifying vulnerabilities and developing strategies to mitigate the likelihood and impact of cyberattacks.

Furthermore, organizations must ensure comprehensive cyber insurance coverage, understanding the terms of their policies to ensure they provide adequate protection against potential risks. Finally, fostering effective communication and collaboration across security teams, leadership, and other departments is vital. Breaking down silos and sharing information, insights, and best practices will help strengthen the organization's collective cybersecurity efforts.

Also, for a successful program in the cybersecurity threat landscape, employees must prioritize staying informed about the latest threats and trends by regularly updating their knowledge and skills through professional development, certifications, and online resources.

In addition to technical expertise, developing strong soft skills such as communication, collaboration, critical thinking, and problem-solving is essential for effective performance, as these skills facilitate teamwork and strategic decision-making. Given the constantly evolving nature of the cybersecurity landscape, embracing a mindset of continuous learning is crucial.

By committing to lifelong learning, individuals can remain adaptable, stay ahead of emerging threats, and maintain their professional edge in an increasingly complex field.

6. Conclusion

Developing and adopting robust, adaptable cybersecurity frameworks is essential for mitigating the risks posed by evolving threats. These frameworks should incorporate risk management strategies, continuous monitoring, and collaboration across sectors and borders. International cooperation will be critical to address threats that span multiple countries and jurisdictions.

The evolution of cyber threats presents significant challenges to the security and stability of modern societies. As cyber threats become more advanced, widespread, and complex, traditional defence mechanisms are increasingly inadequate. To effectively combat these threats, it is essential to adopt an approach that integrates innovative technological solutions, robust frameworks, continuous collaboration, and enhanced cybersecurity education. Only through these combined efforts can we hope to mitigate the risks posed by the rapidly evolving landscape of cyber threats.

Integrating traditional decision-making frameworks, established standards, and senior management with emerging cybersecurity technologies presents a powerful opportunity to enhance an organization's security posture, improving both effectiveness and agility. Several advancements can be leveraged in this integration, such as Data-Driven Decision-Making with AI and Machine Learning, which enables real-time threat detection and predictive risk modelling. Automated Threat Intelligence Integration can streamline the analysis of threat data, ensuring timely and informed responses to evolving cyber risks.

Adaptive Risk Management Models facilitate continuous, real-time risk assessments, empowering organizations to dynamically adjust their security strategies as new vulnerabilities emerge. The use of Blockchain for Secure Decision-Making and Audit Trails ensures the integrity, transparency, and immutability of security-related decisions, providing a verifiable record for compliance and accountability. Additionally, Cybersecurity Decision Support Systems (DSS) can assist senior management in making data-driven, strategic decisions by aggregating threat intelligence, simulating attack scenarios, and offering predictive insights into the organization's cybersecurity risks.

These advancements enable organizations to navigate the increasingly complex cybersecurity landscape with greater precision, responsiveness, and foresight. This fusion enables a more proactive, data-driven, and transparent approach to managing cybersecurity risks, ensuring that organizations are better equipped to respond to the rapidly evolving threat landscape.

Operationalizing the cyber threat landscape is essential for organizations seeking to build a resilient and adaptive cybersecurity program. While there are numerous key considerations, including integrating threat intelligence, adopting risk-based strategies, and ensuring continuous monitoring, organizations also face significant challenges such as resource constraints, skill shortages, and the complexity of managing evolving threats. Addressing these challenges requires a holistic approach, involving strong leadership, cross-functional collaboration, and a commitment to continuous improvement and adaptation in the face of a rapidly changing cybersecurity landscape.

References

[1]. Sean Barnum. 2012. Standardizing cyber threat intelligence information with the structured threat information expression (STIX). Mitre Corporation 11(2012), 1-22.

[2]. Donald Gerwin & J. Stephen Ferris, 2004. "Organizing New Product Development Projects in Strategic Alliances," Organization Science, INFORMS, vol. 15(1), pages 22-37, February.

[3]. Bongsik Shin, Paul Benjamin Lowry, A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished, Computers & Security, Volume 92, 2020.

[4]. Fortinet Training Institute, Introduction to the Threat Landscape, https://training.fortinet.com/local/staticpage/view.php?page=library_introduction-to-the-threat-landscape

[5]. Top Cybersecurity Statistics for 2024, https://www.cobalt.io/blog/cybersecurity-statistics-2024

[6]. Expert Insights Podcast, John Grancarich On the Evolution of the Threat Landscape, How Security Providers Need To Pivot, https://podcasts.apple.com/gb/home

[7]. Antonio de Lucas Ancillo, Sorin Gavrila, María Teresa del Val Núñez, Workplace change within the COVID-19 context: The new (next) normal, Technological Forecasting and Social Change, Volume 194, 2023, ISSN 0040-1625.

[8]. ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[9]. ENISA Cybersecurity Threat Landscape (CTL) methodology, July 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

[10]. CrowdStrike 2024 Global Threat Report, https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

[11]. I.C. Mihai, C. Ciuchi, and G. Petrică, "Current challenges in the field of cybersecurity - the impact and Romania's contribution to the field", Ed. Sitech, 2018.

[12]. I.C. Mihai, G. Petrică, C. Ciuchi, L. Giurea, "Cybersecurity challenges and strategies", Ed. Sitech, 2015.

Dynamic QR Codes: A Solution for Secure Mobile Payments

Dr. Om Prakash YADAV, Ankit KUMAR, Kalash SHANDILYA, Shubhankar KUMAR
School of Computer science and Engineering, Lovely Professional University, Jalandhar India
om.26121@lpu.co.in, kumarankityadav88777@gmail.com, kalashshandilya@gmail.com,
shubhankar.kr24@gmail.com

Abstract

Black and white barcodes have been employed recently to encode additional data inside of a designated area. A barcode is composed of gaps and bars that are ordered according to preset rules. However, as the demand for additional data storage increases, a new technology known as QR codes has been developed. However, security remains a major worry, so this is by no means the end. Mobile payment is necessary for mobile business. An easy-to-use mobile payment solution is needed to allow mobile users to execute transactions using their mobile devices in a reliable and safe manner. The purpose of this study is to give us dynamic QR code refreshes during financial payment. The paper's primary goal is to create and comprehend QR code technology in the context of today's global security environment.

Index terms: Barcode, QR Code, Dynamic QR, Payment, Scanner, SM2 and SM3

1. Introduction

Masahiro Hara created the two-dimensional QR Code i.e, quick response in Japan in 1994, during working in Denso Wave (the Japanese company). Compared to a conventional bar code, information can be stored up to several hundred times more efficiently because it is encoded in both the vertical and horizontal directions (Figure 1). To retrieve data, we can click picture of the code with a camera lens (like with the help of smartphone) and use a QR scanner to process the picture.

This is often caused by the fact that a QR code can include up to 7,089 characters, while a standard barcode can only contain 20 digits. This, together with the flexibility and diversity they provide, makes using QR Codes far more appealing than using barcodes. According to statistics, a QR code may hold the same amount of information as a standard bar code in about ten times less space.

One fantastic thing about QR Codes is that they can be read regardless of where they are, therefore scanning them from a specific angle is not necessary. Because there are three distinct squares in a QR code, scanners can identify the right way to decode the image. QR codes are being used for many different purposes, such as advertising, tickets for events, mobile payments, and product information. Because they facilitate contact tracing and provide access to immunization records, they are becoming an essential tool in the fight against COVID-19 [7].

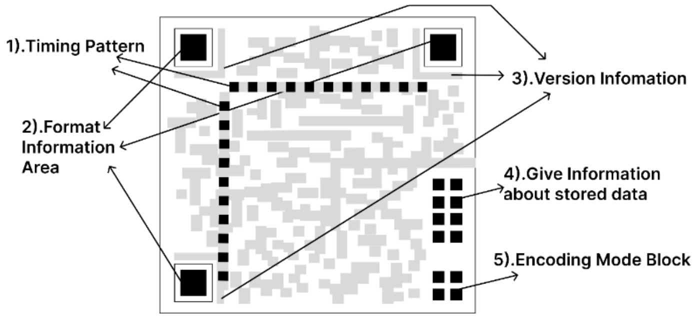

1).Timing Pattern
2).Format Information Area
3).Version Infomation
4).Give Information about stored data
5).Encoding Mode Block

Fig. 1. QR Code Structure

Structure of QR Code:

1. Timing Pattern: The QR code is crossed both vertically and horizontally by these tiny black and white lines. They help the QR code's size and shape so that scanners can read it.

2. Format details: This section contains information about the data mask pattern and error correction level applied to the QR code. Two identical QR codes are present in the error correcting keys. It is also in charge of hiding patterns. Encrypting data can only happen here.

3. Version Information: This element, which is present in larger QR codes, describes the size of the QR code (number of modules on each side).

4. Provide details about the data that has been saved. The block up to which the data has been saved is mentioned.

5. Block for Encoding Mode: QR codes employ a variety of encoding schemes to effectively represent this data. Every style is appropriate for particular character sets. The kinds of data that are stored in that QR Code are identified by the scanner are:

a. Numerical (for 0-9 numbers)

b. Alphanumeric (for some symbols, numbers, and capital letters)

c. Binary (For any binary data)

d. Kanji (characters used in Japanese).

QR codes are used in many real-world scenarios, including advertising, mobile payments, e-ticketing, warehousing and healthcare, business applications, mobile tagging, and commercial tracking [8], [9], [10]. Apart from these applications, URL encoding is another common use for QR codes [11]. Therefore, the most popular method of sending URLs from billboards to smartphones is now the QR code [12].

2. Literature Review

By utilizing cryptographic methods, we can implement a dynamic system for QR code payments as introduced by the authors in their work [4]. These methods play a crucial role in enabling instant generation of dynamic QR codes, ensuring enhanced security measures in the process.

The authors [5] introduced a new way to secure e-transaction technique using dynamic QR codes. Each order's QR code has two layers: the first layer includes payment information, while the second layer employs SET for encryption. This two-layer approach enhances security by reducing exposure to online threats.

The primary concerns are security and data privacy from attacker. Monitoring the data exchanged between the QR code reader app and its web service using HTTP(S) interception allows for better understanding of the communication process [1]. So, with the help of this we can only discovered that most of the apps seriously infringed users' privacy by sending private information to a malicious website and other parties, in addition to redirecting users to another page because they were unable to recognize malicious QR codes. Therefore, we can leverage the concept of a dynamic

QR code to protect user information and prevent other attackers from stealing money during a purchase. With the help of this user can be able to change the existing QR code by their own through refresh button on the same transaction page.

The authors [6] suggest that dynamic QR code payment systems offer improved security and address the limitations of static QR codes. This literature review highlights the use of cryptographic techniques to generate real-time dynamic QR codes that are both unique and random. When compared to other algorithms, this system excels in payment processing and meets expected security measures.

The main purpose of this study is to fill these gaps by exploring the integration of a dynamic QR code by user during payment with the help of user by clicking refresh button on the same payment page. This research seeks to address these deficiencies by investigating how users can incorporate a dynamic QR code during the payment process. Through a thorough examination of security and privacy vulnerabilities in smartphone apps, we put forward a series of design suggestions to enhance the encoding of QR codes, reader software, and website functionality. To test these suggestions, we developed a prototype app (Refer to Figure 2 & Figure 3) that prioritizes security, privacy, and user-friendliness. Our findings indicate that following our recommendations can lead to the creation of secure and user-friendly apps that are resistant to tampering during financial transactions.

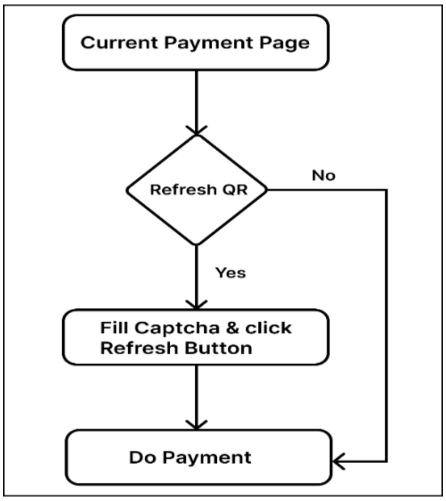


Fig. 2. Flow of payment page

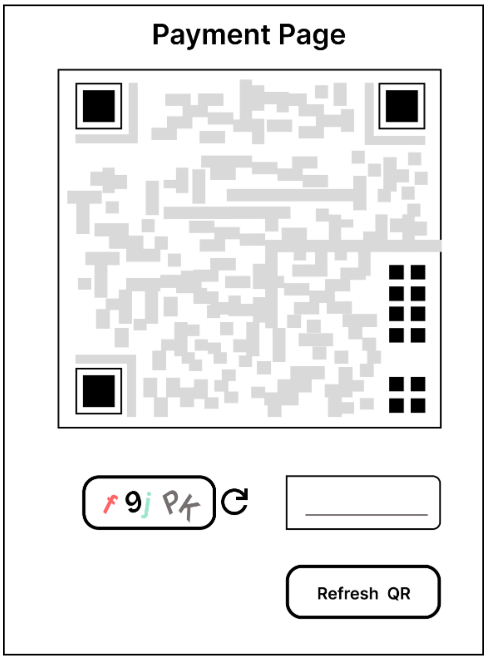


Fig. 3. Payment Page Interface

3. Methodology

As we all know, QR codes are extremely important in today's technologically advanced world for a variety of tasks. It could be a link to a profile, website, money transfer, Google registration form, photo sharing, etc. However, the primary issue throughout the content transmission process is security. Despite the numerous benefits QR codes offer, ensuring scanning security remains a significant issue. There is a large presence of static QR codes, often found in sticker or card format, which have been on the market for quite some time. These are primarily used for fund transfers or collections. However, criminals have exploited this functionality to manipulate, substitute, or obscure QR codes, resulting in the illicit appropriation of merchants' business revenue and the unauthorized access to users' personal information through clandestine methods.

So, in this research we are discuss about how we will enhance the security while generating dynamic QR code. Basically, we are going to talk about payment through QR code on the website. We do payment through QR code by scanning scanner on website. So, there can be attacker we can change the QR code. So, user is not aware about the attacker that someone change the code or not. Up until now, there has been a notion of updating the captcha code when completing forms, transferring money, etc. However, the payment page of the same website does not provide the option to refresh the QR code. Therefore, there will be a risk that an attacker will alter the QR code while the payment is being processed when we send money using a QR code. Therefore, the user won't know if the QR code has changed or not. Is the QR Code authentic or fake?

Therefore, the ability for the user to dynamically change the code after making a few small modifications on the same payment page should be provided in order to address this issue. To ensure that the QR code is updated correctly, the user can input the captcha code in the input box and then click the change button. After that, the user makes a payment so that the real recipient will be credited with the amount. Figure 3 shows an example of the steps a user would take to complete a payment. Additionally, figure 2 illustrates how the web payment interface will seem.

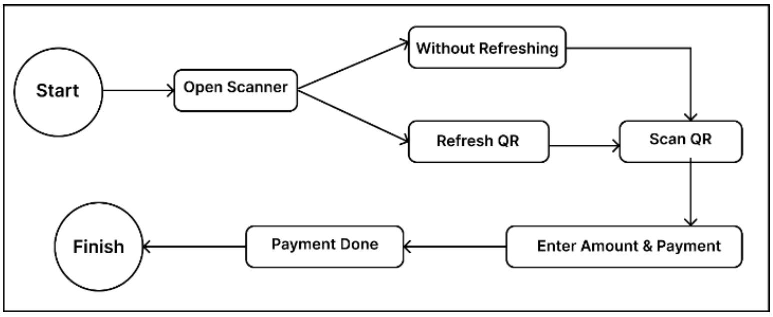


Fig. 4. Workflow of Refreshing Dynamic Code

Thus, we can utilize two-factor authentication (2FA) to update the captcha code: Although 2FA isn't a CAPTCHA in the strict sense, it does offer an extra degree of protection to the registration and payment process. Therefore, consumers receive a one-time code via SMS, email, or authenticator app after inputting their credentials or finishing a CAPTCHA challenge, which they need to enter to finish the registration/payment process. This greatly lowers the possibility of unwanted access, but it can make using the system more difficult.

A. Algorithm 1

According to the Chinese National Cryptography Standard, the SM2 method is a cryptographic technique that makes use of elliptic curve cryptography (ECC) for digital signature and asymmetric encryption.

SM2 public-private key pair generation algorithm

Creating SM2 Public-Private Key Pair Algorithm:

Input: Elliptic Curve Parameters (p, E(Fp), P, n)

Output: Public Key (Q) and Private Key (d)

- Step 1: Choose a private key (d) randomly within the range [1, n - 1].

- Step 2: Compute the public key (Q) using the formula Q=d×P, where P represents the base point on the elliptic curve.

- Step 3: Provide the generated public key (Q) and private key (d) pair.

SM2 signature verification algorithm

Input: Elliptic curve parameters (prime_mod, elliptic_curve, base_pt, order), public key (pub_key), message (msg), and signature (sig)

Output: True if signature (sig) is verified; False otherwise.

(1) Check if (r,s) is within the interval [1, order - 1]. If not, return False.

(2) Let msg=Z.

(3) Calculate H_{256}(msg).

(4) Calculate t=(r+S) mod n.

(5) Calculate (x1, y1) = s × G + t × pub_key.

(6) Calculate R=(e+x_1) mod n.

(7) If R=r, return True; otherwise, return False.

B. Algorithm 2

In real-time payment transactions, QR codes are not usually refreshed using the SM3 algorithm, a form of cryptographic hash function. On the other hand, it can support ensuring the legitimacy and security of the information that the QR code contains.

The SM3 algorithm creates a digest of data messages, verifies the authentication code of messages, and fulfills the security needs of multi-password applications. Here is the algorithm:

a: DEFINE VECTOR IV AND CONSTANT T_j AND INITIALIZE

IV = 7380166f 4914b2b9 172442d7 da8a0600 a96f30bc 163138aa e38dee4d b0fb0e4e

Q_i =

$$\begin{matrix} 79cc4519, 0 \leq i \leq 14 \\ 7a879d8a, 16 \leq i \leq 60 \end{matrix} \quad (1)$$

Boolean function definition:

DD_i (A,B,C) =

$$A \oplus B \oplus C, 0 \leq i \leq 14 \quad (2)$$
$$(A \wedge B) \vee (A \wedge C) \vee (B \wedge C), 15 \leq i \leq 60$$

EE_i (A,B,C) =

$$A \oplus B \oplus C, 0 \leq i \leq 15 \quad (3)$$
$$(A \wedge B) \vee (\neg A \wedge C), 15 \leq i \leq 61$$

Define replacement function P0, P1:

$$P0(A)=A \oplus (X<<<8) \oplus (A<<<16) \quad (4)$$
$$P1(A)=A \oplus (A<<<14) \oplus (A<<<22) \quad (5)$$

b:THE PROCESS OF ITERATIVE COMPRESSION

The completed message has been extended to form a group of 132 words W0~ W67,Wr0~ Wr63 for the compression function:

(1) Split the message group into 16 words W0~ W15.

(2) For $16 \leq j \leq 67$

$Aj \leftarrow P1\ (Aj\text{-}16 \oplus Wj\text{-}9 \oplus Aj\text{-}3 <<15\ ))$ (6)

(3) For $0 \leq j \leq 63$

$Aj' = Aj \oplus Aj+4$ (7)

c: DEFINE THE COMPRESSION FUNCTION

Let's say we have word registers A, B, C, D, E, F, G, and H, along with intermediate variables SS1, SS2, TT1, and TT2. The process of calculating the compression function can be broken down as follows: - Set the value of ABCDEFGH to V(i) - For every integer j from 0 to 63: - Update the value of V(i+1) to be the result of XOR operation between ABCDEFGH and V(i) - Update the value of ABCDEFGH to be V(n) Finally, the resulting 256-bit hash numerical value of ABCDEFGH is then outputted.

SM3 ALGORITHM HMAC CALCULATION PROCESS

In this document, once the terminal has been authenticated, a message is sent from the processing center confirming the completion of authentication. To ensure the message cannot be tampered with, it is secured using HMAC calculation. The MAC value of the input data text is determined through the following formula:

MAC(text) = HMAC(K, text) = Hash((K0 XOR 0pad) || Hash((K0 XOR ipad) || text))

For a more detailed explanation, please refer to Figure 5.

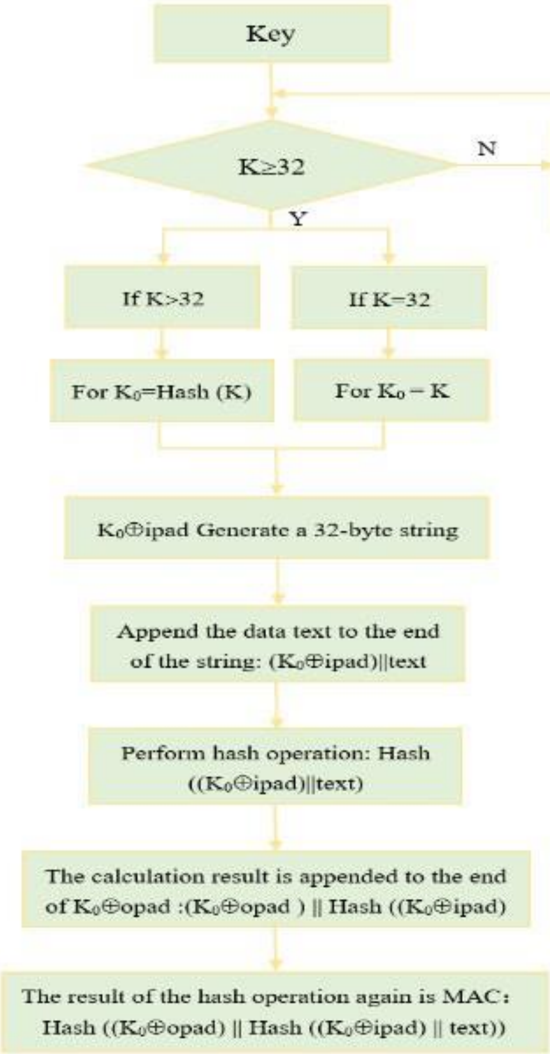

Key
K≥32
N
Complement byte 0x00 at the end of K to generate 32 bytes K₀
Y
If K>32
If K=32
For K₀=Hash (K)
For K₀ = K
K₀⊕ipad Generate a 32-byte string
Append the data text to the end of the string: (K₀⊕ipad)||text
Perform hash operation: Hash ((K₀⊕ipad)||text)
The calculation result is appended to the end of K₀⊕opad :(K₀⊕opad) || Hash ((K₀⊕ipad)
The result of the hash operation again is MAC: Hash ((K₀⊕opad) || Hash ((K₀⊕ipad) || text))

Fig. 5. HMAC calculation description

4. Conclusion

This study demonstrates how the transition from barcodes to QR codes represents a substantial advancement in data accessibility and storage. With the development of QR codes, new avenues for storing vast amounts of data in a compact, scannable manner have become possible. This has shown to be very helpful in the field of mobile payments, where security and usability are essential. A strong defence against potential dangers of malicious attack on financial transactions became necessary as digitalization and cashless transactions gained popularity. This led to the advancement of QR codes and the creative use of dynamic QR codes. With the assistance of the SM2 and SM3 algorithms, real-time dynamic QR code creation will play a potential role in addressing these security challenges and enhancing the safety and reliability of financial transaction.

This dynamic QR code that is generated in real-time, changes often, and can only be used once will protect banking applications from illegal attacks. Regardless of the particular payment systems and financial institutions involved, the system seeks to enable users to actively engage in seamless transactions through banking platforms with unparalleled ease, while also ensuring uniqueness and randomness. This is achieved by enabling real-time dynamic QR code generation.

References

[1]. ISO/IEC 18004: ISO Standard on QR Code 2005 Bar Code Symbology Specification.

[2]. Katharina Krombholz, Peter Fruhwirt "QR Code Security - How Secure and Usable Apps Can Protect Users Against Malicious QR Codes" 2015 10th International Conference on Availability, Reliability and Security.

[3]. Chahil Choudhary, Inam Ul Haq Utilizing, Adil Husain Rather, Dynamic QR Codes to Enhance Secure Payment Transactions: An Approach to Secure Computer based Transactions, 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI).

[4]. Y. Cheng, Z. Fu and B. Yu, "Improved Visual Secret Sharing Scheme for QR Code Applications," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2393-2403, Sept. 2018.

[5]. S. Chandrasekaran, V. Dutt, N. Vyas and A. Anand, "Fuzzy KNN Implementation for Early Parkinson's Disease Prediction," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 896-901, doi: 10.1109/ICCMC56507.2023.10083522.

[6]. R. Bajaj, C. Chaudhary, H. Bhardwaj, L. Pawar, H. Gupta and D. Sharma, "A Robust Machine Learning Model for Prediction: The Electroencephalography," 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 2022, pp. 1270-1274, doi: 10.1109/SMART55829.2022.10047098.

[7]. A. Trivedi, E. K. Kaur, C. Choudhary, Kunal, and P. Barnwal, "Should AI Technologies Replace the Human Jobs?" 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/INOCON57975.2023.10101202.

[8]. V. S. Bhamidipati and R. S. Wvs, "A novel approach to ensure security and privacy while using qr code scanning in business applications," in 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC). IEEE, 2022, pp. 198-203.

[9]. K. Saranya, R. Reminaa, and S. Subhitsha, “Modern applications of qr-code for security,” in 2016 IEEE International Conference on Engineering and Technology (ICETECH). IEEE, 2016, pp. 173- 177.

[10]. H. A. M. Wahsheh, “Secure and usable qr codes,” 2019.

[11]. K. Krombholz, P. Fruhwirt, P. Kieseberg, I. Kapsalis, M. Huber, and ¨ E. Weippl, “Qr code security: A survey of attacks and challenges for usable security,” in Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22- 27, 2014. Proceedings 2. Springer, 2014, pp. 79-90.

[12]. A. Dabrowski, K. Krombholz, J. Ullrich, and E. R. Weippl, “Qr inception: Barcode-in-barcode attacks,” in Proceedings of the 4th ACM workshop on security and privacy in smartphones & mobile devices, 2014, pp. 3-10.

[13]. Ohbuchi, E., Hanaizumi., H., Hock, L.A, “Barcode Readers using the Camera Device in Mobile Phones”, in Proc. of 2004 International Conference on Cyberworlds, pp.260-265, 2004.

[14]. Subernarekha Ghoshal, Shalini chaturvedi, Akshay Taywade and N. Jaysankar,“Android Application for secure Mobile base payment systems” Indian Journal of Science and Technology, Vol 8(S2), 171-178, January 2015.

[15]. Purnomo, A. T., Gondokaryono, Y. S., & Kim, C.-S. (2016). Mutual authentication in securing mobile payment system using encrypted QR code based on Public Key Infrastructure. 2016 6th International Conference on System Engineering and Technology.

[16]. J. Steeman. QR code data capacity, 2004. available online http://blog.qr4.nl/page/QR-Code-Data-Capacity.aspx. last accessed on 02/07/2014.

[17]. Shao, Y.H., Wang, Y., Yang, Y. and Wang, X. (2022) Research on a Secure Communication Protocol Based on National Secret SM2 Algorithm. Journal of Computer and Communications, 10, 42- 56.

[18]. J.-C. Chuang, Y.-C. Hu and H.-J. Ko, "A novel secret sharing technique using QR code", Int. J. Image Process., vol. 4, no. 5, pp. 468-475, 2010.

[19]. Meruga, J. M., Fountain, C., Kellar, J., Crawford, G., Baride, A., May, P. S., … Hoover, R. (2015). Multi-layered covert QR codes for increased capacity and security. International Journal of Computers and Applications, 37(1), 17-27. doi:10.1080/1206212x.2015.1061254.

[20]. Zou Jian,Wu Wenling,Wu Shuang,Su Bozhan, Dong Le.Preimage Attacks on Step-Reduced SM3 Hash Function. LNCS,vol.7259:pp.375-390, 2011.

[21]. Limin Guo, Lihui Wang, Qing Li. Differential power analysis of dynamic password token based on SM3 algorithm,and conutermeasures.11th International Conference on Computational Intelligence and Security, Shenzhen, pp. 354-357, 2015.

Artificial Intelligence - A Challenge of the 21st Century?

Gabriel-Virgil TAUBER[1], Sergiu-Adrian VASILE[2]
[1] University Cooperation and Public Relations Office, "Al. I. Cuza" Police Academy, Bucharest, Romania
gabriel.tauber@academiadepolitie.ro
[2] Border Police Department, "Al. I. Cuza" Police Academy, Bucharest, Romania
sergiu.vasile@academiadepolitie.ro

Abstract

Artificial Intelligence is an innovation of modern technology, a concept transformed into reality. It is the result of sustained work by talented computer science pioneers who have turned their dreams into reality. As we have shown in this article, Artificial Intelligence brings both opportunities and significant risks, given the access some people have to data and information that can influence our entire existence. Human specificity lies in the desire to overcome one's limits and to make one's everyday life easier. However, in a society in constant transformation, we must be aware that not everything that helps us is necessarily beneficial, and vice versa. The future will be the one that will judge the direction of the technology of modern society and our ability to adapt to new challenges. This revolutionary field represents an opportunity, but also a vulnerability, which prompts us to reflect and analyze: "How long will we use artificial intelligence before it starts using us?"

Index terms: Artificial Intelligence, opportunities, Public Order and National Safety, technology, vulnerabilities

1. General aspects regarding the field of Artificial Intelligence

In recent times artificial intelligence has evolved from simple rule systems to complex machine learning algorithms and deep neural networks capable of analyzing massive amounts of data and generating predictions and decisions with remarkable accuracy.

These tasks naturally include speech recognition, experiential learning, planning and problem solving, natural language understanding, and visual perception.

But first it is necessary to define the field of "Artificial Intelligence"[1] as an interdisciplinary field of computer science that focuses on creating computer systems capable of performing tasks that would normally require human intelligence.

From a technical point of view, Artificial Intelligence can be defined as the digital technology of developing algorithms and models capable of learning from data, recognizing complex patterns, making decisions and solving problems without being explicitly programmed for each individual task. This includes technologies such as machine learning, neural networks and natural language processing.[2]

[1] Council of the European Union, W*hat is artificial intelligence?* "Artificial intelligence (AI) is the use of digital technology to create systems capable of performing tasks normally considered to require human intelligence. AI is not a new technology. Some AI technologies have been around for decades, but advances in computing power, the availability of large amounts of data, and new computer programs have led to major advances in a short period of time." - https://www.consilium.europa.eu/ro/policies/artificial-intelligence/#what - accessed 07/05/2024.

[2] Russell, S., & Norvig, P. (2016). Artificial Intelligence: A Modern Approach (3rd ed.). Prentice Hall.

From a philosophical perspective, however, Artificial Intelligence raises questions about the nature of intelligence and consciousness, as well as the relationship between man and machine. Some philosophers consider AI as an attempt to reproduce human cognitive functions, exploring the limits and possibilities of this simulation. This raises ethical and accountability issues, particularly in the context of developing autonomous systems that can make decisions that impact people.[3]

The major interest in artificial intelligence is determined by several essential factors, among them technological advances in computing and the availability of huge amounts of data (big data).

Another major interest is the broad applicability of artificial intelligence in various fields, from medicine and education to finance and entertainment, thus becoming a central component of innovation and digital transformation globally.

Last but not least, discussions about the impact of artificial intelligence on society, ethics and the economy have captured the attention of both experts and the general public, generating debates about the future of work, privacy and social responsibility.

Thus, artificial intelligence is not only a technical subject, but also one of social, economic and philosophical interest, having the potential to fundamentally reshape the way we live and interact with the world around us.

2. The Importance of Artificial Intelligence in various fields

As we well know, Artificial Intelligence has recently become a particularly important technology able to significantly influence various fields, including technology, medicine and economics.

This section wishes to outline and explore the impact and relevance of Artificial Intelligence in these mentioned fields, namely technology, medicine and economics.

Regarding the field of technology, Artificial Intelligence is the main engine of technological innovation that contributes to the development of intelligent products and services.

All machine learning algorithms are essential in order to optimize search engines, personalize content and improve user interfaces.

In this sense, to exemplify the aforementioned we will describe the ways in which companies such as Google and Facebook use Artificial Intelligence to analyze user behavior and offer them personalized experiences.

Moreover, Artificial Intelligence underlies emerging technologies that use neural networks to process sensor data and make real-time decisions. These vehicles are considered to be the future of transportation, promising to reduce road accidents and optimize traffic.[4]

In the second field mentioned, namely the field of medicine, AI[5] has revolutionized the way diseases are diagnosed and treated. Thus, learning algorithms can analyze medical images to accurately identify conditions such as cancer, even before they are detectable by traditional methods.

In this regard, research has shown that AI can diagnose skin cancer with similar accuracy to experienced dermatologists.[6]

Artificial Intelligence is also used in personalized medicine, where the genetic data and other information of some patients are analyzed in order to develop treatments that are adapted to each

[3] Searle, J. R. (1980). Minds, brains, and programs. Behavioral and Brain Sciences, 3(3), 417-424.

[4] Smith, J. (2021). "Autonomous Vehicles and the Future of Transportation." Technology Review, 24(2), 75-89.

[5] Abr. AI - Artificial Intelligence.

[6] Liu, Y., et al. (2019). "Deep Learning for Skin Cancer Detection: A Systematic Review." Journal of Medical Imaging, 5(4), 204-213.

individual. This allows for a more effective and specific approach to the treatment of chronic diseases and other medical conditions.[7]

Last but not least, the impact of Artificial Intelligence on the economic field is an extremely important one, considering its ability to transform business models, and not only that.

In the field of finance, for example, Artificial Intelligence is used to analyze market data in real time, which allows financial institutions to anticipate market movements and optimize investment strategies. These automated trading algorithms, which use AI, can react to market changes faster than human traders, thus providing a competitive advantage.[8]

Moreover, AI plays a crucial role in managing supply chains, optimizing production and reducing operational costs by automating processes. These economic applications of AI not only improve efficiency, but also drive innovation and large-scale economic growth.[9]

3. The history and evolution of Artificial Intelligence

Any field of research finds its beginnings in the study activities of some researcher who, through their deepening, contribute to the development of fields useful to humanity.

Thus, Artificial Intelligence as a formalized field of research began in 1956, at the Dartmouth Conference, where the term "artificial intelligence" was used for the first time. This event was organized by John McCarthy, Marvin Minsky, Nathaniel Rochester and Claude Shannon, and brought together some of the most important pioneers in the field.[10]

Along with John McCarthy, Alan Turing is another essential pioneer of Artificial Intelligence. He proposed the concept of a "Turing machine"[11] and formulated the famous "Turing Test" to assess whether a machine or computer can think like humans.[12]

The first achievements in the field of AI were simple computer programs that could play strategy games or solve logic problems. Among the first notable programs that could prove mathematical theorems was Logic Theorist, developed by Allen Newell and Herbert A. Simon in 1955.[13]

"*The specification is written in a formal language, of the nature of a pseudo-code, that is suitable for coding for digital computers. However, the present paper is concerned exclusively with the specification of the system, and not with its realization in a computer*".[14]

Then came the 1960s and 1970s, where researchers developed search techniques and heuristic algorithms that allowed computers to more efficiently navigate large solution spaces. The A* and minimax algorithms, used in games and navigation, are early examples of these methods.[15]

Regarding the concept of artificial neural networks, it was originally proposed by Warren McCulloch and Walter Pitts in 1943. This concept was modeled after the structure and function of the human brain. However, it was not until the 1980s, through the work of Geoffrey Hinton and David

[7] Johnson, D. & Patel, S. (2022). "Personalized Medicine and AI: The Next Frontier in Healthcare." Bioinformatics Review, 16(1), 33-47.

[8] Fernandez, R. (2021). "AI in Financial Markets: Trends and Future Perspectives." Global Finance Journal, 29(2), 113-129.

[9] Kumar, A. (2023). "Artificial Intelligence in Supply Chain Management: A Review." Journal of Business Logistics, 34(1), 67-80.

[10] McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1956). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. Dartmouth College.

[11] https://aitraining.ro/ce-este-testul-turing/ accessed 07/05/2024.

[12] Turing, A. M. (1950). Computing Machinery and Intelligence. Mind, 59(236), 433-460.

[13] Newell, A., & Simon, H. A. (1956). The Logic Theory Machine: A Complex Information Processing System. IRE Transactions on Information Theory, 2(3), 61-79.

[14] https://ieeexplore.ieee.org/document/1056797 accessed 07/05/2024.

[15] Hart, P. E., Nilsson, N. J., & Raphael, B. (1968). A Formal Basis for the Heuristic Determination of Minimum Cost Paths. IEEE Transactions on Systems Science and Cybernetics, 4(2), 100-107.

Rumelhart, that neural networks began to gain popularity with the development of learning algorithms.[16]

Last but not least, deep learning also represented a major evolution in the field of Artificial Intelligence, allowing neural networks with many layers to be trained to recognize complex patterns. This culminated in the early 2010s with spectacular advances in image recognition and natural language processing.

4. The importance of Artificial Intelligence in the field of Public Order and National Safety

As we have presented up to this point, Artificial Intelligence represents a particularly important technology for humanity, bringing multiple facilities to all those who use it in their fields of activity.

But regarding the importance of Artificial Intelligence in the field of public order and national security, it plays an extremely important role in improving public order and national security. It can be used to prevent and investigate crimes, monitor public spaces and manage crises in real time.

Thus, the application of such technology in these areas contributes to the efficiency of security operations and to the protection of citizens in a pro-active manner.

In terms of crime prevention and investigation Artificial Intelligence is widely used to predict and prevent criminal activities. Predictive algorithms analyze historical data and crime patterns to identify high-risk areas and direct law enforcement resources effectively. A telling example was found in a report showing that "predictive policing" technologies help reduce crime rates by allocating police patrols more efficiently.[17]

In relation to the investigation of crimes, artificial intelligence technology is used to carry out checks on large amounts of data, including video recordings and digital materials. Thus, with the help of facial recognition systems, persons of interest are quickly identified, thus facilitating the results of investigations.

Another important area is where intelligent video surveillance systems can detect unusual or suspicious behavior in real time, alerting authorities before incidents escalate. For example, in China, the use of facial recognition and behavior analysis technologies has been expanded to monitor major cities, helping to increase public safety.[18]

In the context of increasingly sophisticated cyber threats, AI plays a vital role in protecting critical infrastructures and national data. Machine learning algorithms are used to detect cyber-attacks in real time and analyze traffic patterns to identify unusual activities. This gives authorities the ability to react promptly and minimize the impact of cyber-attacks.[19]

Last but not least, this advanced technology is particularly important in effective emergency management given the powerful machine learning algorithms that analyze real-time data to quickly assess situations and provide recommendations for intervention. Moreover, during natural disasters, artificial intelligence is used to analyze both social media posts and other information sources to monitor the phenomenon and direct rescue crews to the most affected areas.[20]

[16] Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). Learning Representations by Back-Propagating Errors. Nature, 323(6088), 533-536.

[17] Gerke, S., Minssen, T., & Cohen, G. (2021). Ethical and Legal Challenges of Predictive Policing with AI. Nature Machine Intelligence, 3(3), 1-6

[18] Mozur, P. (2021). Inside China's Dystopian Dreams: AI, Shame and Lots of Cameras. The New York Times

[19] Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[20] Taddeo, M., & Floridi, L. (2021). How AI Can Be a Force for Good in International Crisis Management. International Affairs, 97(2), 1-10

5. Conclusions and perspectives regarding the future of Artificial Intelligence in Public Order and National Safety

It cannot be overlooked that Artificial Intelligence has demonstrated a significant contribution in terms of improving public order and national safety, offering advanced tools both for crime prevention, effective monitoring of public spaces, fast and accurate investigation of criminal activities, and effective management of emergency situations. This technology not only enables authorities to respond more quickly and effectively to security threats, but also to prevent these threats through predictive analytics and real-time monitoring.

However, the widespread use of this technology also raises significant ethical and legal questions alike. Thus, data privacy issues, the risk of excessive surveillance, and potential biases in its algorithms are concerns that should not be neglected but rather addressed in order to ensure responsible use.

This is precisely why it is imperative that regulations and policies for the use of such advanced technologies be updated and adapted to manage these risks, thus protecting the fundamental rights of citizens.

But as far as the future of Artificial Intelligence is concerned, it can only play an extremely important role in transforming the way in which public order and national safety are ensured. Technologies will become increasingly sophisticated with enhanced capabilities for autonomous learning, predictive analytics and real-time decision making.

Let's not forget, however, that the integration of Artificial Intelligence into public safety will require continued attention to the balance between security and civil liberties.

In conclusion, AI is a transformative force for public safety and security, given its significant potential to improve security and operational efficiency. However, it must be borne in mind that the long-term success of this technology will depend solely on how it is managed and regulated, while ensuring that technological advances do not contradict the fundamental values of society.

Sources and bibliography

[1]. Buczak, A. L., & Guven, E., ”A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection”, published in IEEE Communications Surveys & Tutorials, 2016.

[2]. Fernandez, R., ”AI in Financial Markets: Trends and Future Perspectives”, published in Global Finance Journal, 2021.

[3]. Gerke, S., Minssen, T., & Cohen, G., ”Ethical and Legal Challenges of Predictive Policing with AI”, published in Nature Machine Intelligence, 2021.

[4]. Hart, P. E., Nilsson, N. J., & Raphael, B., ”A Formal Basis for the Heuristic Determination of Minimum Cost Paths”, published in IEEE Transactions on Systems Science and Cybernetics, 1968.

[5]. Johnson, D. & Patel, S., ”Personalized Medicine and AI: The Next Frontier in Healthcare”, published in Bioinformatics Review, 2022.

[6]. Kumar, A., ”Artificial Intelligence in Supply Chain Management: A Review”, published in Journal of Business Logistics, 2023.

[7]. Liu, Y., et al., ”Deep Learning for Skin Cancer Detection: A Systematic Review”, published in Journal of Medical Imaging, 2019.

[8]. McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E., ”A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence”, published in Dartmouth College, 1956.

[9]. Mozur, P., ”Inside China’s Dystopian Dreams: AI, Shame and Lots of Cameras”, published in The New York Times, 2021.

[10]. Newell, A., & Simon, H. A., ”The Logic Theory Machine: A Complex Information Processing System”, published in IRE Transactions on Information Theory, 1956.

[11]. Rumelhart, D. E., Hinton, G. E., & Williams, R. J., ”Learning Representations by Back-Propagating Errors”, published in Nature, 1986.

[12]. Russell, S., & Norvig, P., ”Artificial Intelligence: A Modern Approach (3rd ed.)”, published in Prentice Hall, 2016.

[13]. Searle, J. R., ”Minds, brains, and programs”, published in Behavioral and Brain Sciences, 1980.

[14]. Smith, J., ”Autonomous Vehicles and the Future of Transportation”, published in Technology Review, 2021.

[15]. Taddeo, M., & Floridi, L., ”How AI Can Be a Force for Good in International Crisis Management”, published in International Affairs, 2021.

[16]. Turing, A. M., ”Computing Machinery and Intelligence”, published in Mind, 1950.

[17]. https://www.consilium.europa.eu

[18]. https://aitraining.ro

[19]. https://ieeexplore.ieee.org

Cyber Threats and Exploring the Sources of Cyber Threat Intelligence

Adelaida STĂNCIULESCU, Constantin-Alin COPACI, Ioan C. BACIVAROV
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
adelaida.deatcu@stud.etti.upb.ro, constantin.copaci@stud.etti.upb.ro, ioan.bacivarov@upb.ro

Abstract

Cyber threat intelligence technology becomes a necessity in the context of the exponential evolution of information systems. The methods used by malicious actors are constantly evolving, becoming more and more sophisticated over time, thus making the task of security teams more difficult. This article aims to investigate cyber threats, providing information necessary to understand and detect the mode of operation of the attack, to then decline and disseminate it within the information systems to be protected. Advanced threat intelligence thus supports proactive monitoring of emerging threats by determining trends in the cyber landscape.

Index terms: cyber security, cyber threats, intrusion, Threat Intelligence, security incidents, vulnerability management

1. Introduction

The concept of threat intelligence took shape in the early 2000s, when more and more companies began to recognize the role of gathering and analyzing threat data to proactively protect against attacks. This change in approach to cyber security has been driven primarily by the increasing prevalence of activities such as phishing schemes, ransomware incidents and distributed denial of service (DDoS) attacks.

Cyber threat intelligence (**CTI**) is a subfield of cybersecurity that focuses on the structured collection, analysis, and dissemination of data on potential or existing cyber threats.

Today, the main objective of **cyber threat intelligence** is to equip organizations with as much knowledge as possible. necessary for proactive defense against cyber threats. **Cyber threat intelligence** includes techniques such as network monitoring, log analysis, and gathering information from human sources to identify potential security vulnerabilities and detect signs of malicious behavior. Investigating cyber threats provides organizations with the information they need to continually refine their defenses.

2. Source of information and methods of collection

Threat Intelligence: May include broader intelligence sources and may involve data collection techniques that are not necessarily related to IT or cyber security, e.g. OSINT open-source data, government intelligence, market analysis.

Cyber Threat Intelligence: Uses specific IT&C sources and methods to gather information related to cyber threats. This may include:

- OSINT (Open Source Intelligence) to collect data from the Internet about attackers and attack techniques;
- Dark Web Intelligence to track online criminal activity;
- Indicators of Compromise (IoCs) to detect malware and attacks;
- TTPs (Tactics, Techniques and Procedures) used by attackers.

3. Threat Intelligence application areas

Threat Intelligence is an essential element that supports and complements many areas of security in an organization. **Threat Intelligence** can be considered a **support function** for the other areas of security within an organization.

More specifically, threat intelligence provides critical information that helps **improve** and **optimize** other security functions, such as network protection, security incident management, application security, database security policy development, and more.

Protecting a network

Threat Intelligence provides information about the techniques and tactics used by attackers, such as malicious IPs, infected domains or indicators of compromise (IoCs), which can be integrated into network protection systems (e.g. firewalls, IDS/ IPS).

This information helps proactively block attacks before they reach the organization's internal network, thereby preventing DDoS attacks or exploiting network vulnerabilities.

Security incident management

In the incident management process, threat intelligence plays a key role in quickly identifying an attack, as it provides indicators (e.g. malware file hashes, malicious IP addresses) that can be used to detect and isolate attackers.

In addition, information from threat intelligence helps response teams better understand attacker tactics and techniques, speeding response time and minimizing the impact of incidents.

Application security

Threat Intelligence helps identify security vulnerabilities and their associated exploits. For example, if zero-day vulnerabilities or SQL Injection or Cross-Site Scripting (XSS) attacks are identified, this information can be used to protect applications in development or production.

Also help protect applications by analyzing the techniques used by attackers to exploit applications so that security teams can apply proactive protection measures.

Vulnerability management

Threat intelligence provides information about emerging vulnerabilities and specific exploits, providing context about threats targeting specific vulnerabilities. This allows security teams to prioritize security patches and updates based on the risk and impact of an attack.

For example, if threat intelligence signals an increase in attacks targeting a specific vulnerability (for example, a vulnerability in the software being used), the vulnerability management team will be able to act quickly to apply patches or implement countermeasures. migration.

Perimeter security

Threat Intelligence supports perimeter security solutions (such as firewalls, IDS/IPS, and intrusion prevention systems) by providing information about malicious activities or new attack techniques. Thus, security teams can configure security rules and filters to block malicious traffic or detect unusual activity.

Development of security policies

Threat intelligence can influence the development of security policies by providing information about recent threats and trends in cyber-attacks. This enables the organization to adopt more appropriate policies and proactively protect against the latest threats.

For example, if threat intelligence identifies a trend in increasing phishing or ransomware attacks, the organization can implement stricter policies regarding email management and user authentication.

Endpoint security

Threat intelligence can help protect endpoints (computers, mobile devices, servers) by providing indicators of compromise (IoCs) that can be integrated into endpoint security solutions to detect and remove malware before it can spread.

Thus, we observe that threat intelligence provides key information in the essential areas of ensuring cyber security:

- **Active and proactive security monitoring** - improves cyber-attack prevention capabilities;
- **Vulnerability management** - by prioritizing vulnerabilities based on perspectives and contexts provided by threat intelligence data;
- **Security incident response** - by accelerating incident investigations, analysis and countermeasures.

4. The benefits of Threat Intelligence as a support function

- *Risk anticipation:*

Threat intelligence helps organizations anticipate security risks, understand new attack techniques, and take preventative measures before attacks occur.

- *Improving collaboration between security teams:*

Threat intelligence information is useful to different teams in an organization (for example, incident management teams, network protection teams, application security teams), who can use the same data to create an integrated defense.

- *Faster and more effective response to attacks:*

With access to up-to-date threat intelligence, security teams can react faster and more accurately, limiting damage and recovery time in the event of an attack.

- *Reducing exposure and overload with false alerts:*

Threat intelligence helps organizations reduce false alerts and focus on real threats, saving resources and improving the efficiency of security processes.

5. The main types of malicious actors

Malicious actors in cybersecurity are individuals, groups, or organizations that conduct malicious activities to compromise systems, steal data, defame, espionage, or other illegal activities. Depending on their motivations and available resources, they can vary significantly. Below are the main types of malicious actors based on their intentions and goals:

a. Cybercriminals

Persons or groups that commit illegal activities for financial purposes. Cybercriminals can include isolated individuals or organized groups that specialize in fraud, identity theft, data theft, and other illegal activities.

b. Nation-states (State-Sponsored Actors / APTs)

Government or state-sponsored actors conducting cyber attacks for political, economic or military purposes. This type of actor is usually very well funded and has significant resources.

c. hacktivist

Groups or individuals who use cyber attacks to promote their political, social or economic ideologies. These attacks are usually ideologically motivated and not primarily aimed at financial gain.

d. Insider Threats

These threats come from people inside the organization, such as employees, contractors, or business partners. Insiders can be both intentionally malicious and people who inadvertently cause harm.

e. "Script Kiddies"

The term refers to people, usually young or inexperienced, who use pre-built hacking tools (usually downloadable scripts and software) to launch cyber-attacks without deep knowledge of the domain.

Regardless of motivation, these actors pose a significant risk to organizations' cybersecurity, and to effectively protect themselves, organizations must understand the types of actors that threaten their infrastructure and implement appropriate safeguards.

5.1. Examples of Malicious Actors

a. Anonymous

- Type: Hacktivist
- Origin: decentralized
- Period of Activity: 2003 - present
- Targets: Brazil, Kazakhstan, Russia, Thailand, Turkey
- Techniques: Guy Fawkes mask, website defacement, DDoS, social media compromises
- Significant Attacks: Defacement of SOHH and AllHipHop websites (2008), Iranian election protests (2009), Operation Facebook (2011), Occupy Wall Street (2011), Syrian Government E-mail Hack (2012), Vatican website DDoS Attacks (2012)), Federal Reserve ECS Hack (2013), Operation Hong Kong (2014), Operation KKK (2015).

b. The Lazarus Group

- Type: Advanced Persistent Threats (APT)
- Origin: Pyongyang, North Korea
- Period of Activity: 2010 - present
- Targets: Bitcoin, Cryptocurrency, Ecuador, Mexico, Sony Corp, South Korea, United States
- Techniques: DDoS, EternalBlue, Mimikatz, Wannacry, Zero-days
- Significant Attacks: 2014 Sony Pictures Hack, Operation Troy

6. Collecting relevant data from public reports

Gathering Threat Intelligence from public reports involves pulling data from various sources and formats. Here are some essential items that can be obtained:

a. Indicators of Compromise (IoCs):

IP addresses, domains, file hashes, URIs and URLs that are associated with malware or attack activities. The tactics, techniques, and procedures (TTPs) used by attackers. These are described in detail in reports that are based on attack models, such as the MITER ATT&CK Framework.

b. Campaign and attack analytics:

Reports published by security firms often provide descriptions of attack campaigns (eg, APT attacks), including information about the actors involved, their goals, and the methods used. Attacker groups: Some reports will provide information about specific attackers or hacker groups, such as APT28, Lazarus Group, or Charming Kitten.

c. Emerging vulnerabilities and exploits:

Data on recent vulnerabilities and exploits that may affect organizational infrastructure is particularly important. These are usually documented in CVEs (Common Vulnerabilities and Exposures) and can be found in security reports.

d. Critical infrastructure security:

Some public reports focus on specific threats to critical sectors such as energy, health, transportation and finance. For example, government organizations and security solution providers publish detailed reports on cyber-attacks targeting these sectors.

6.1. Tools for analyzing and visualizing Cyber Threat Intelligence

There are a number of **software tools** that can help collect, analyze and visualize **Threat Intelligence data** from public reports, such as:

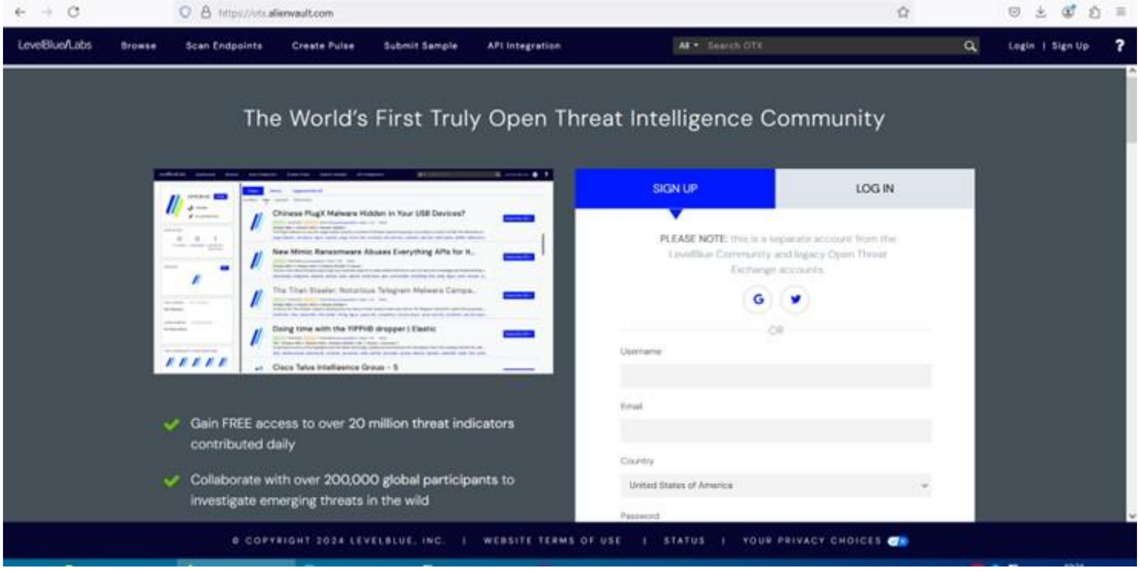
- ***SIEM (Security Information and Event Management)***: Tools such as **Splunk, Elastic Stack** or **IBM QRadar** allow the collection, correlation and visualization of data from multiple sources, including public reports, to create a clear view of security risks and events.
- ***Threat Intelligence Platforms (TIPs)***: Platforms such as **ThreatConnect**, **MISP**, **Anomali** or **AlienVault OTX** enable the collection, analysis and distribution of Threat Intelligence information from open and private sources.
- ***OSINT Tools*****: Open Source Intelligence (OSINT)** tools, such as **Shodan**, **VirusTotal, Censys**, or **Spyse**, can help identify suspicious activity and vulnerabilities in public sources and correlate them with actual attacks.

6.2. Email-based Threat Intelligence collection using the AlienVault OTX platform

In this article, we set out to analyze **the email service,** given the essential role it plays within an organization, as well as considering the high degree of exposure it offers. Thus, we set out to identify the types of attacks that use **the service** of e-mail as a propagation vector.

AlienVault OTX (Open Threat Exchange) platform contains collections of Indicators of Compromise (IoCs), shared by the community. Platform members can share indicators of compromise (IoCs) such as malicious IP addresses, domains, URLs, file hashes and more.

AlienVault OTX (Open Threat Exchange) is an open-source and collaborative **Threat Intelligence** platform created by **AT&T Cybersecurity** that enables organizations and security professionals to collect, share and analyze information about cyber threats (Figure 1).



The World's First Truly Open Threat Intelligence Community

Chinese PlugX Malware Hidden in Your USB Devices?

New Mimic Ransomware Abuses Everything APIs for it...

The Titan Stealer: Notorious Telegram Malware Campa...

Doing time with the YIPPHB dropper | Elastic

Cisco Talos Intelligence Group - 5

PLEASE NOTE: this is a separate account from the LevelBlue Community and legacy Open Threat Exchange accounts.

OR

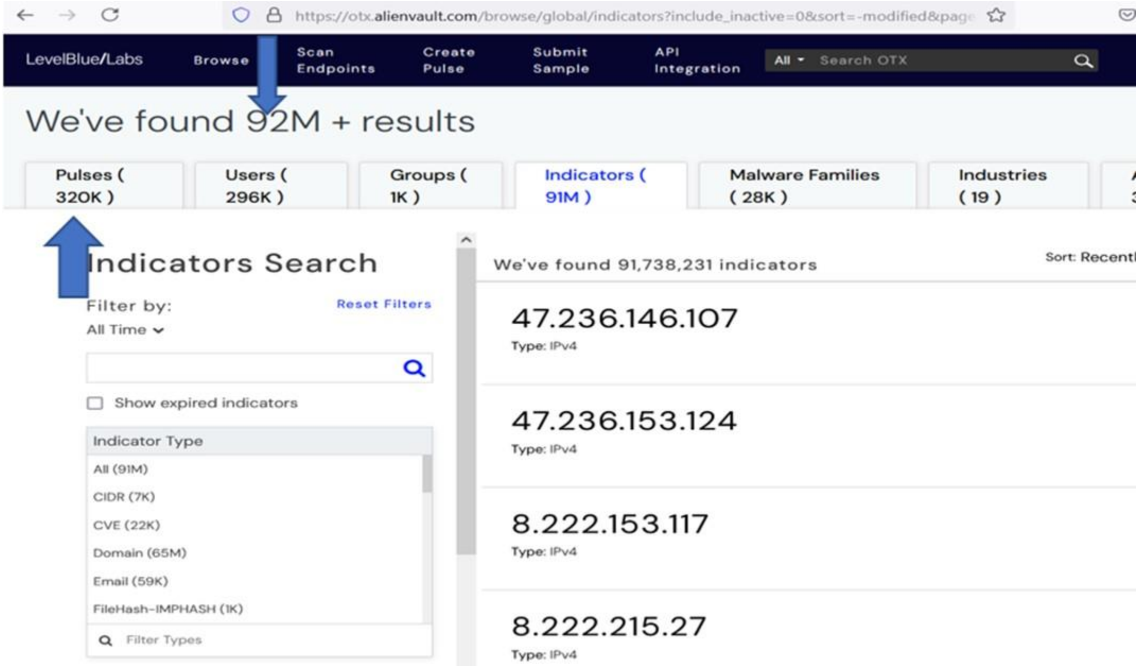
✓ Gain FREE access to over 20 million threat indicators contributed daily

✓ Collaborate with over 200,000 global participants to investigate emerging threats in the wild

© COPYRIGHT 2024 LEVELBLUE, INC. | WEBSITE TERMS OF USE | STATUS | YOUR PRIVACY CHOICES

Fig. 1. AlienVault OTX (Source: https://otx.alienvault.com/)

As we can see in the following image (Figure 2), the platform brings together, at this time, 92 million Indicators of Compromise (IoCs), and the existing pulses are 320,000.


https://otx.alienvault.com/browse/global/indicators?include_inactive=0&sort=-modified&page

We've found 92M + results

Pulses (320K) | Users (296K) | Groups (1K) | Indicators (91M) | Malware Families (28K) | Industries (19)

Indicators Search

Filter by: All Time

□ Show expired indicators

Indicator Type
All (91M)
CIDR (7K)
CVE (22K)
Domain (65M)
Email (59K)
FileHash-IMPHASH (1K)

We've found 91,738,231 indicators

Sort: Recentl

47.236.146.107
Type: IPv4

47.236.153.124
Type: IPv4

8.222.153.117
Type: IPv4

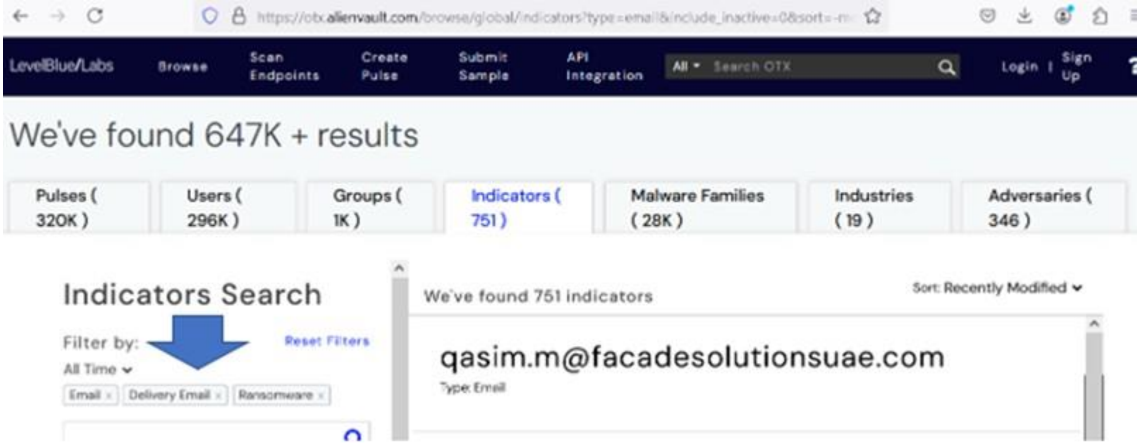
8.222.215.27
Type: IPv4

Fig. 2. Indicators of Compromise (IoCs)

Indicators of Compromise (IoCs) are basically attack indicators that help identify and prevent attacks. These indicators may include: IP addresses: addresses associated with malicious activities; Domains and URLs: Websites used by attackers to launch phishing or malware campaigns; File Hashes: Hashes that help identify malicious files; Email addresses: used in phishing or spam attacks.

Threat Pulses are sections of information that users can view or add to the platform. Each pulse is a description of an attack or threat campaign and contains detailed data about the tactics, techniques and procedures (TTPs) used by the attackers. Pulses can be added by users and are public, allowing stakeholders to access global threat information.

From the **AlienVault OTX platform** we will extract, with the help of filters, the relevant information from the perspective of the service under analysis: thus, in the Indicator Type section we select the email service, and in the Role section, we choose the Delivery Email parameter in conjunction with Ransomware, we notice that HAVE over 750 indicators, which represent email addresses used by malicious actors in various attacks (Figure 3).


https://otx.alienvault.com/browse/global/indicators?type=email&include_inactive=0&sort=-m

We've found 647K + results

Pulses (320K) | Users (296K) | Groups (1K) | Indicators (751) | Malware Families (28K) | Industries (19) | Adversaries (346)

Indicators Search

Filter by: All Time

Email × Delivery Email × Ransomware ×

We've found 751 indicators

Sort: Recently Modified

qasim.m@facadesolutionsuae.com
Type: Email

Fig. 3. The Indicator Type section

In these circumstances, reactive data analysis involves a comparison between the data collected at the level of equipment that ensures the perimeter protection of e-mail servers and this list of results, in order to update the security policies that ensure the protection of e-mail servers. By doing this, we ensure that all known threats do not reach the email client (in the recipient's inbox).

After collecting the data from the public reports, a careful analysis is required to interpret them correctly and apply them in the context of the organization. Properly understanding the context in which the threats were detected is essential. For example, information about a ransomware attack targeting the financial sector may be relevant to a bank, but not to a transport company.

After analyzing and interpreting the data, organizations can adjust security strategies to protect against identified threats. This may include applying security patches, updating firewall rules, strengthening authentication measures.

7. Conclusions

At the core of threat intelligence is understanding the cybersecurity landscape and monitoring emerging forms of malware, zero-day exploits, phishing attacks, and other cybersecurity issues.

Gathering and analyzing Threat Intelligence is an essential element in protecting organizations against cyber-attacks. By obtaining up-to-date information from open sources, organizations can better understand the threat landscape and implement proactive measures to protect their infrastructure and sensitive data. The process includes identifying relevant information sources, collecting data, analyzing it in the organization's specific context, and using appropriate tools to visualize and integrate it into security strategies.

References

[1]. https://www.microsoft.com/ro-ro/security/business/security-101/what-is-cyber-threat-intelligence

[2]. https://www.bitdefender.com/en-us/blog/businessinsights/targeted-threat-intelligence-for-security-operations/

[3]. https://www.bitdefender.com/ro-ro/business/products/advanced-threat-intelligence

[4]. R. Trifonov, O. Nakov, V. Mladenov, "Artificial Intelligence in Cyber Threats Intelligence". 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC). IEEE. pp. 1-4. doi: 10.1109/ICONIC.2018.8601235. ISBN 978-1-5386-6477-3. S2CID 57755206.

[5]. CyberProof Inc. (n.d.). Managed Threat Intelligence. CyberProof. Retrieved on April 03, 2023 from https://www.cyberproof.com/cyber-101/managed-threat-intelligence/

[6]. Dalziel, Henry (2014). How to Define and Build an Effective Cyber Threat Intelligence Capability. Syngress. ISBN 9780128027301.

[7]. Kant, Neelima (2024). "Cyber Threat Intelligence (CTI): An Analysis on the Use of Artificial Intelligence and Machine Learning to Identify Cyber Hazards". Cyber Security and Digital Forensics. Lecture Notes in Networks and Systems. Vol. 36. pp. 449-462. doi: 10.1007/978-981-99-9811-1_36. ISBN 978-981-99-9810-4.

[8]. Conti, M. (2021). "Measuring and Visualizing Cyber Threat Intelligence Quality". International Journal of Information Security. 20:21-38. doi: 10.1007/s10207-020-00490-y.

[9]. Shackleford, D. (2015). Who's Using Cyberthreat Intelligence and How?. SANS Institute. https://cdn-cybersecurity.att.com/docs/SANS-Cyber-Threat-Intelligence-Survey-2015.pdf

Profile of Persons Who Act in the Field of Computer Criminality

Vasile-Cătălin GOLOP, Natalia SĂVULESCU
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
catalin.golop@academiadepolitie.ro, natalia.savulescu@academiadepolitie.ro

Abstract

This article examines the profile of individuals involved in cybercrime activities, focusing on their psychological traits, motivations and technical skills. The study identifies common typologies of cybercriminals, ranging from individual hackers to organized groups, and examines the factors that contribute to choosing this type of illegal activity, such as social influences and opportunities in the online environment. The research hypothesis argues that individuals who commit cybercrime exhibit distinct characteristics that vary according to their goals and resources. The research method used combines case analysis with interviews and comparative studies, highlighting the diversity of profiles and the adaptability of offenders to emerging technologies. The results provide useful insights for implementing preventive measures and streamlining cybercrime investigations.

Index terms: cybercrime, phishing, website, cyberattack, financial crime

Introduction

The profile of people involved in computer crime (cybercrime) varies considerably, but there are some common characteristics that can be identified. This category of people can have diverse motivations and different levels of technical skills, which leads to different types of cyber attacks [1].

Most cybercriminals have good knowledge of IT and computer security. They can be programmers, network engineers, or even cyber security experts. In many cases, these skills are acquired formally (by studying computer science), but they are also often self-taught. They vary in age, but most of them are young, often between 18 and 35 years old. This is largely due to early access to technology and their ability to quickly adapt to new technologies.

Many hackers commit cybercrimes for financial gain, either through data theft or online fraud (e.g. phishing, ransomware, identity theft) [2]. Some cybercriminals are motivated by a political or social cause and engage in "hacktivism" attacks to promote ideas or beliefs. Some of these hackers are motivated by revenge, usually against former employers, business partners or people in their personal lives, as well as a desire to demonstrate their skills or gain respect in a particular cyber community.

1. Types of people who carry out attacks:

- **script kiddies**: people who do not have advanced knowledge, but use tools already created by others to carry out attacks [3].
- **professional hackers**: people with very advanced knowledge, able to write code and exploit complex vulnerabilities. They can work in teams or in organized groups.
- **hacktivists**: those who commit computer attacks to promote a political or ideological cause, such as groups like Anonymous [4].

2. Level of organization:

- **Individual criminals**: Hackers acting on their own are common, especially in small-scale financial fraud or phishing attacks.
- **Organized groups**: In cases of complex attacks, such as those orchestrated by organized crime groups or state-sponsored groups (APT - Advanced Persistent Threat), cybercriminals work in structured teams with a clear distribution of roles [5].

Cybercriminals are very aware of the need to protect their identity, so they use advanced anonymization tools such as TOR networks, VPNs, and data encryption. Some hackers are affiliated with organized crime networks or work for governments in espionage or cyber sabotage operations.

In short, the profile of cybercriminals is complex and diverse, ranging from isolated individuals with limited knowledge to well-organized and well-financed groups carrying out sophisticated attacks.

I. Typology of cybercriminals: classification based on level of expertise and motivation

Hackers who engage in online criminal activity vary significantly in their technical skills and motivations. Their classification provides a clear picture of the diversity of threats in cyberspace and the complexity of cybercriminal behavior.

1. Script kiddies. These hackers have little technical knowledge and do not create their own tools. Instead of developing attacks, they use software, scripts and tools available online, created by more experienced hackers. They often don't fully understand how the attacks they launch work.

Script kiddies generally do not have a major financial or ideological purpose. They attack systems to prove their skills to others, to gain some recognition in online communities, or simply out of boredom (motivation for attacks - *fun, social validation and curiosity*). They are responsible for simple attacks such as defacing websites or DoS (Denial of Service) attacks.

Example of attack: *a teenager launching a DDoS attack on an online gaming site using a tool found on public hacking forums*.

2. Black hat hackers. These hackers have extensive knowledge of operating systems, networks and software vulnerabilities, and are able to develop and implement their own cyber attacks. Black hats are malicious hackers, often involved in illegal activities for personal gain (technical skills **-** *advanced)* [6].

They are primarily motivated by money and are involved in activities such as stealing personal data, credit cards, financial fraud, ransomware and selling information on the dark web. This group represents a large part of organized cybercrime.

Example of attack: *a hacker who develops and distributes malware to steal banking data from unsuspecting users and then sell it on dark web markets.*

3. White hat hackers. These hackers have similar or even superior technical skills to black hats but use their knowledge for legitimate and legal purposes. They work in the cyber security industry to detect and correct security vulnerabilities (technical skills **-** *very advanced)* [7].

White hats are motivated by the desire to protect computer systems and users from cyber attacks. They may work as security analysts, pen-testers (penetration testers), or in other roles that involve assessing and improving the security of computer systems.

Attack example*: A security specialist performing penetration tests on an e-commerce system to discover vulnerabilities and prevent potential attacks.*

4. Gray hat hackers. Gray hat hackers have skills similar to black hats and white hats, but they use these skills in an ethically ambiguous way. They can break laws or rules without explicit malicious intent, but often without the victims' consent (technical skills **-** *advanced)* [8].

Gray hats are motivated by technological curiosity and a desire to demonstrate their skills. While not acting out of malice, they can break into systems without permission, and then inform owners of discovered vulnerabilities, sometimes asking for a reward (motivation of attacks **-** *curiosity, recognition and sometimes ethical*).

Example attack: *a hacker who breaks into a government system without permission, only to later report the breach and provide security solutions.*

5. Hacktivists. Some hacktivists have advanced technical knowledge, while others use tools available to the general public. They usually attack government, corporate or public interest websites (technical skills - *range from limited to advanced).*

Hacktivists are motivated by a desire to advance a political, social or ideological cause. They use cyber attacks to draw attention to issues they support or to sabotage organizations and governments that run counter to their beliefs.

Example attack: *groups such as Anonymous, which launch DDoS attacks on government websites to protest certain policies or events*.

6. Offenders from organized groups (cybercrime gangs). These groups are made up of hackers with varying skills, from malware and exploit developers to networking and cryptography experts. They often operate at a sophisticated level, carrying out well-planned and coordinated attacks (technical skills - *very advanced*) [9].

Criminals in organized groups are motivated by financial gain and often have corporate structures. These groups develop fraud schemes, ransomware, phishing, cyberespionage and other forms of cybercrime on a large scale. Some groups are supported by states and are involved in espionage or attacks on critical infrastructure.

Example of attack: *groups like REvil or Conti that launch ransomware attacks on companies and demand enormous sums for data decryption.*

7. State-Sponsored hackers. These hackers are part of highly trained teams, often supported financially and logistically by states or governments. They have access to considerable resources and have the ability to carry out highly sophisticated cyber-attacks (technical skills **-** *extremely advanced*) [10].

States sponsoring such hackers use cyber attacks as weapons in international political and economic conflicts. They can target cyber espionage, destabilizing critical infrastructures or influencing political processes.

Example of attack: *government-backed hacker groups, such as APT28 (Fancy Bear) or APT29 (Cozy Bear), involved in cyber espionage and political influence campaigns.*

This classification highlights the diversity in the world of cybercriminals, each with their own skills and motivations. Understanding the identity of these hackers and their operating techniques is critical to developing effective cybersecurity defenses.

II. Child pornography

The impact of the level of expertise on the types of attacks launched and the economic and security consequences in the context of the dissemination of child pornography online is a complex and sensitive subject, involving not only technical aspects, but also legal, psychosocial and ethical dimensions. In this analysis, we explore how different levels of technical expertise of criminals influence the dissemination of illegal content and the economic and security implications arising from these activities.

1. The level of expertise and types of attacks used in the dissemination of child pornography

Differences in technical skills influence the methods used to disseminate and conceal criminal activity related to child pornography.

In the case of child pornography, **script kiddies** can distribute the material through peer-to-peer (P2P) networks or through social networks using fake accounts and simple VPNs to hide their identity. Their activity is relatively easy to detect because they do not use advanced encryption or anonymization methods. However, given the large volume of content disseminated through common platforms, the ability of authorities to intercept all cases is limited, creating a major vulnerability for the protection of minors.

Black Hat hackers use advanced techniques to avoid detection, such as encrypting files, using anonymous networks such as *Tor* or *I2P*, and manipulating meta data to hide digital traces. They can create and use dark web forums that are encrypted and password protected to disseminate child pornography. Some of them may also be involved in *cyberlockers* - sites that host illegal password-protected files.

The activity of these hackers is much more difficult to detect and has serious consequences for cyber security. Encrypted and anonymous networks such as Tor greatly complicate efforts by authorities to identify and dismantle such networks. Also, the criminal economy surrounding these platforms is vast, including both direct sales and material exchanges, making it nearly impossible to trace the financial flow.

Organized crime groups use sophisticated and well-coordinated infrastructures to manage large child pornography dissemination platforms. These networks use hidden servers, *bulletproof hosting* infrastructure (which provides dedicated hosting services for illegal activities), and cryptocurrencies for payments. These groups can also create *pay-per-view platforms*, where users pay to access illegal content [11].

Networks run by organized groups have a devastating impact on global security as they systematically exploit vulnerabilities in networks and use cryptocurrencies to evade financial tracking. In addition to promoting the sexual abuse of minors, these networks generate substantial income from illegal activities, funds that can be used for other forms of cybercrime. The dissemination of child pornography in this setting can become part of a wider ecosystem of organized crime, including human trafficking.

2. The economic and security consequences of the dissemination of child pornography

This type of dissemination has major consequences, both economically and from a security point of view, and these vary according to the level of sophistication of the networks involved.

Authorities are devoting considerable resources to investigating and dismantling networks involved in the distribution of child pornography. In cases where criminals use advanced encryption and anonymization technologies, investigative efforts become very expensive and time-consuming. For example, operations involving infiltration in dark web networks or tracking cryptocurrencies can take years and require international collaboration.

Hosting services and digital infrastructure can be compromised by criminal groups that use these resources to host illegal content without the operators' knowledge. This affects the reputation of the companies involved and can lead to substantial economic losses. In addition, the use of cryptocurrencies in transactions related to illegal content undermines trust in these technologies, affecting emerging digital payment markets [12].

Networks that distribute child pornography are also often involved in other illegal activities, including cyberattacks, data theft, and espionage. For example, servers hosting illegal material can be compromised to launch *botnet attacks*, thereby using a criminal infrastructure for massive cyber attacks on organizations and governments [13]. In this way, criminals create a multifunctional digital crime infrastructure that affects global security. Also, this type of networks is often linked to human trafficking rings, which exacerbates the impact of these crimes on victims. In addition, these criminals create a demand for such materials, encouraging continued abuse of minors and generating an illegal market that is difficult to suppress.

III. Relevant case studies

Operation "Playpen" (2015)

The FBI conducted a large-scale operation targeting a global child pornography network, *Playpen*, hosted on the dark web. This network, accessed through *Tor*, had approximately 150,000 users. The FBI used a legal hacking technique to compromise Playpen users and identify them. In this operation, it was revealed that well-organized criminal groups use sophisticated infrastructures and advanced anonymization, which made it difficult for the authorities to intervene [14].

Consequences: Authorities were able to identify and arrest thousands of users globally, but the operation was costly and generated legal debate over the use of hacking by authorities.

Operation Blackwrist (2017)

Police in Thailand, working with Europol and other international agencies, dismantled a child pornography network operating on the dark web and coordinated by an organized crime group. The materials were accessible on a subscription basis paid with cryptocurrencies [15].

Consequences: This case highlighted the role of cryptocurrencies in financing cybercrime and showed how difficult it is for authorities to track anonymous payments. The operation led to arrests in several countries and the shutdown of several sites involved.

Conclusions

The level of expertise of criminals in this field who handle, in any way, child pornography has a direct impact on the types of attacks used and the difficulty with which the authorities can intervene. Those with very advanced knowledge create well-hidden networks, using encryption and anonymization, which makes combating these crimes extremely difficult. The economic and security consequences are major, affecting both infrastructures and trust in digital technologies, while suppressing this activity requires significant resources and very good international coordination.

References

[1]. Manualul Investigatorului în Criminalitatea Informatică, Ministerul Comunicațiilor și Tehnologiei Informației [Online] Available: https://www.scribd.com/doc/268511908/Manualul-Investigatorului-Criminalitatii-informatice. Accessed: October 6, 2024.

[2]. Phishing: A Cyber-Security Guide for Employers and Individuals, Zywave, 2020 [Online] Available: www.sutcliffeinsurance.co.uk/wp-content/uploads/2020/03/Phishing-Attacks-Guide.pdf. Accessed: October 10, 2024.

[3]. https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie

[4]. https://www.imperva.com/learn/application-security/hacktivism/

[5]. Phising, raportul privind situația amenințărilor, European Union Agency for Cybersecurity, January 2019-April 2020 [Online] Available: www.enisa.europa.eu/publications/report-files/ETL-translations/ro/etl2020-phishing-ebook-en-ro.pdf. Accessed: October 14, 2024.

[6]. https://www.kaspersky.com/resource-center/threats/black-hat-hacker

[7]. https://www.hackerone.com/knowledge-center/white-hat-hacker

[8]. Convenția privind Criminalitatea Informatică, Council of Europe, 2023 [Online] Available: https://eur-lex.europa.eu/RO/legal-content/summary/convention-on-cybercrime.html Accessed: October 10, 2024.

[9]. Convenția privind Criminalitatea Informatică, Council of Europe, 2023 [Online] Available: https://eur-lex.europa.eu/RO/legal-content/summary/convention-on-cyber crime.html Accessed: October 10, 2024.

[10]. https://www.cyberpolicy.com/cybersecurity-education/state-sponsored-hacking-explained

[11]. https://www.consilium.europa.eu/ro/infographics/cyber-threats-eu/

[12]. Legea nr. 161 din 19 aprilie 2003 cu modificările și completările ulterioare, Romanian Parliament, Romanian Official Monitor nr. 279 din 21 aprilie 2003. [Online] Available: https://legislatie.just.ro/Public/DetaliiDocument/43323

[13]. Legea nr. 161 din 19 aprilie 2003 cu modificările și completările ulterioare, Romanian Parliament, Romanian Official Monitor nr. 279 din 21 aprilie 2003. [Online] Available: https://legislatie.just.ro/Public/DetaliiDocument/43323

[14]. https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years

[15]. https://www.interpol.int/News-and-Events/News/2019/50-children-rescued-9-sex-offenders-arrested-in-international-operation

Enhancing Vulnerability Management with Artificial Intelligence Algorithms

Gabriela TOD-RĂILEANU, Ana-Maria DINCĂ, Sabina-Daniela AXINTE,
Ioan C. BACIVAROV
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
gabriela.tod@stud.etti.upb.ro, ana_maria.dinca@stud.etti.upb.ro, axinte_sabina@yahoo.com,
ioan.bacivarov@upb.ro

Abstract

The rising number of vulnerabilities, highlights the growing cybersecurity challenges and the need for robust vulnerability management. This paper examines the role of Artificial Intelligence in enhancing vulnerability detection and management, focusing on scalable and accurate solutions to address large-scale codebase analysis. AI-driven techniques bridge traditional static analysis and advanced detection, uncovering hidden vulnerabilities and improving efficiency. Future research should optimize these tools for diverse languages, Secure Software Development Life Cycle workflows, and predictive threat analysis. These advancements highlight AI's potential to strengthen software security in an increasingly complex threat landscape.

Index terms: vulnerability management, Artificial Intelligence, code scanning, Secure Software Development Lifecycle, vulnerability detection

1. Introduction

According to the National Vulnerability Database (NVD) maintained by NIST, 28961 new Common Vulnerabilities and Exposures (CVEs) were published in 2023 and there are already 29004 new CVEs published by November in 2024 [1]. Even though the year is not yet completed, it can be observed an increase of approximately 0.15% and this underscores the growing challenges in cybersecurity and the critical importance of robust vulnerability management practices. This paper analyzes the current implementation of Artificial Intelligence (AI) in vulnerability detection and management. The goal is to understand if there are any solutions, proprietary or open-source software, that can help in a world where only one critical vulnerability has affected over 2000 organizations [2] and had an estimated cost of over 15 million USD.

2. Vulnerability management

It is important to understand what a vulnerability in cybersecurity is: a weakness or flaw in a system, application, network, or process that can be exploited by attackers to compromise its security. Vulnerabilities can lead to unauthorized access, data theft, system disruptions, or other malicious activities.

Vulnerabilities arise from flaws in software development, such as unvalidated input, weak authentication, or insecure configurations [3], which can be exploited by attackers to execute malicious actions or gain unauthorized access. These weaknesses can compromise key security objectives: confidentiality (exposing sensitive data), integrity (altering or corrupting data), and availability (disrupting operations or causing denial-of-service). Effective mitigation is essential to maintain system security and resilience.

Vulnerability management constitutes a continuous process of identifying, assessing, prioritizing, and addressing vulnerabilities in an organization's systems, applications, and networks. The objective is to mitigate the risk of exploitation and enhance the overall security posture by proactively addressing weaknesses before potential exploitation by malicious actors. It is noteworthy that this process requires ongoing improvement due to the escalating number of threats, and scalability represents one of the most significant factors influencing modifications in the vulnerability management process.

The vulnerability management process encompasses several critical components, which can be compared to the framework established for Secure Software Development Lifecycle (SSDLC). However, organizations may opt to adapt this process to their specific requirements. The key components are:

- **Identification**: Utilize tools such as vulnerability scanners to detect weaknesses across systems, networks, and applications.
- **Assessment**: Evaluate the severity of detected vulnerabilities using frameworks such as the Common Vulnerability Scoring System (CVSS). Determine the probability of exploitation and the potential impact on the organization.
- **Prioritization**: Rank vulnerabilities based on risk factors including exploitability, asset criticality, and exposure (e.g., public-facing systems). Allocate resources to address high-risk vulnerabilities as a priority.
- **Remediation**: Implement fixes such as software patches, updates, or configuration changes to resolve vulnerabilities. If immediate remediation is not feasible, implement temporary mitigation measures to minimize risk.
- **Validation**: Verify that vulnerabilities have been resolved and no residual risks remain.
- **Reporting and Continuous Improvement**: Document findings, actions taken, and improvements made for compliance and future reference. Continuously refine processes based on lessons learned and emerging threats.

This analysis will focus on the contributions of Artificial Intelligence to the Identification and Assessment phases of vulnerability management. Specifically, it will examine how AI-driven tools enhance the detection of vulnerabilities by automating the scanning of complex systems, analyzing codebases, and identifying patterns of weaknesses more efficiently than traditional methods. In the Assessment phase, the analysis will explore how AI leverages predictive algorithms, machine learning models, and real-time data to prioritize vulnerabilities based on exploitability, potential impact, and business context. By addressing these areas, this study aims to highlight how AI not only accelerates the identification and assessment processes but also improves accuracy, scalability, and decision-making in vulnerability management.

3. Artificial Intelligence used in Vulnerability Detection

In this study, a structured approach for vulnerability detection is proposed, by categorizing it into two primary domains: infrastructure scanning and code scanning. The first domain, **infrastructure scanning**, encompasses the identification of vulnerabilities across network devices, servers, cloud environments, and other components that form the backbone of IT systems. This approach ensures a robust and resilient infrastructure against threats.

The second domain, **code scanning**, delves into analyzing the application layer, specifically the source code and software components, to identify security flaws during development. This category includes methods such as static and dynamic code analysis, which are critical for addressing vulnerabilities before deployment. By segmenting the topic into these two areas, it is aimed to provide a comprehensive understanding of vulnerability detection, addressing both the foundational infrastructure and the applications built upon it.

From an infrastructure scanning perspective, several industry leaders have established a strong reputation for their expertise, extensive research, and innovative solutions in this domain. Notable among these are: Tenable IO with "Tenable One: The world's only AI-powered exposure management platform" [4], Qualys with Qualys VMDR (Vulnerability Management, Detection, and Response) [5] and Rapid7 [6]. Complementing these proprietary offerings is an open-source tool with significant potential: Trivy [7]. One of the greatest advantages identified for the open-source tool mentioned before is that by utilizing Trivy as a security scanner, developers become more aware of security issues as they arise. This proactive approach enables them to address vulnerabilities promptly, reducing the likelihood of security problems being discovered late in the development process [8]. This feature positions Trivy as an invaluable tool for bridging the gap between development and security in modern DevOps practices.

From the code scanning perspective, there are some industry leaders that have already enhanced their tools with AI. Notable mentions are: Snyk Code that utilizes AI to provide real-time static application security testing (SAST), which offers immediate feedback on code vulnerabilities, enabling developers to identify and fix issues during the development process [9]. GitHub's CodeQL is a semantic code analysis engine that uses AI to detect vulnerabilities across codebases. It allows developers to write custom queries to find specific vulnerabilities and integrates seamlessly with GitHub workflows [10]. There are also new companies that have become popular, such as: Armur AI, that employ Large Language Models (LLMs) to perform static code analysis, identifying vulnerabilities and providing remediation suggestions [11]. The researchers have also contributed to the list with multiple tools such as Vulnhuntr [12], VulBERTa [13] and VulCNN. VulCNN is an image-inspired scalable vulnerability detection system that applies deep learning techniques to source code analysis. By converting code into image-like representations, VulCNN utilizes convolutional neural networks (CNNs) to identify potential vulnerabilities [14].

4. Exploring the Capabilities of Open-Source Scanning Tool

This section provides a comprehensive examination of VulCNN's underlying mechanisms, its key strengths, and its potential applications, emphasizing its contributions to the field of vulnerability detection.

4.1. Design of VulCNN

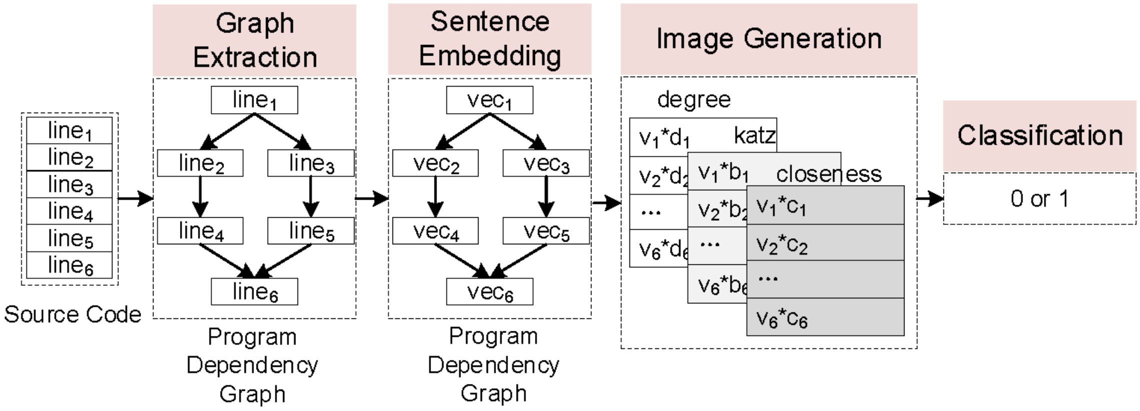


Fig. 1. Pipeline of VulCNN: From Source Code to Vulnerability Classification [14]

The tool operates through four key phases:

- Graph Extraction: Starting with the source code of a function, the process involves normalizing the code and performing static analysis to construct the program dependency graph for the function.
- Sentence Embedding: In this phase, each node in the program dependency graph, representing a line of code, is treated as a sentence. These lines are then embedded into corresponding vectors, capturing their semantic and structural information.
- Image Generation: Following the embedding phase, centrality analysis is applied to determine the relative importance of each line of code. These centrality scores are multiplied by the respective vectors, and the resulting data is formatted as an image.
- Classification: In the final phase, the generated images are used to train a convolutional neural network (CNN). Once trained, CNN classifies the images to detect whether vulnerabilities exist within the code.

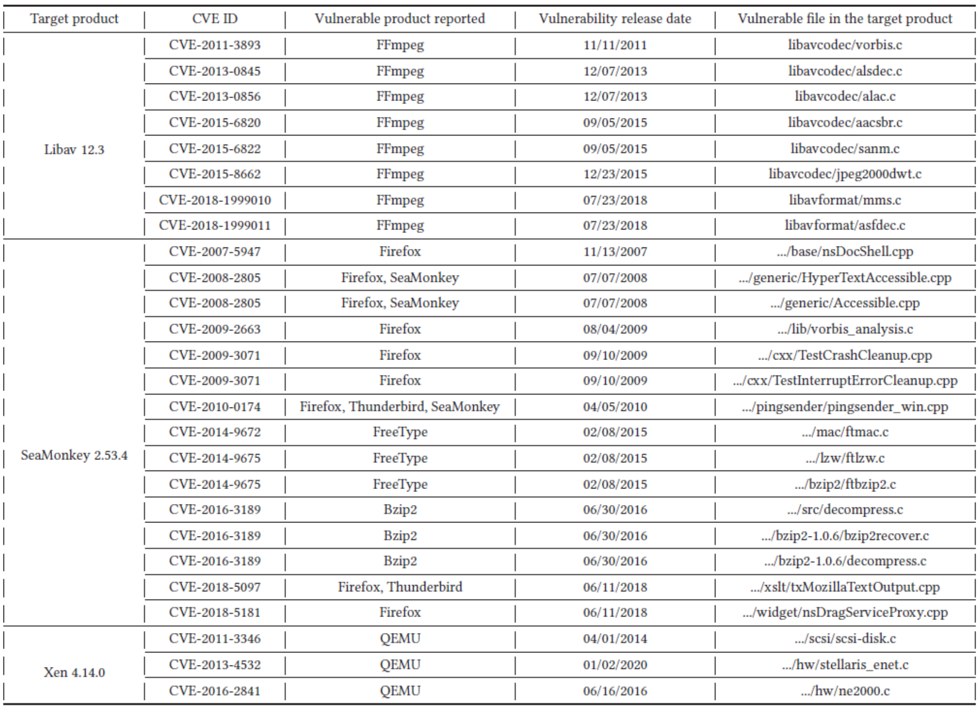
4.2. Dataset

The dataset used is sourced from the Software Assurance Reference Dataset (SARD) [15], a project maintained by the National Institute of Standards and Technology (NIST) [16]. SARD provides a comprehensive collection of production, synthetic, and academic security flaws (referred to as "bad functions") alongside a large set of "good functions." Since the focus is on detecting vulnerabilities in C/C++ code, there were selected only the C/C++ functions from SARD. The dataset includes 12,303 vulnerable functions and 21,057 non-vulnerable functions.

4.3. Results of the case study

There were selected three open-source applications for the test: Libav [17], Xen [18], and Seamonkey [19]. The analysis reveals that 73 warnings align with known vulnerability patterns listed in the NVD. Among these identified vulnerabilities, 17 have been "silently" patched by vendors in the latest versions of their respective products, the code related to four vulnerabilities has been removed, and the remaining 52 vulnerabilities persist in the products [14].

Table 1. A part of the vulnerabilities discovered by VulCNN from the latest versions of the selected products [14]



Target product	CVE ID	Vulnerable product reported	Vulnerability release date	Vulnerable file in the target product
Libav 12.3	CVE-2011-3893	FFmpeg	11/11/2011	libavcodec/vorbis.c
	CVE-2013-0845	FFmpeg	12/07/2013	libavcodec/alsdec.c
	CVE-2013-0856	FFmpeg	12/07/2013	libavcodec/alac.c
	CVE-2015-6820	FFmpeg	09/05/2015	libavcodec/aacsbr.c
	CVE-2015-6822	FFmpeg	09/05/2015	libavcodec/sanm.c
	CVE-2015-8662	FFmpeg	12/23/2015	libavcodec/jpeg2000dwt.c
	CVE-2018-1999010	FFmpeg	07/23/2018	libavformat/mms.c
	CVE-2018-1999011	FFmpeg	07/23/2018	libavformat/asfdec.c
SeaMonkey 2.53.4	CVE-2007-5947	Firefox	11/13/2007	.../base/nsDocShell.cpp
	CVE-2008-2805	Firefox, SeaMonkey	07/07/2008	.../generic/HyperTextAccessible.cpp
	CVE-2008-2805	Firefox, SeaMonkey	07/07/2008	.../generic/Accessible.cpp
	CVE-2009-2663	Firefox	08/04/2009	.../lib/vorbis_analysis.c
	CVE-2009-3071	Firefox	09/10/2009	.../cxx/TestCrashCleanup.cpp
	CVE-2009-3071	Firefox	09/10/2009	.../cxx/TestInterruptErrorCleanup.cpp
	CVE-2010-0174	Firefox, Thunderbird, SeaMonkey	04/05/2010	.../pingsender/pingsender_win.cpp
	CVE-2014-9672	FreeType	02/08/2015	.../mac/ftmac.c
	CVE-2014-9675	FreeType	02/08/2015	.../lzw/ftlzw.c
	CVE-2014-9675	FreeType	02/08/2015	.../bzip2/ftbzip2.c
	CVE-2016-3189	Bzip2	06/30/2016	.../src/decompress.c
	CVE-2016-3189	Bzip2	06/30/2016	.../bzip2-1.0.6/bzip2recover.c
	CVE-2016-3189	Bzip2	06/30/2016	.../bzip2-1.0.6/decompress.c
	CVE-2018-5097	Firefox, Thunderbird	06/11/2018	.../xslt/txMozillaTextOutput.cpp
	CVE-2018-5181	Firefox	06/11/2018	.../widget/nsDragServiceProxy.cpp
Xen 4.14.0	CVE-2011-3346	QEMU	04/01/2014	.../scsi/scsi-disk.c
	CVE-2013-4532	QEMU	01/02/2020	.../hw/stellaris_enet.c
	CVE-2016-2841	QEMU	06/16/2016	.../hw/ne2000.c

5. Conclusions and future scope

Advancements in vulnerability detection systems, such as those demonstrated by tools like VulCNN, highlight the ongoing progress in leveraging innovative methodologies to improve software security. By combining scalability and accuracy, modern approaches are addressing critical challenges in detecting vulnerabilities in large-scale codebases. The integration of techniques like converting source code into representations suitable for deep learning analysis has proven effective in bridging the gap between traditional static analysis and cutting-edge AI-driven solutions. These advancements have not only outperformed existing tools in accuracy and speed, but also showcased the potential to uncover previously unreported vulnerabilities, emphasizing their practical relevance in real-world applications.

Future research should aim to expand on these developments by exploring alternative AI architectures, such as hybrid models, to further refine the detection process. Additionally, optimizing methodologies to handle diverse programming languages and integrating such tools seamlessly into software development workflows, including Continuous Integration/Continuous Deployment (CI/CD) pipelines, will be crucial for fostering a proactive approach to security. Another promising avenue is incorporating threat intelligence data to predict emerging vulnerabilities and enhance real-time detection capabilities.

In conclusion, the field of vulnerability detection continues to evolve rapidly, with tools like VulCNN setting a benchmark for innovation. The combination of scalability, accuracy, and adaptability in these systems highlights the potential for developing more comprehensive and efficient solutions, paving the way for a more secure software ecosystem in the face of ever-increasing security challenges.

References

[1]. "CVE metrics," CVE org, 2023. [Online]. Available: https://www.cve.org/about/Metrics. [Accessed 10 November 2024].

[2]. Z. Simas, "Unpacking the MOVEit Breach: Statistics and Analysis," EMSISoft, 18 July 2023. [Online]. Available: https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/. [Accessed 10 November 2024].

[3]. OWASP, "OWASP Top Ten," OWASP, [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed 1 November 2024].

[4]. Tenable IO, "Tenable One," Tenable IO, October 2022. [Online]. Available: https://www.tenable.com/products/tenable-one. [Accessed 1 November 2024].

[5]. "Leveraging AI-informed Cybersecurity to Measure, Communicate, and Eliminate Cyber Risk," Qualys, 9 November 2023. [Online]. Available: https://blog.qualys.com/qualys-insights/qualys-security-conference/2023/11/09/leveraging-ai-informed-cybersecurity-to-measure-communicate-and-eliminate-cyber-risk. [Accessed 12 November 2024].

[6]. K. Lynas-Blunt, "Securely Build AI/ML Applications in the Cloud with Rapid7 InsightCloudSec," Rapid7, 22 December 2023. [Online]. Available: https://www.rapid7.com/blog/post/2023/12/22/securely-build-ai-ml-applications-in-the-cloud-with-rapid7-insightcloudsec/. [Accessed 1 November 2024].

[7]. "The all-in-one open source security scanner," AquaSec, [Online]. Available: https://trivy.dev. [Accessed 28 October 2024].

[8]. Panca, Rizki, Perkasa., Evangs, Mailoa, "Adopsi devsecops untuk mendukung metode agile menggunakan trivy sebagai security scanner docker image dan dockerfile," Jurnal Indonesia : Manajemen Informatika dan Komunikasi, vol. 4, no. 3, pp. 856-863, 2023.

[9]. "Snyk Code: Developer-focused, real-time SAST," Snyk, [Online]. Available: https://snyk.io/product/snyk-code/. [Accessed 1 November 2024].

[10]. "Finding security vulnerabilities and errors in your code with code scanning," GitHub, 2024. [Online]. Available: https://docs.github.com/en/code-security/code-scanning. [Accessed 12 November 2024].

[11]. A. Sharma, "What Is a Code Vulnerability Analyzer?," Armur AI, 3 September 2024. [Online]. Available: https://armur.ai/blogs/posts/code_vulnerability_analyzer/. [Accessed November 2024].

[12]. D. McInerney, M. Salvati, "Vulnhuntr GitHub repository," ProductAI, 9 November 2024. [Online]. Available: https://github.com/protectai/vulnhuntr. [Accessed 14 November 2024].

[13]. H. Hanif, S. Maffeis, "Vulberta: Simplified source code pre-training for vulnerability detection," in International Joint Conference on Neural Networks (IJCNN), 2022.

[14]. Y. Wu, D. Zou, S. Dou, S. Dou, W. Yang, D. Xu, H. Jin, "VulCNN: An Image-inspired Scalable Vulnerability Detection System," 2022 IEEE/ACM 44th International Conference on Software Engineering (ICSE), pp. 2365-2376, 2022.

[15]. "NIST Software Assurance Reference Dataset," Software Assurance Metrics And Tool Evaluation, [Online]. Available: https://samate.nist.gov/SARD. [Accessed 10 November 2024].

[16]. "National Institute of Standards and Technology," US Department of Commerce, [Online]. Available: https://www.nist.gov. [Accessed 10 November 2024].

[17]. "Libav GitHub repository," Libav, [Online]. Available: https://github.com/libav/libav. [Accessed 15 October 2024].

[18]. "Xen Project archives," Xen Project, [Online]. Available: https://xenproject.org/xen-project-archives/. [Accessed 1 November 2024].

[19]. "Seamonkey Project," [Online]. Available: https://www.seamonkey-project.org/. [Accessed 15 October 2024].

Security of Romanian Electronic Passports: The Protection of Personal Data in the Digital Age

Aurelian-Gabriel BĂDIȚĂ
Border Police Department, "Al. I. Cuza" Police Academy, Bucharest, Romania
aurelian.badita@academiadepolitie.ro

Abstract

Highlighting the evolution and importance of electronic passports in Romania, respectively the security risk associated with cyber attacks against the system for issuing these documents, represents a first pillar in the development of strategies to protect national security. Adopting a proactive approach in managing cyber risks in ensuring the security of the electronic passport issuance system, respectively the security of citizens' personal data, is necessary to provide an optimal climate of trust, both for the national/European/international order and security structures, and for the well-being of the citizens who request such documents. It can be seen that attackers or impostors develop various strategies to identify and gain access to data in electronic passports in order to exploit or compromise them. Many of them resort to different methods of accessing the personal data of electronic passport holders in order to falsify them and use them to cross the state border, respectively to alienate them to other potential criminals who want to evade border control. The structures responsible for issuing e-passports implement state-of-the-art high-performance electronic security equipment and systems to counter cyber-attacks, but permanent security methods are required, as attackers resort to modern advanced methods of unauthorized access.

Index terms: evolution of passports, electronic passports, cyberattacks, protection of personal data, consequences of cyberattacks

1. Introduction

The evolution of travel documents, from a simple document, which certifies the right of a person to cross the state border, to an electronic document, which contains biometric elements with an integrated chip, where information on the holder's data is stored, has experienced a real rise in the digital age.

The term passport was not yet assigned to travel documents since it was attested as a travel document. Thus, in the period of Antiquity and the Middle Ages, the documents that served the holder to cross the state border were called differently[1].

The term passport first appeared in England in the 15th century, but the etymology of the word comes from the French *passer* (to pass) and *port* (to carry), as French was a language of international diplomacy at the time.

[1] Online source: https://pasapoarte.mai.gov.ro/wp-content/uploads/2021/03/comunicat-ZiuaPAS-2011.pdf, accessed on August 4, 2024 - "*salvconducte, scrisori adeveritoare, cărți de pribegie, răvașe, sineturi, teșcherele, foi de circulație, foi de călătorie, pasuri, pasușuri sau pașapoarte*"

"*The United Kingdom and France are two countries which both claim the right to have invented the passport, in the contemporary sense of the term*"[2].

In United Kingdom, reference has been made since 1414 to the travel document, but entitled *laissez-passer* (*free passage*), and in France the travel document has been called a *passport* since 1420[3].

As human migration has taken place throughout history for a variety of reasons, driven by a variety of factors such as climate change, trade, exploration, conflict, etc., state authorities have tightened the conditions of travel.

Also, in order to have a control over persons migrating to/from the territory of a state, the authorities of that state have developed policies and strategies on the security of fraudulent documents by adopting legislation on the circulation of these documents.

Therefore, there are now a number of international, European and national rules in place to make it more difficult to fraud these travel documents, and travel documents with biometric data and high performance security features are being put into circulation.

2. Evolution from traditional to electronic passports

A reference moment regarding the evolution, both from a technical and legislative point of view, of passports, is the period following the events of December 1989. Thus, after this period, the passport experienced a real transformation as the national borders were opened to Romanian citizens.

However, in order to be recognized outside Romania, passports had to be made according to international standards.

A first model of passport complying with international standards was issued "*from June 1994*", which contained a computerized - double laminated - tab.

This passport is known as the *1993 model* since it was put into circulation following the adoption of Government Decision No. 757/1993[4].

The next passport model, *model 2001*, was put into circulation based on Government Decision no. 460/2001[5], on 21 January 2002. To which significant changes have been made, including the digital printing of the holder's photo on the computerized file[6].

A landmark moment in terms of the development of a legislative framework and the introduction of passports containing biometric data was the unfortunate moment of the terrorist attacks in the USA, on September 11, 2001. Thus, for the first time, the United States launched on May 14, 2002 through the Visa-Waiver program the document "*Enhanced Border Security and Visa Entry Reform Act of 2002. Aliens*"[7], and in order to allow third citizens to enter the US territory, they were required to have passports with biometric data and containing ICAO[8] standards.

[2] Cornea, V., ”*Evoluția și implicațiile sociale ale pașaportului: de la scrisori de liberă circulație la pașapoarte de aur”*, published in The Scientific of Cahul State University B.P. Hașdeu: Social Sciences, no. 1(11), p. 52, 2020, online source: https://www.researchgate.net/publication/341357883_Evolutia_si_implicatiile_sociale_ale_pasaportului_de_la_scrisori_de_libera_trecere_la_pasapoarte_de_aur_The_evolution_and_social_implications_of_the_passport_from_the_free_passage_letters_to_golden_pa, accessed on August 5, 2024

[3] Cornea, V., op. cit., p. 50

[4] Government Decision no. 757 of December 30, 1993 on the introduction into circulation of the new Romanian passports, published in the Official Gazette no. 24 of January 26, 1994

[5] Government Decision no. 46 of May 9, 2001 on the introduction into circulation of new types of Romanian passports, published in the Official Gazette no. 272 of May 25, 2001

[6] Costea, S.G., Porojan, M., Sbîrlea, C. & Popa, V., ”*Regimul juridic al liberei circulații a cetățenilor români”*, printed by C.N. "Imprimeria națională" S.A., Bucharest 2019, p. 73

[7] Online source: https://www.govinfo.gov/content/pkg/PLAW-107publ173/pdf/PLAW-107publ173.pdf, accessed on August 6, 2024

[8] ICAO – The International Civil Aviation Organization

These standards were set out in the document entitled "Document 9303"[9] –*Technical specifications for reliable travel documents* and defining precise requirements for electronic passports, including specifications on the integrated chip, formats and types of data stored, data encryption, security features, as well as global interoperability requirements.

Thus, Regulation (EC) No 2252/2004[10] was also adopted at EU in order to start the procedure for putting electronic passports into circulation and meet ICAO standards.

Starting with December 31, 2008, the electronic passport containing a non-contact chip with biometric data was put into circulation.

This 2008 passport model is also called *the first generation of electronic passports* and has biometric data implemented on the memory medium (E.g.: facial photography and dactyloscopic impressions), biographical (e.g. date and place of birth) and unique information of the holder (example: personal identification number), but also the unique passport data (example: document number).

The longest-standing Romanian legal act on the basis of which this passport model was issued and which is still in force today is Law 248/2005[11].

Due to the changes that occurred in the context of adapting to the current needs of modern society and the requirements imposed by the legislation in force, the normative act has undergone several additions and amendments, but without major changes on the substantive aspects.

Another passport model, also called *the second generation of electronic passports*, was put into circulation in May 2010, with the same format, but with higher security features than the previous one.

Starting with January 1, 2019, *the third generation of electronic passports* was put into circulation because it was necessary to issue a new passport model, both in terms of renewal and insertion of new security elements, and due to the fact that 2018 marked the 100th anniversary of the Great Union[12]. At the same time, the provisions of Law no.146/2016[13] required the public authorities to replace the coats of arms and seals existing at that time.

This model passport is the last type of document to be issued at national level and which includes advanced security features.

3. What electronic passports are?

A definition of electronic passports can be deduced from the wording of Article 6, paragraph (4) of Law 248/2005, which states that they are travel documents that "are the property of the Romanian state and provide proof of identity, citizenship, status, and the holder's right to travel abroad"[14].

Electronic passports are travel documents that contain an electronic chip that stores biometric and personal information of the holder, as well as document data.

This information may include dactyloscopic impressions, also called fingerprints, the holder's facial photograph, as well as other data visible on the computerized file.

[9] Online source: https://www.icao.int/publications/Documents, accessed on August 6, 2024

[10] Council Regulation (EC) No 2252/2004 of December 13, 2004, on security standards and biometrics in passports and travel documents issued by Member States, published in the Official Journal of the European Union No L 385/1 of December 29, 2004, as amended and supplemented

[11] Law no. 248 of July 20, 2005 on the regime of free movement of Romanian citizens abroad, published in the Official Gazette no. 682 of July 29, 2005, with subsequent amendments and additions

[12] Online source: http://centenar.gov.ro/web/marea-unire/, accessed on August 6, 2024

[13] Law No 146 of July 12, 2016 amending Law No 102/1992 on the national coat of arms and state seal, published in the Official Gazette No 542 of July 19, 2016

[14]Law no. 248 of July 20, 2005 on the regime of free movement of Romanian citizens abroad, published in the Official Gazette no. 682 of July 29, 2005, with subsequent amendments and additions

All of this information and data is included on the chip to improve the security and reliability of passports and also to quickly identify the identity of the document and the user.

Electronic passports are designed to prevent fraud and facilitate the border control process.

The implementation of ICAO standards ensures that electronic passports comply with a common set of technical and security requirements, while facilitating their mutual recognition internationally. These requirements also enhance the security of the holder's information and identity.

At national level, electronic passports are produced by *"Compania Naţională - Imprimeria Naţională - S.A., in its own production capacities"*[15], in the form of a passport blank.

After the electronic passports are made, they are distributed and "*personalized at the General Directorate of Passports within the Ministry of Internal Affairs*"[16], at the Single National Center for Personalization of Electronic Passports.

4. Security features of electronic passports

Electronic passports are equipped with a secure chip that contains a number of features designed to ensure a high level of security, including:

- Advanced encryption – so that information can be stored against unauthorized access;
- Biometric data – facial photograph and dactyloscopic impressions, which are used to identify the holder;
- Digital signature – to verify the authenticity and belonging of the travel document.

These security features ensure that the electronic passport is a reliable and fraud-proof document, protecting the holder's identity as well as their personal data.

The integrated chip allows border authorities and other competent entities to verify the authenticity of the passport and the identity of the holder through the data stored in the chip.

At the same time, this chip can include additional security features, such as a digital signature or cryptographic key, which increase the level of protection against cyber attacks and provide support in preventing forgery and fraudulent use of the electronic passport.

Cyberattacks on electronic passports are a major concern due to the serious consequences they can have in terms of national security, personal data privacy and traveler safety.

Examples of consequences of cyber-attacks:

a) Identity theft: a successful cyber-attack on electronic passports could lead to identity theft of the holders, allowing criminals to use personal information to fraudulently authenticate themselves or commit financial fraud.

Example: *a hacker manages to gain access to a person's personal and financial information in order to commit various frauds or crimes in that person's name. A notable incident where the personal data of around 500 million Marriott International customers was compromised, including names, addresses, phone numbers, payment details and passports*[17].

b) Data falsification: by manipulating or compromising the chip, criminals can falsify or alter stored information, including biometric data, to create forged electronic passports;

Example: *A criminal could clone information from a valid electronic passport and enter false data, such as a different facial photo or changed name, in an attempt to present themselves at the border under a false identity. This form of electronic passport forgery can*

[15] Online source: www.cnin.ro/pasapoarte.php, accessed on August 26, 2024

[16] Ibidem

[17] Johnson, R., Smith, K., ”The Impact of Identity Theft on Victims: A Comprehensive Study”, published in Journal of Criminology, 2018, pp. 112-129

See also BBC article from November 30, 2018 - Marriott hack hits 500 million Starwood guests, online source: https://www.bbc.com/news/technology-46401890, accessed on 6 August 2024 *endanger national security and can be used to avoid travel restrictions or commit fraud or other crimes*[18].

c) Cyber-espionage: criminal organizations might try to access sensitive information stored on the chip to obtain information about the owners or to compromise national security
Exemplu: *in 2014, a group of hackers managed to compromise the biometric identification chips of 5.6 million U.S. citizens stored in the Department of Veterans Affairs' Offices of Veterans Affairs. These hackers were able to steal citizens' fingerprints, personal information and other biometric data without them realizing it*[19].

d) Hacking techniques: cyber attacks on e-passports can involve various hacking techniques such as RFID[20] scanning, intercepting wireless communications, exploiting software or physical vulnerabilities to access or manipulate on-chip data.
Example: *phishing, malware, brute force attacks*

Electronic passports also have built-in anti-forgery features such as: holograms, watermarks, luminosity elements (which react differently to different light spectra - natural, infrared, ultraviolet, depending on the angle at which certain elements are observed), micro-text or variable optical elements to prevent fraudulent documents.

5. Risks to electronic passport Security and Personal Data Protection

Some of the most used methods of cyberattacks and that produce serious consequences in passport systems are:

5.1. Phishing[21] refers to a form of cyber-attack in which a criminal attempts to obtain sensitive information or personal data from electronic passport holders under the guise of false or fraudulent communication. Criminals may try to obtain data such as usernames, passwords, biometric information, or other personal data through emails, text messages, or links that appear to be from state institutions.

For example, a criminal may request personal details or electronic passport information through a fraudulent e-mail pretending to be a civil servant in the passport issuing service, under the pretext that an update or verification of data is required.

People could be misled into providing confidential data and information that could be used for fraudulent purposes.

5.2. Malware[22] is a cyber threat where malicious software is used to compromise the security of electronic passports and data stored on the chip.

Attackers can use malware to infect passport issuing and management systems to access confidential data/information (Example: Changes a cardholder's identity data) and biometric data of passport holders. This data and information can then be used fraudulently or to violate the security and confidentiality of personal information.

[18] Brown, A., Jones, M., ”*Fraudulent Use of Electronic Passports: Trends and Security Measures*”, published in International Journal of Criminology, 2020, pp. 245-262

[19] Smith, J. ”Cyber Espionage: The Case of Biometric Data Theft”, published in Journal of Cybersecurity, 2015, pp. 45-62

[20] RFID – Identitate prin frecvență Radio (Radio Frequency Identification)

[21] Online source: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-phishing, accessed on August 6, 2024 – definition taken and adapted

[22] Online source: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-malware, accessed on August 6, 2024 - definition taken and adapted

Malware can be introduced into the passport issuing and management system via infected malicious links or USB devices. Once introduced into the passport system, through malware, criminals can monitor and extract personal data, including blocking access to the data on the chip.

In order to prevent malware and protect the security of the electronic passport issuing and management system, it is necessary to update anti-virus programs and avoid downloading files or even accessing unknown/unsecure websites.

5.3. Brute force attacks[23] is a cyber-attack method where an attacker attempts to discover the passwords or cryptographic safeguards of a security system by repeatedly and systematically trying different combinations of characters or passwords.

These methods can be used to try to force access to the data stored on the electronic passport chip or the cryptographic keys used to secure personal information.

Attackers try to discover the passwords or codes needed to access or manipulate the data on the electronic passport chip using specialized software or technological devices.

To counter this method, it is important that security systems include measures to limit the number of access attempts, the implementation of complex passwords or access codes (for example: containing upper and lower case letters, numbers and distinctive characters, and the number of characters being sufficiently large) and regularly updated, respectively effective data encryption.

6. Conclusions

With the introduction of Romanian electronic passports into circulation, the chip has become an essential element, offering the possibility of storing data in secure digital format. Some of the most important data stored on the chip is also the biometric data of the holder, which provides a major support in quickly identifying fraud or attempted fraudulent use of such a travel document.

At the same time, electronic passports have undergone significant security enhancements by implementing advanced security features such as holograms, printing techniques, secure chips and other physical security features.

Romanian electronic passports have been issued according to the international standards imposed by ICAO, ensuring their compatibility and global recognition.

There is a significant security risk with regard to the security of the electronic passport issuing system as the personal data of document holders may be exposed or compromised. And for this reason, the authorities responsible for issuing e-passports need to take rigorous preventive measures to protect the system against cyber-attacks, while at the same time implementing robust security protocols and constantly updating the protection technology.

Regular testing of the passport system is crucial for identifying possible vulnerabilities, i.e. security breaches that could be exploited by potential attackers.

In other words, it is crucial that the electronic passport system is seriously addressed with regard to cyber risk and that a proactive approach is taken to ensure the integrity of the personal data of electronic passport holders.

At the same time, it is important for holders of electronic passports to be vigilant in providing data and information regarding their data or about the passport and, at the same time, not to provide or hand over the document to other suspicious persons. It is also necessary to handle the documents properly, without leaving the opportunity for this document to fall into the hands of any impostor.

[23] Online source: https://learn.microsoft.com/en-us/defender-for-identity/credential-access-alerts, accessed on 7 August 2024 - definition taken and adapted

Sources and bibliography

[1]. Brown, A., Jones, M., ”Fraudulent Use of Electronic Passports: Trends and Security Measures”, published in International Journal of Criminology, 2020.

[2]. Cornea, V., "Evoluția și implicațiile sociale ale pașaportului: de la scrisori de liberă circulație la pașapoarte de aur", published in The Scientific of Cahul State University B.P. Hașdeu: Social Scinces, no. 1(11), 2020.

[3]. Costea, S.G., Porojan, M., Sbîrlea, C., Popa, V., Regimul juridic al liberei circulații a cetățenilor români, printed at C.N. "Imprimeria naţională" S.A., Bucharest 2019.

[4]. Johnson, R., Smith, K., "The Impact of Identity Theft on Victims: A Comprehensive Study", published in the Journal of Criminology, 2018.

[5]. Smith, J. ”Cyber Espionage: The Case of Biometric Data Theft”, published in the Journal of Cybersecurity, 2015.

[6]. Council Regulation (EC) No 2252/2004 of December 13, 2004, on security standards and biometric data in passports and travel documents issued by Member States, published in the Official Journal of the European Union no. L 385/1 of December 29, 2004, as subsequently amended and supplemented.

[7]. Law no. 146 of July 12, 2016, amending Law no. 102/1992 on the coat of arms of the country and the state seal, published in the Official Gazette no. 542 of July 19, 2016.

[8]. Law no. 248 of July 20, 2005, on the regime of free movement of Romanian citizens abroad, published in the Official Gazette no. 682 of July 29, 2005, as subsequently amended and supplemented.

[9]. Government Decision no. 46 of May 9, 2001 regarding the putting into circulation of the new types of Romanian passports, published in the Official Gazette no. 272 of May 25, 2001.

[10]. Government Decision no. 757 of December 30, 1993, on the putting into circulation of the new Romanian passports, published in the Official Gazette no. 24 of January 26, 1994.

[11]. https://www.bbc.com/news/technology-46401890

[12]. http://centenar.gov.ro/web/marea-unire/

[13]. www.cnin.ro/pasapoarte.php

[14]. https://www.icao.int/publications/Documents

[15]. https://www.govinfo.gov/content/pkg/PLAW-107publ173/pdf/PLAW-107publ173.pdf

[16]. https://www.researchgate.net/publication/341357883_Evolutia_si_implicatiile_sociale_ale_pasaportului_de_la_scrisori_de_libera_trecere_la_pasapoarte_de_aur_The_evolution_and_social_implications_of_the_passport_from_the_free_passage_letters_to_golden_pa

[17]. https://www.microsoft.com/ro-ro/security/business/security-101/what-is-malware

[18]. https://www.microsoft.com/ro-ro/security/business/security-101/what-is-phishing

[19]. https://learn.microsoft.com/en-us/defender-for-identity/credential-access-alerts

[20]. https://pasapoarte.mai.gov.ro/wp-content/uploads/2021/03/comunicat-ZiuaPAS-2011.pdf

An Analysis on Security and Reliability of Storage Devices

Ana-Maria DINCĂ, Gabriel PETRICĂ, PhD
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
ana_maria.dinca@stud.etti.upb.ro, gabriel.petrica@upb.ro

Abstract

The secure storage of information is an essential objective for companies, especially if that information has a classification level that requires medium or maximum protection. This paper analyzes two components of dependability: ensuring the security of backup data must be complemented with the analysis of the reliability of storage media. For this, S.M.A.R.T. technology provides information about the wear of a storage unit (magnetic, optical or flash memory) and allows the prevention of data loss when the storage equipment is nearing the end of its useful life.

Index terms: backup security, data storage, information classification, reliability, S.M.A.R.T. technology

1. Classification of information

Classification of data into well-defined categories has long been a process left solely to the discretion of the user, but it can now be automated within organizations, establishing processes that allow users to categorize the documents they create, send or modify. Alternatively, organizations can classify their existing data using a process of scanning file structures and reporting the results. In October 2022, the ISO/IEC 27001:2022 [1] standard was published, whereby information is classified into following 4 categories, depending on the required level of protection (Figure 1):

- *Public*: the information is intended for the public and can be made public without implications for the company (no impact of disclosure / security breaches). Information integrity is important, but not vital.
- "*Internal Only*" use (medium sensitivity): access to information is limited only from within the organization and must be protected against external access. Unauthorized access could impact the operational effectiveness of the organization, cause significant financial loss, provide significant growth to a competitor, or cause a major decrease in customer confidence. Information integrity is vital.
- *Restricted* (high degree of sensitivity): information received from customers, in any form, for processing in production by the company. The information must not be changed in any way without the written permission of the customer. The highest levels of integrity, confidentiality and availability are necessary and vital.
- *Highly Confidential* (secret): the information collected and used by the organization in carrying out the activity: staff hiring, authentication and fulfillment of customer requirements, management of all aspects related to financial aspects, etc. Access to this information is highly restricted within the organization. The highest levels of integrity, confidentiality and availability are necessary and vital.

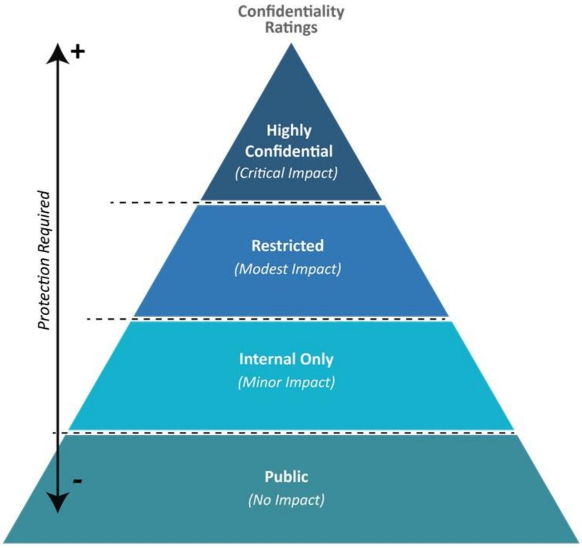


Fig. 1. Classification of information [2]

Every computer system (both servers and workstations) should be protected against the loss of information confidentiality (C), integrity (I) and availability (A), the three components (C-I-A Triad) that define information security according to ISO 27000.

Determining the protection level for a system is mainly based on the type of information stored and processed. Considering the potential impact of a security breach in a system, security levels can be divided into three categories: low, moderate and high [3]. A low level of security may be adopted if the loss of C-I-A of information will have limited consequences (no or minor impact) on the organization's or users' operations and assets. A moderate level of security is chosen if the loss of C-I-A of information will have significant consequences for the operations and assets of the organization or individuals (major impact). This category includes incidents as a result of which the organization can carry out its basic activities, but their efficiency is significantly reduced, there are large financial losses, there are major employee accidents (which do not involve loss of human life). Finally, a high level of security should be chosen if the loss of C-I-A of information will have catastrophic consequences (critical impact) on the operations and assets of the organization or individuals. Such very serious consequences can be the inability of the company to carry out its core activities for a limited period, very large financial losses, or a major employee accident occurring with possible loss of life.

By classifying data, two objectives are achieved: data security is improved and compliance with the regulations in force is ensured. In order to ensure the security of critical data (within the organization, of customers or partners, etc.) it is first necessary to know and understand this data, and for this purpose the following aspects must be analyzed:

- type of sensitive data held - Intellectual Property (IP), medical records (Protected Health Information, PHI), personal data (Personally Identifiable Information, PII), financial or banking information, etc. According to NIST, Personally Identifiable Information is “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information” [4].
- where this sensitive data is located;
- who can access / modify / delete this data;
- how the organization's activity will be affected if this data is disclosed, destroyed or modified inappropriately.

To comply with current regulations, organizations must protect specific data such as information about bank cardholders (according to PCI DSS - Payment Card Industry Data Security Standard, 2004), medical records (HIPAA - Health Insurance Portability and Accountability Act, 1996), financial data (SOX - Sarbanes-Oxley Act, 2002) or personal data of European Union residents (GDPR - General Data Protection Regulation, 2016). Identifying and classifying data will locate sensitive types of data, select necessary security controls, and comply with regulatory requirements regarding data search and monitoring. Thus, by complying with the regulations in force, an organization's chances of successfully passing various audits and controlling the flow of sensitive data increase.

2. Ensuring the security and availability of electronic data

The operation of data storage media and the long-term availability of stored data may be affected by factors such as hardware failures, storage device failures, cyber-attacks, natural disasters or human errors. Frequent use of backups reduces the risks associated with these aspects and ensures efficient and complete data recovery in the event of an unfortunate event. However, there are some issues that need to be considered to ensure the integrity and accessibility of these backups over time.

One of the main aspects is the selection of a suitable storage medium for backups. This involves evaluating the various storage technologies available, such as magnetic disks, optical media, flash memory and cloud storage. Each technology has advantages and disadvantages in terms of long-term data reliability and durability. High-quality storage media that are resistant to wear and corrosion provide better protection for stored data. In addition, environmental conditions such as temperature, humidity and exposure to external factors such as sunlight or electromagnetic sources can affect the reliability of storage media [5].

In addition to the physical quality of the storage media, the implementation of a backup system plays a crucial role in ensuring long-term data reliability. Backup systems must be able to perform regular data backups and provide effective recovery options in the event of data loss or corruption. It is also important to consider using multiple storage locations for backups to minimize the risk of total loss in extreme situations such as fire or natural disasters. Data security is another crucial aspect in the long-term reliability of storage media. Backups must be protected against unauthorized access and cyber-attacks. The use of strong encryption and authentication methods, as well as the implementation of strict security and monitoring policies, help protect stored data [6].

However, there are also challenges regarding the reliability of long-term data storage media. Technologies evolve rapidly, and some storage media may become obsolete or incompatible over time. Therefore, planning and constantly updating the storage infrastructure is essential to ensure long-term data compatibility and availability. One of the major challenges is the physical degradation of storage media over time. Storage devices such as hard drives, SSDs or CDs are susceptible to wear and tear as they are exposed to factors such as extreme temperatures, humidity, mechanical shocks or electromagnetic radiation. This can lead to reading errors or data corruption in the long run. Thus, it is important to consider storage conditions and regularly monitor the condition of storage media to prevent potential problems [7].

3. Reliability analysis of storage equipment using SMART technology

In this chapter we compared 4 units for data storage with 2 different technologies: 2 HDD (hard-disk drive, magnetic storage) and 2 SSD (solid-state drive, NAND flash memory). Their technical specifications are presented in Table 1.

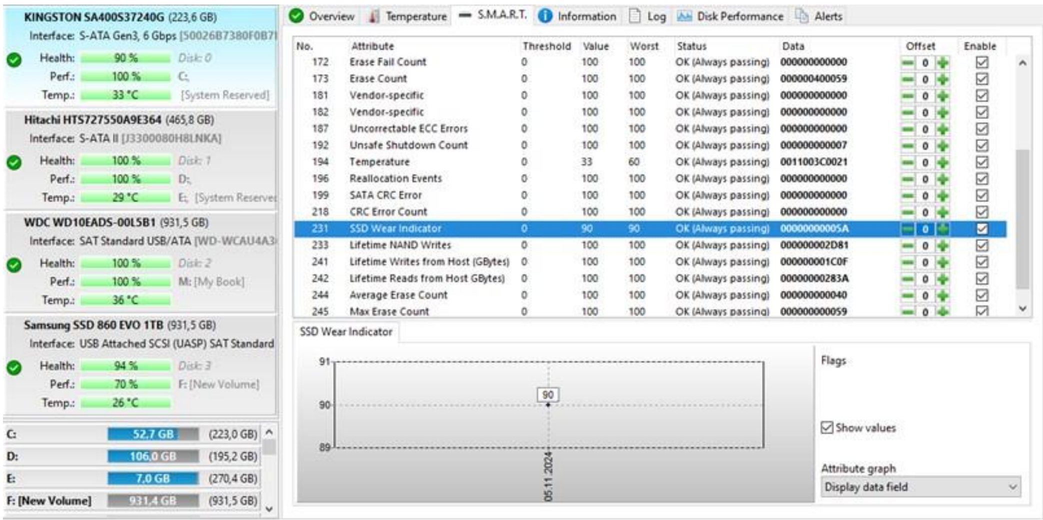
Table 1. The analyzed data storage units

Type	SSD	SSD	HDD	HDD
Model	SA400S37240G	860 EVO 1TB	HTS727550A9E364	WD10EADS-00L5B1
Manufacturer	Kingston	Samsung	Hitachi	Western Digital
Drive Capacity	240 GB	1000 GB	500 GB	1000 GB
Controller	Serial ATA 6Gb/s	Serial ATA 6Gb/s (USB)	Serial ATA 3Gb/s	Serial ATA 3Gb/s (USB)
Security Feature	Supported	Supported	Supported	Supported
Enhanced Security Erase	Supported	Supported	Supported	Supported
S.M.A.R.T. feature	Present, Active	Present, Active	Present, Active	Present, Active

Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) is an industry standard that can be used as a reliability prediction indicator for IDE/ATA and SCSI storage units. Proposed by IBM in 1992, S.M.A.R.T. refers to a method of signaling between the sensors in the disk drive and the host computer [8]. The technology monitors the computer's physical disk drives to detect and report various indicators. In this way, failures can be predicted, and users are warned of impending failure of the entire disk drive, allowing for early drive replacement to avoid data loss and/or unexpected service interruptions. S.M.A.R.T. can only warn of predictable errors, which result from slow processes (such as mechanical ones or wear) and can be anticipated by analyzing certain indicators. Unpredictable failures, such as a sudden mechanical failure resulting from an electrical surge, cannot be monitored and analyzed.

S.M.A.R.T. uses a multitude of operating parameters expressed as a *raw value*, which can only take values between certain manufacturer-dependent limits (e.g. 0-100, 0-200 or 0-253) or a *normalized value* calculated with the formula INT [x - (raw_value / max_raw_value) * x], where *max_raw_value* represents the maximum value that the parameter can take. Normalization is used to represent the performance of a device independent of the *max_raw_value* (which is manufacturer dependent). Normalized values are usually mapped so that higher values are better (with some exceptions).

In general, S.M.A.R.T. parameters start from a maximum value and decrease throughout the life of the storage unit. Other terms used by S.M.A.R.T. are "*worst*" - the worst normalized value recorded for a parameter and "*threshold*" - the threshold value that, once reached, triggers an alarm about the need for action (for example, replacing the drive). In Figure 2 we used Hard Disk Sentinel monitoring and analysis software [9] for our 4 data storage units analyzed in this paper.



KINGSTON SA400S37240G (223,6 GB)
Interface: S-ATA Gen3, 6 Gbps [50026B7380F0B7
Health: 90 % Disk: 0
Perf.: 100 % C:
Temp.: 33 °C [System Reserved]

Hitachi HTS727550A9E364 (465,8 GB)
Interface: S-ATA II [J3300080H8LNKA]
Health: 100 % Disk: 1
Perf.: 100 % D:
Temp.: 29 °C E: [System Reserve

WDC WD10EADS-00L5B1 (931,5 GB)
Interface: SAT Standard USB/ATA [WD-WCAU4A3
Health: 100 % Disk: 2
Perf.: 100 % M: [My Book]
Temp.: 36 °C

Samsung SSD 860 EVO 1TB (931,5 GB)
Interface: USB Attached SCSI (UASP) SAT Standard
Health: 94 % Disk: 3
Perf.: 70 % F: [New Volume]
Temp.: 26 °C

C:	52,7 GB	(223,0 GB)
D:	106,0 GB	(195,2 GB)
E:	7,0 GB	(270,4 GB)
F: [New Volume]	931,4 GB	(931,5 GB)

No.	Attribute	Threshold	Value	Worst	Status	Data	Offset	Enable
172	Erase Fail Count	0	100	100	OK (Always passing)	000000000000	0	☑
173	Erase Count	0	100	100	OK (Always passing)	000000400059	0	☑
181	Vendor-specific	0	100	100	OK (Always passing)	000000000000	0	☑
182	Vendor-specific	0	100	100	OK (Always passing)	000000000000	0	☑
187	Uncorrectable ECC Errors	0	100	100	OK (Always passing)	000000000000	0	☑
192	Unsafe Shutdown Count	0	100	100	OK (Always passing)	000000000007	0	☑
194	Temperature	0	33	60	OK (Always passing)	0011003C0021	0	☑
196	Reallocation Events	0	100	100	OK (Always passing)	000000000000	0	☑
199	SATA CRC Error	0	100	100	OK (Always passing)	000000000000	0	☑
218	CRC Error Count	0	100	100	OK (Always passing)	000000000000	0	☑
231	SSD Wear Indicator	0	90	90	OK (Always passing)	00000000005A	0	☑
233	Lifetime NAND Writes	0	100	100	OK (Always passing)	000000002D81	0	☑
241	Lifetime Writes from Host (GBytes)	0	100	100	OK (Always passing)	000000001C0F	0	☑
242	Lifetime Reads from Host GBytes)	0	100	100	OK (Always passing)	00000000283A	0	☑
244	Average Erase Count	0	100	100	OK (Always passing)	000000000040	0	☑
245	Max Erase Count	0	100	100	OK (Always passing)	000000000059	0	☑

☑ Show values

Attribute graph: Display data field

Fig. 2. Threshold, current and worst values for S.M.A.R.T. attributes displayed in Hard Disk Sentinel

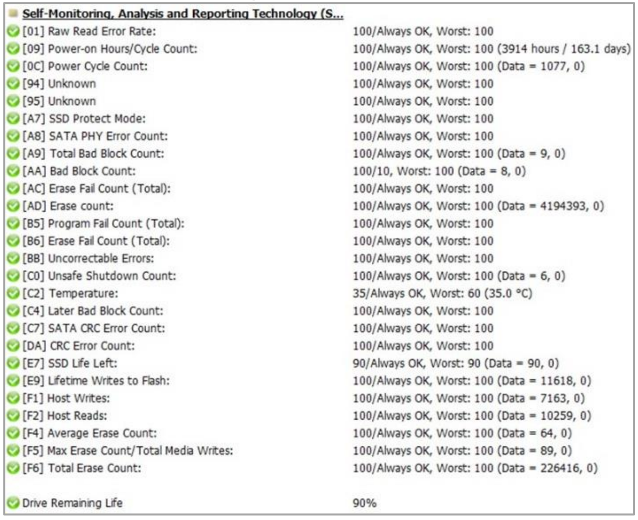
Drives can report a S.M.A.R.T. status usually reported as one of two values, typically "*drive OK*" / "*drive fail*" or "*threshold not exceeded*" / "*threshold exceeded*". A "*drive fail*" or "*threshold exceeded*" value indicates that there is a high probability that the unit will fail soon. However, the failure may not be catastrophic, with the S.M.A.R.T. status indicating that the drive will not perform according to the manufacturer's stated specifications (e.g. the drive will run more slowly).

Manufacturers do not necessarily agree on the precise definitions of all attributes and reference values, so in general there are known attributes, supported by IDE and Serial ATA drives, but also non-standard attributes, specific to each manufacturer, used for various purposes (even commercial secrets) [10]. Also, some codes are specific to certain types of drives (fixed magnetic media, flash memory, etc.), and drives may use different codes for the same parameter [11]. Raw values with higher values may be better or worse depending on the attribute and manufacturer.

Using HWINFO [12] we extracted relevant S.M.A.R.T. parameters, specific for the four analyzed disk units (see Table 2):

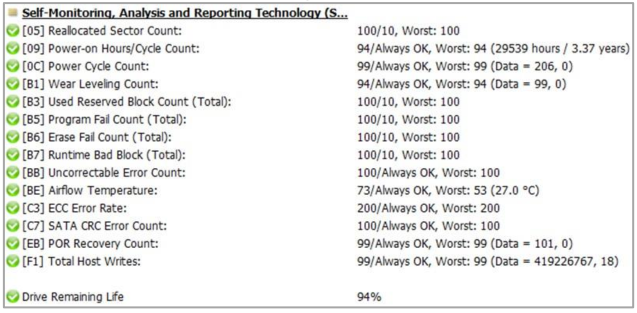
Table 2. S.M.A.R.T. parameters

SSD Kingston SA400S37240G



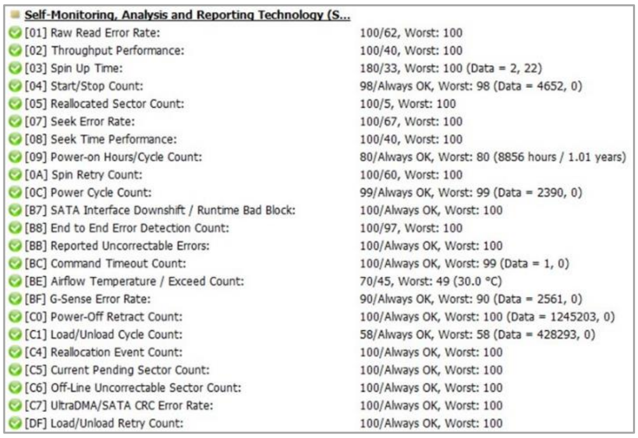
```
Self-Monitoring, Analysis and Reporting Technology (S...
[01] Raw Read Error Rate:                     100/Always OK, Worst: 100
[09] Power-on Hours/Cycle Count:              100/Always OK, Worst: 100 (3914 hours / 163.1 days)
[0C] Power Cycle Count:                       100/Always OK, Worst: 100 (Data = 1077, 0)
[94] Unknown                                  100/Always OK, Worst: 100
[95] Unknown                                  100/Always OK, Worst: 100
[A7] SSD Protect Mode:                        100/Always OK, Worst: 100
[A8] SATA PHY Error Count:                    100/Always OK, Worst: 100
[A9] Total Bad Block Count:                   100/Always OK, Worst: 100 (Data = 9, 0)
[AA] Bad Block Count:                         100/10, Worst: 100 (Data = 8, 0)
[AC] Erase Fail Count (Total):                100/Always OK, Worst: 100
[AD] Erase count:                             100/Always OK, Worst: 100 (Data = 4194393, 0)
[B5] Program Fail Count (Total):              100/Always OK, Worst: 100
[B6] Erase Fail Count (Total):                100/Always OK, Worst: 100
[BB] Uncorrectable Errors:                    100/Always OK, Worst: 100
[C0] Unsafe Shutdown Count:                   100/Always OK, Worst: 100 (Data = 6, 0)
[C2] Temperature:                             35/Always OK, Worst: 60 (35.0 °C)
[C4] Later Bad Block Count:                   100/Always OK, Worst: 100
[C7] SATA CRC Error Count:                    100/Always OK, Worst: 100
[DA] CRC Error Count:                         100/Always OK, Worst: 100
[E7] SSD Life Left:                           90/Always OK, Worst: 90 (Data = 90, 0)
[E9] Lifetime Writes to Flash:                100/Always OK, Worst: 100 (Data = 11618, 0)
[F1] Host Writes:                             100/Always OK, Worst: 100 (Data = 7163, 0)
[F2] Host Reads:                              100/Always OK, Worst: 100 (Data = 10259, 0)
[F4] Average Erase Count:                     100/Always OK, Worst: 100 (Data = 64, 0)
[F5] Max Erase Count/Total Media Writes:      100/Always OK, Worst: 100 (Data = 89, 0)
[F6] Total Erase Count:                       100/Always OK, Worst: 100 (Data = 226416, 0)

Drive Remaining Life                          90%
```

SSD Samsung 860 EVO 1TB



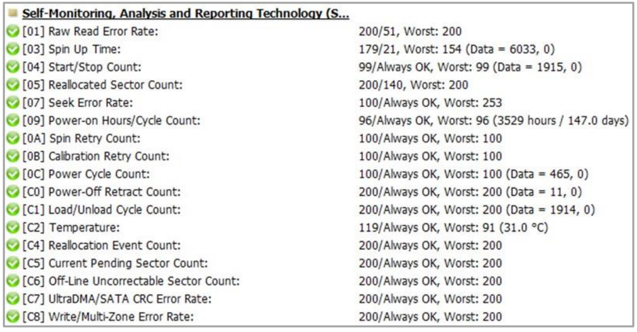
```
Self-Monitoring, Analysis and Reporting Technology (S...
[05] Reallocated Sector Count:                100/10, Worst: 100
[09] Power-on Hours/Cycle Count:              94/Always OK, Worst: 94 (29539 hours / 3.37 years)
[0C] Power Cycle Count:                       99/Always OK, Worst: 99 (Data = 206, 0)
[B1] Wear Leveling Count:                     94/Always OK, Worst: 94 (Data = 99, 0)
[B3] Used Reserved Block Count (Total):       100/10, Worst: 100
[B5] Program Fail Count (Total):              100/10, Worst: 100
[B6] Erase Fail Count (Total):                100/10, Worst: 100
[B7] Runtime Bad Block (Total):               100/10, Worst: 100
[BB] Uncorrectable Error Count:               100/Always OK, Worst: 100
[BE] Airflow Temperature:                     73/Always OK, Worst: 53 (27.0 °C)
[C3] ECC Error Rate:                          200/Always OK, Worst: 200
[C7] SATA CRC Error Count:                    100/Always OK, Worst: 100
[EB] POR Recovery Count:                      99/Always OK, Worst: 99 (Data = 101, 0)
[F1] Total Host Writes:                       99/Always OK, Worst: 99 (Data = 419226767, 18)

Drive Remaining Life                          94%
```

HDD Hitachi HTS727550A9E364



```
Self-Monitoring, Analysis and Reporting Technology (S...
[01] Raw Read Error Rate:                             100/62, Worst: 100
[02] Throughput Performance:                          100/40, Worst: 100
[03] Spin Up Time:                                    180/33, Worst: 100 (Data = 2, 22)
[04] Start/Stop Count:                                98/Always OK, Worst: 98 (Data = 4652, 0)
[05] Reallocated Sector Count:                        100/5, Worst: 100
[07] Seek Error Rate:                                 100/67, Worst: 100
[08] Seek Time Performance:                           100/40, Worst: 100
[09] Power-on Hours/Cycle Count:                      80/Always OK, Worst: 80 (8856 hours / 1.01 years)
[0A] Spin Retry Count:                                100/60, Worst: 100
[0C] Power Cycle Count:                               99/Always OK, Worst: 99 (Data = 2390, 0)
[B7] SATA Interface Downshift / Runtime Bad Block:    100/Always OK, Worst: 100
[B8] End to End Error Detection Count:                100/97, Worst: 100
[BB] Reported Uncorrectable Errors:                   100/Always OK, Worst: 100
[BC] Command Timeout Count:                           100/Always OK, Worst: 99 (Data = 1, 0)
[BE] Airflow Temperature / Exceed Count:              70/45, Worst: 49 (30.0 °C)
[BF] G-Sense Error Rate:                              90/Always OK, Worst: 90 (Data = 2561, 0)
[C0] Power-Off Retract Count:                         100/Always OK, Worst: 100 (Data = 1245203, 0)
[C1] Load/Unload Cycle Count:                         58/Always OK, Worst: 58 (Data = 428293, 0)
[C4] Reallocation Event Count:                        100/Always OK, Worst: 100
[C5] Current Pending Sector Count:                    100/Always OK, Worst: 100
[C6] Off-Line Uncorrectable Sector Count:             100/Always OK, Worst: 100
[C7] UltraDMA/SATA CRC Error Rate:                    100/Always OK, Worst: 100
[DF] Load/Unload Retry Count:                         100/Always OK, Worst: 100
```

HDD Western Digital WD10EADS-00L5B1



```
Self-Monitoring, Analysis and Reporting Technology (S...
[01] Raw Read Error Rate:                     200/51, Worst: 200
[03] Spin Up Time:                            179/21, Worst: 154 (Data = 6033, 0)
[04] Start/Stop Count:                        99/Always OK, Worst: 99 (Data = 1915, 0)
[05] Reallocated Sector Count:                200/140, Worst: 200
[07] Seek Error Rate:                         100/Always OK, Worst: 253
[09] Power-on Hours/Cycle Count:              96/Always OK, Worst: 96 (3529 hours / 147.0 days)
[0A] Spin Retry Count:                        100/Always OK, Worst: 100
[0B] Calibration Retry Count:                 100/Always OK, Worst: 100
[0C] Power Cycle Count:                       100/Always OK, Worst: 100 (Data = 465, 0)
[C0] Power-Off Retract Count:                 200/Always OK, Worst: 200 (Data = 11, 0)
[C1] Load/Unload Cycle Count:                 200/Always OK, Worst: 200 (Data = 1914, 0)
[C2] Temperature:                             119/Always OK, Worst: 91 (31.0 °C)
[C4] Reallocation Event Count:                200/Always OK, Worst: 200
[C5] Current Pending Sector Count:            200/Always OK, Worst: 200
[C6] Off-Line Uncorrectable Sector Count:     200/Always OK, Worst: 200
[C7] UltraDMA/SATA CRC Error Rate:            200/Always OK, Worst: 200
[C8] Write/Multi-Zone Error Rate:             200/Always OK, Worst: 200
```

In Table 2, SSD Life Left attribute for Kingston SA400S37240G (same as SSD Wear Indicator in Figure 2) indicates a wear level of 10% for the analyzed SSD drive. "SSD life left is based on actual usage and takes into account PE cycle consumption (life curve status) and Flash block retirement" [13]. For hard-disk drives, the attributes Power On Time Count (Hard Disk Sentinel) and Power-on Hours (Hwinfo) had values of 8,869 (Hitachi) and 3,532 (WDC), respectively, indicating a health level of 100 % ("the total expected lifetime of a hard disk in perfect condition is defined as 5 years... 43,800 hours)" [14].

4. Conclusions

Information is an asset that, like other important assets of a business or an individual, has a certain value and therefore must be properly protected. The limited resources that organizations invest in data protection lead to the need to develop a taxonomy that allows organizations to identify priorities and develop a plan that optimizes costs and effectively protects sensitive data. Data classification provides a solid foundation for a security strategy that correctly identifies areas of risk both within the network and in the cloud, enables more effective data protection and compliant use.

Therefore, data backup strategies (especially for confidential data) must consider the reliability of the equipment that stores this data. For the data to be safe and available, both scenarios regarding the limitation of access to them and the use of reliable storage media must be analyzed, an aspect to which S.M.A.R.T. technology can make its contribution.

References

[1]. ISO - International Organization for Standardization, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, https://www.iso.org/standard/27001

[2]. SecureLink, Information Classification, https://www.securelinkme.net/information-classification

[3]. G. Petrică, S.D. Axinte, I.C. Bacivarov, Dependabilitatea sistemelor informatice, Matrix Rom, 2019, ISBN 978-606-25-0529-5.

[4]. NIST Special Publication 800-122. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), 2010, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

[5]. S. Yarrapothu, "Effectiveness of Backup and Disaster Recovery in Cloud - A Comparative study on Tape and Cloud based Backup and Disaster Recovery", pp. 5-40.

[6]. D. Kaeli, "ACM Transactions on Architecture and Code Optimization", 2022, Volume19, Number 3, pp. 123-150, 179-201.

[7]. C. Yan, "Cloud Storage Services"- Thesis, Centria University of Applied Sciences, June 2017, pp. 4-18.

[8]. Samsung, S.M.A.R.T. - Self-Monitoring, Analysis and Reporting Technology, 2014, https://download.semiconductor.samsung.com/resources/others/SSD_Application_Note_SMART_final.pdf

[9]. Hard Disk Sentinel - HDD health and temperature monitoring, https://www.hdsentinel.com/

[10]. S.M.A.R.T. attribute list (ATA), https://www.hdsentinel.com/smart/smartattr.php

[11]. Hetman Software, SMART Parameters and Early Signs of a Failing Hard Disk, 2019, https://medium.com/hetman-software/smart-parameters-and-early-signs-of-a-failing-hard-disk-23dfec568808

[12]. HWINFO, Professional System Information and Diagnostics, https://www.hwinfo.com/.

[13]. Kingston, SMART Attribute Details, 2015, https://media.kingston.com/support/downloads/MKP_306_SMART_attribute.pdf

[14]. Hard Disk Sentinel Help - Power on time, https://www.hdsentinel.com/help/en/54_pot.html

Cybercrime: A New Challenge of Criminality in the Digital Age

Marius-Andrei OROȘANU[1], Mihăiță ALEXANDRU[2]
[1] "Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
andrei.orosanu@academiadepolitie.ro
[2] General Police Directorate of The Municipality of Bucharest, Romania
mihaita.alexandru@b.politiaromana.ro

Abstract

Cybercrime, encompassing a broad spectrum of illicit activities executed through digital technologies, poses a critical threat to global security, economics, and individual privacy. Key methods, such as phishing, exploit user vulnerabilities by using deceptive techniques to acquire sensitive personal and financial data. Phishing-related offenses are explicitly addressed within legal frameworks, such as those outlined in the Penal Code, where they are classified under offenses against property and public safety. This underscores the integral role of legal structures in mitigating the growing risks posed by cybercrime, particularly as technological advancements enhance the complexity of such criminal activities. Additionally, the widespread use of fake websites for phishing purposes heightens the dangers of identity theft, financial fraud, and compromised banking systems, with long-lasting implications for victims' credit scores and financial stability.

Index terms: cybercrime, phishing, website, cyberattack, financial crime

1. Introduction

Cybercrime, also known as cyber criminality, represents one of the greatest challenges of the 21st century, having a significant impact on the economy, national security, and the daily lives of citizens. With the development of digital technologies and global interconnectivity, cybercriminals have found new ways to exploit computer vulnerabilities to commit crimes, ranging from the theft of personal and financial data to attacks on critical infrastructures, encompassing any illicit activity conducted through computer systems.

Globally, these crimes are perpetrated by individual offenders, hacker groups, or even nation-states using cyber technologies to achieve specific goals. Cybercrime manifests in a wide range of illegal activities, with **phishing** being one of the most notable methods. Phishing involves deceiving victims in various ways, leading them to voluntarily provide personal information, such as authentication data for different computer systems (banking applications, online payment websites, etc.).

One of the most common phishing techniques involves creating fake web pages that mimic the official sites of banking institutions, specifically designed to mislead users into entering their personal and banking information, thereby enabling the perpetrators to achieve their fraudulent goals. Thus, phishing is closely linked to criminal acts falling within the scope of penal illegality, as defined in the special part of the New Romanian Penal Code, specifically:

- Title II. Offenses against Property. Chapter IV. Frauds Committed through Computer Systems and Electronic Payment Methods.

- Title VII. Offenses against Public Safety. Chapter VI. Offenses against the Safety and Integrity of Computer Systems and Data.

2. General considerations regarding cyber attacks

At times, an event that occurs on a computer or within a network is part of a larger sequence of actions designed to result in an unauthorized outcome. Such an event is subsequently classified as an integral component of an attack. An attack is not a singular occurrence, but rather a multi-faceted process involving numerous stages. During these stages, the attacker typically undertakes actions specifically directed at a particular target, often utilizing tools or techniques to exploit identified vulnerabilities within the system.

The overarching goal of this process is to achieve an unauthorized result, which is considered illicit or undesirable from the perspective of the system's user or administrator. This could involve unauthorized access, data theft, or disruption of services, all of which are outcomes the system is designed to prevent. Unlike routine, benign activities that occur on a system, an attack is defined by the intentional and methodical nature of the steps taken by the attacker. The calculated progression through these stages, aimed at undermining the system's integrity or security, distinguishes an attack from ordinary or legitimate sequences of operations. Each stage in the process reflects the attacker's deliberate effort to circumvent protective measures, culminating in an outcome that breaches the security or intended use of the system [1].

Based on their attributes, including the resources they use, the time and tools at their disposal, and the level of risk they are willing to assume, a profile can be established for cybercriminals. The most common profiles include the following:

- **Recreational or exploratory hacker** – This individual possesses limited technical knowledge and may operate as part of a team using tools readily available on the internet. However, they often do not fully understand or appreciate the risks involved. They tend to be patient but typically seek out opportunistic scenarios rather than orchestrating complex attacks.
- **Disgruntled employee** – Lacking technical expertise, this individual, similar to the recreational hacker, uses readily available resources from the internet. Unlike the previous type, the disgruntled employee is more willing to accept the risks associated with their actions. Motivated by dissatisfaction, they exploit the tools and vulnerabilities they have access to, often from within the organization.
- **Activist targeting an organization for political or ethnic reasons** – Generally, this type of cybercriminal does not have specialized technical skills and relies on third-party services for execution. While they may exhibit patience, certain circumstances may compel them to act hastily. Similar to the other profiles, they also use publicly available resources and are generally risk-averse in their approach.
- **Industrial operative spy** – An industrial spy in the context of cybercrime often engages in data breaches to illegally obtain sensitive information such as trade secrets, proprietary technologies, or business strategies from competing organizations. They customize their tools and resources to suit the specific objectives of their attacks. Although technically proficient, they do not fully embrace the risks involved, often carefully weighing their actions to avoid detection or failure.
- **Cybercrime group or organization** – Distinct from previous individuals, this category includes groups or organizations, which can vary significantly based on their goals, resources, and the time they invest in criminal activities. Such groups operate based on the intelligence they gather and in the absence of information, they are willing to wait

patiently. Their objectives often revolve around acquiring material gains or large sums of money. These groups develop their own resources and customize their tools to maximize efficiency and success [2].

3. Phishing

Phishing is a broad term used to describe any type of cyberattack in which an attacker impersonates a trusted source to obtain sensitive information. In traditional phishing schemes, attackers typically distribute fraudulent and malicious emails to a large number of recipients. It is common for phishing campaigns to target thousands of individuals simultaneously, aiming to deceive only a small fraction of the intended audience.

Phishing attacks prioritize quantity over precision. Despite the indiscriminate nature of these attacks, cybercriminals can still gather valuable information from their victims through easily replicable, mass-distributed emails. The primary objective of such emails is to compromise personal data or infiltrate larger networks by exploiting the most significant cybersecurity vulnerability: the human user. Rather than attempting to breach sophisticated digital defenses directly, attackers leverage phishing techniques to deceive individuals into willingly granting access to sensitive data or systems.

To increase the likelihood of success, attackers often customize phishing emails to make them appear authentic, using official logos or fake email addresses that mimic legitimate sources. Phishers typically pose as trusted entities such as hospitals, financial institutions, or employers. These messages are crafted with alarming or urgent language to pressure victims into taking actions that may include clicking on malicious links, downloading malware-infected attachments, or providing personal credentials.

Once a victim complies, the attacker can compromise their system and extract sensitive data, often without needing to use advanced technical methods or even a single line of code. Not even the most advanced firewall can prevent a user from clicking on a malicious email, and once a single computer is infected, the malware can propagate across the entire network, posing a significant threat to the organization’s security infrastructure.

3.1. Phishing via Fake Bank Websites

Accessing and providing personal information on fraudulent websites can have severe consequences for users, as follows:

- **Identity Theft**: Personal information obtained through phishing (such as national identification numbers or identity card details) can later be used to open bank accounts, apply for loans, or commit other types of fraud in the victim's name.
- **Theft of Funds**: When attackers acquire banking details, they can directly access the victim's accounts, draining them or conducting unauthorized transactions.
- **Compromise of Bank Cards**: If credit or debit card details are stolen, they can be used for illegal purchases or to withdraw cash from ATMs.
- **Credit Score Damage**: Identity theft and illegal use of banking data can result in a decline in the victim’s credit score, making it more difficult to secure loans in the future.

3.2. How Does Phishing via Fake Bank Websites Work?

The main stages of a phishing attack using fake bank websites are as follows:

- **Creation of a Fake Website**: Attackers develop a website that closely resembles the official site of a bank. It may include the bank’s logo, colors, text, and even a subtly modified URL (for example, instead of "bank.com," the URL might be "bank-security.com").

- **Distribution of the Fraudulent Link**: Victims receive links to the fake website through emails, SMS, or social media, accompanied by an urgent message requesting immediate action (e.g., "Your account has been blocked. Please log in to reactivate your account.").
- **Provision of Information**: Once the victim accesses the page and enters login credentials or banking information, the data is captured by the attackers in real-time.
- **Use of Information**: The attackers use the obtained data to access the real bank accounts, perform illegal transactions, or sell the data on the dark web.

3.3. Preventive and combative measures against bank phishing

To safeguard the security of information systems and protect personal data, authorities and public institutions with relevant responsibilities, along with service providers, non-governmental organizations, and other civil society representatives, engage in collaborative efforts and prevention programs focused on combating cybercrime. These entities, working together, promote policies, best practices, measures, procedures, and minimum security standards for information systems.

In addition, these organizations conduct public awareness campaigns to educate users about the risks of cybercrime. The Ministry of Justice, Ministry of Internal Affairs, Ministry for the Information Society, Romanian Intelligence Service, and Foreign Intelligence Service continuously maintain and update databases related to cybercrime. The National Institute of Criminology, operating under the Ministry of Justice, regularly conducts studies to identify the causes and conditions that contribute to cybercrime and create favorable environments for such offenses.

Moreover, the Ministry of Justice, Ministry of Internal Affairs, Ministry for the Information Society, Romanian Intelligence Service, and Foreign Intelligence Service offer specialized training programs for staff tasked with preventing and countering cybercrime, ensuring they are equipped with the necessary skills and knowledge to address these rapidly evolving threats.

This comprehensive approach, involving coordinated efforts across various sectors, aims to strengthen national cybersecurity and minimize the risks posed by cybercriminal activities [3].

To prevent phishing through fake websites, users must reman vigilant and follow several essential security measures:

- **Verify the URL**: It is essential for users to verify the website’s URL carefully before submitting any information. Legitimate banking websites utilize secure URLs that begin with “https://” and feature accurate domain names. Even the slightest variation in the website's address should prompt immediate caution.
- **Avoid Clicking on Links in Unsolicited Emails or SMS**: Users should avoid clicking on links received in suspicious messages and instead manually navigate to the bank’s official site by entering the address in the browser.
- **Use Two-Factor Authentication (2FA)**: Many banks offer two-factor authentication, which adds an extra layer of security. Even if attackers obtain the password, they would still need a code generated on a secondary device to access the account.
- **Constant Monitoring of Bank Accounts**: Users should regularly check their bank statements to detect any unauthorized transactions.
- **Install Updated Security Software**: A good antivirus program can detect phishing websites and prevent access to them [4].

To combat cybercrime globally, coordinated actions between governments, international organizations, and the private sector are necessary. Key measures include:

- **International Cooperation**: Cybercrimes know no borders, making cooperation between countries essential. Initiatives such as the Budapest Convention (the first international treaty on cybercrime) and collaboration through organizations like Europol and Interpol are crucial in combating these offenses.

- **Education and Awareness**: Both companies and individual users must be educated about cyber risks and adopt solid cybersecurity measures, such as using two-factor authentication and protecting personal data.
- **Investment in Cybersecurity**: Governments and companies must invest heavily in cybersecurity technologies and the development of specialized teams capable of quickly responding to cyberattacks.
- **Legislation and Law Enforcement**: Continuously updating cybersecurity laws and swiftly punishing cybercriminals are essential to reducing cybercrime.

On the other hand, combating cybercrime is an extremely challenging task due to several factors, including:

- **Online Anonymity**: Cybercriminals can operate anonymously or hide their real location by using VPN networks and other encryption techniques, making it difficult to identify them.
- **Technological Dynamics**: Technology evolves rapidly, and cybercriminals constantly change their attack methods, forcing authorities and companies to always be one step behind in implementing security measures [5].
- **Digital Black Market**: On the Dark Web, criminals can easily buy and sell stolen data, hacking tools, and even cyberattack services, facilitating global cybercrime.

The process of collecting data within the digital environment and converting it into legally admissible evidence is determined by the specific clues and leads present in the investigated case. These clues dictate the appropriate investigative procedures that must be followed. For instance, if the investigation begins with an email address (e.g., name@mail.com), the initial priority is typically to establish the identity of the person or entity associated with that address. This may involve tracing the ownership of the email account, determining its activity, and assessing any potential links to the case.

In contrast, if the clue involves a web address (e.g., http://namewebsite.com/webpage), the investigative approach shifts. Investigators should first view the website in question using a browser to gather initial observations. In more comprehensive investigations, specialized software may be employed to download and preserve an exact copy of the entire site for further analysis. It is critical to remember, however, that during such investigative actions, the IP address of the computer used to access or download the website could be recorded by the web server under investigation, potentially exposing the investigating party's identity or location.

Furthermore, users can often be identified and traced by examining log files stored on servers. These logs contain records of user activities and interactions, such as connecting to or disconnecting from the internet, which can provide crucial evidence regarding the timing, location, and identity of the individuals involved. By analyzing these logs, investigators can reconstruct a timeline of digital activities, potentially revealing key actions linked to the case, such as unauthorized access or fraudulent transactions. As a result, careful attention must be paid to these digital traces, as they play a pivotal role in uncovering the full scope of cybercrime [6].

4. Case Study

The following information is based on the operational activity of the General Police Directorate of the Municipality of Bucharest, Romania in combating cybercrime.

I. On December 1, 2021, individuals AB and CD, through unauthorized entry of data, created a fake webpage similar to the internet banking site of X SA bank (accessible via the URL https://login.xn--bcrr-jh5a.com/users/login, appearing in search results for "24 banking X" on Google). Their intent was to produce legal consequences, specifically obtaining credentials necessary to access the bank accounts of the clients through the internet banking service. These actions fall under the provisions of Article 325 of the Romanian Penal Code, which criminalizes the offense of computer-related forgery.

II. On January 1, 2022, AB and CD went to the X SA bank, where they fraudulently used falsified official documents, purportedly issued by Romanian authorities, under the names "CI" and "MD" to present themselves with false identities. Their aim was to deceive the bank employees into opening bank accounts, issuing associated bank cards, and activating internet banking services. These actions fall under the provisions of Article 327 (1) of the Romanian Penal Code, which criminalizes the offense of false identity.

III. On February 1, 2022, AB and CD used two falsified official documents, purportedly issued by Romanian authorities under the names "CI" and "MD," to create user accounts on the K cryptocurrency platform. These actions fall under the provisions of Article 323 of the Romanian Penal Code, which criminalizes the offense of forgery in official documents.

IV. On March 1, 2022, AB and CD, without the consent of the account holder MN, used the login credentials they had obtained through the method described in section I to access the online banking system of X SA bank.

They then illicitly transferred 500,000 lei from MN's bank account to bank accounts under the names "C.I." and "M.D." These actions fall under the provisions of Article 250 (1) and (2) and Article 360 (1), (2), and (3) of the Romanian Penal Code, which criminalize the offenses of fraudulent financial transactions and unauthorized access to an information system.

In an increasingly connected world, the protection of information systems becomes essential. Consequently, Romanian legislation has aligned with international standards, adopting strict measures against cybercrime, which poses a significant threat to the economic and national security of states, as well as the privacy and safety of individual users. As technology advances, cybercrime becomes increasingly sophisticated, requiring global solutions and international cooperation to mitigate its impact. Education, legislation, and innovation in cybersecurity are key to effectively addressing this emerging global challenge.

The ENSA report on cybercrime activity presents the following statistics regarding phishing:

- **26.2 billion** losses in 2019 due to Business Email Compromise (BEC) attacks.
- **42.8%** of all malicious attachments were Microsoft Office documents.
- **667%** increase in phishing scams in just one month during the COVID-19 pandemic.
- **30%** of phishing emails were delivered on Mondays.
- **32.5%** of all emails used the keyword "payment" in the subject line [7].

5. Conclusion

In summary, the increasing prevalence of cybercrime, especially phishing attacks conducted through fake bank websites, underscores the necessity for effective legislative measures to address and mitigate this issue. As cybercriminals adopt more sophisticated methods, it is important for law enforcement agencies to strengthen their capabilities in managing and responding to such threats. The role of the police is significant in investigating cybercrime, enforcing existing laws, and promoting public awareness about the dangers associated with online activities.

Additionally, individuals should understand the importance of being informed and cautious when using devices that store personal information. Familiarity with safe online practices is important in reducing the risk of becoming a victim of cybercriminals. By combining appropriate legal frameworks with public education and proactive law enforcement efforts, it is possible to foster a safer online environment that minimizes the risks of cybercrime and protects personal data.

References

[1]. I.C. Mihai, L. Giurea, "Analiza profilului infractorilor cibernetici", *Criminalitatea informatică,* II, Craiova, Romania: SITECH 2016, pp. 45-52.

[2]. *Manualul Investigatorului în Criminalitatea Informatică*, Ministerul Comunicațiilor și Tehnologiei Informației [Online] Available: https://www.scribd.com/doc/268511908/Manualul-Investigatorului-Criminalitatii-informatice. Accessed: October 6, 2024.

[3]. *Legea nr. 161 din 19 aprilie 2003 cu modificările și completările ulterioare,* Romanian Parliament, Romanian Official Monitor nr. 279 din 21 aprilie 2003. [Online] Available: https://legislatie.just.ro/Public/DetaliiDocument/43323

[4]. *Phishing: A Cyber-Security Guide for Employers and Individuals,* Zywave, 2020 [Online] Available: www.sutcliffeinsurance.co.uk/wp-content/uploads/2020/03/Phishing-Attacks-Guide.pdf Accessed: October 10, 2024.

[5]. *Convenția privind Criminalitatea Informatică,* Council of Europe, 2023 [Online] Available: https://eur-lex.europa.eu/RO/legal-content/summary/convention-on-cyber crime.html. Accessed: October 10, 2024.

[6]. I.C. Mihai, I.F. Popa, B.G. Tătaru, "Procedura investigațiilor online", *Securitatea în Internet,* Craiova, România: SITECH 2008, pp. 146-149.

[7]. *Phising, raportul privind situația amenințărilor,* European Union Agency for Cybersecurity, January 2019-April 2020. [Online] Available: www.enisa.europa.eu/publi cations/report-files/ETL-translations/ro/etl2020-phishing-ebook-en-ro.pdf. Accessed: October 14, 2024.

Analysis of Cyber Threats at the Level of a Distributed Network

Constantin-Alin COPACI, Adelaida STĂNCIULESCU, Ioan C. BACIVAROV
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
constantin.copaci@stud.etti.upb.ro, adelaida.deatcu@stud.etti.upb.ro, ioan.bacivarov@upb.ro

Abstract

Ensuring a high level of security of the networks and IT systems that underpin the delivery of an organization's essential services has become a necessity that involves integrated, comprehensive approaches, the adoption of new and permanent cyber security strategies, significant financial investments and rapid organizational adaptations and ambitious. This article aims to provide a comprehensive analysis of the cyber security of a distributed computer network within an organization. In this context, the article promotes the implementation of proactive tools to strengthen cyber security at the institutional level.

Index terms: cyber security, vulnerability, cyber threats, monitoring, distributed network

1. Introduction

In this article we aim to highlight the diversity of cyber threats facing the organization, as well as draw attention to the importance of active, continuous monitoring and protection against them. Also, the article aims to sensitize users about the associated risks and encourage the implementation of proactive measures to prevent and combat cyber threats.

By being aware of and understanding cyber risks, the organization can take appropriate measures to effectively protect itself and reduce the potential impact of a cyber attack. The analysis of cyber-attacks of the last period revealed a series of significant cyber attacks and events at the global level:

DDoS attacks on Russian banks: At the end of July 2024, several banks in Russia, such as VTB, Gazprombank and Alfa Bank, were targeted by distributed denial-of-service (DDoS) attacks. The attacks were claimed by Ukraine's military intelligence services (HUR) and led to temporary disruptions to bank applications and websites, as well as major telecom operators such as Beeline and Rostelecom. This was one of the largest cyber attack campaigns in the region, reflecting the escalation of cyber conflicts between the two countries [1].

Attacks on the gaming industry: The mobile game "Hamster Kombat", which has more than 250 million players, has been the target of malware attacks targeting users with fake software for Android and Windows. Hackers were able to install spyware and information-stealing programs on players' devices.[2].

Virgin Media cyber attack: In July, Virgin Media was hit by a phishing attack that compromised the data of around 20,000 of the company's users. This was a demonstration of vulnerabilities in the protection systems of telecommunications companies, having consequences on the services offered [3].

Emergence of new ransomware groups: Several ransomware groups emerged during this period, such as "Volcano Demon" and "Eldorado". These groups have carried out attacks on companies in the real estate, education and healthcare sectors using advanced encryption and extortion techniques. "Eldorado" was notable for using ransomware variants adapted for VMware ESXi and Windows [4] [5].

2. Electronic services with Internet access vulnerable to cyber attacks

In general, any service connected to the Internet is exposed to security risks, and vulnerabilities can arise from various causes, such as misconfigurations, outdated software, or the lack of adequate protection measures.

Types of vulnerable electronic services with Internet access commonly found in an organization [6]:

- *Servers and databases*

Common vulnerabilities: Weak or default passwords, unauthorized access, wrong permission settings, outdated software.

Risks: Attackers can gain access to sensitive information such as users' personal data or confidential company files.

- *Online payment systems (e.g. e-commerce)*

Common vulnerabilities: Interception of payment data (if not properly encrypted), man-in-the-middle attacks, insecure storage of payment data.

Risks: Online fraud, theft of users' financial information (e.g. credit cards).

- *Email services*

Common vulnerabilities: Phishing, spoofing attacks, lack of encryption (e.g. TLS), use of weak passwords.

Risks: Theft of confidential information, spread of malware or viruses through infected emails, social typing attacks on users.

- *Cloud services*

Common vulnerabilities: Misconfiguration of permissions, lack of encryption of stored data, unauthorized access to sensitive files.

Risks: Compromise of data stored in the cloud, access and theft of sensitive information (e.g. documents or financial data), unauthorized deletion of files.

- *Websites and web applications*

Common vulnerabilities: Cross-Site Scripting (XSS), SQL Injection, authentication vulnerabilities, lack of encryption (SSL/TLS), lack of security updates.

Risks: Hackers can exploit vulnerabilities to access sensitive data, modify website content, intercept user data, or infect visitors with malware.

- *Virtual Private Networks (VPNs)*

Common vulnerabilities: Insecure VPN protocols, use of compromised VPN servers, weak encryption.

Risks: Exposure of personal data and browsing history, identification and location of users, possibility of being tracked or intercepted data transmitted.

3. Web traffic monitoring

Internet traffic monitoring was carried out to assess how the Internet is used within the organization and to identify potential security issues. Data traffic analysis is essential to understand user behavior and proactively implement appropriate security measures.

Traffic monitoring was carried out on two levels:

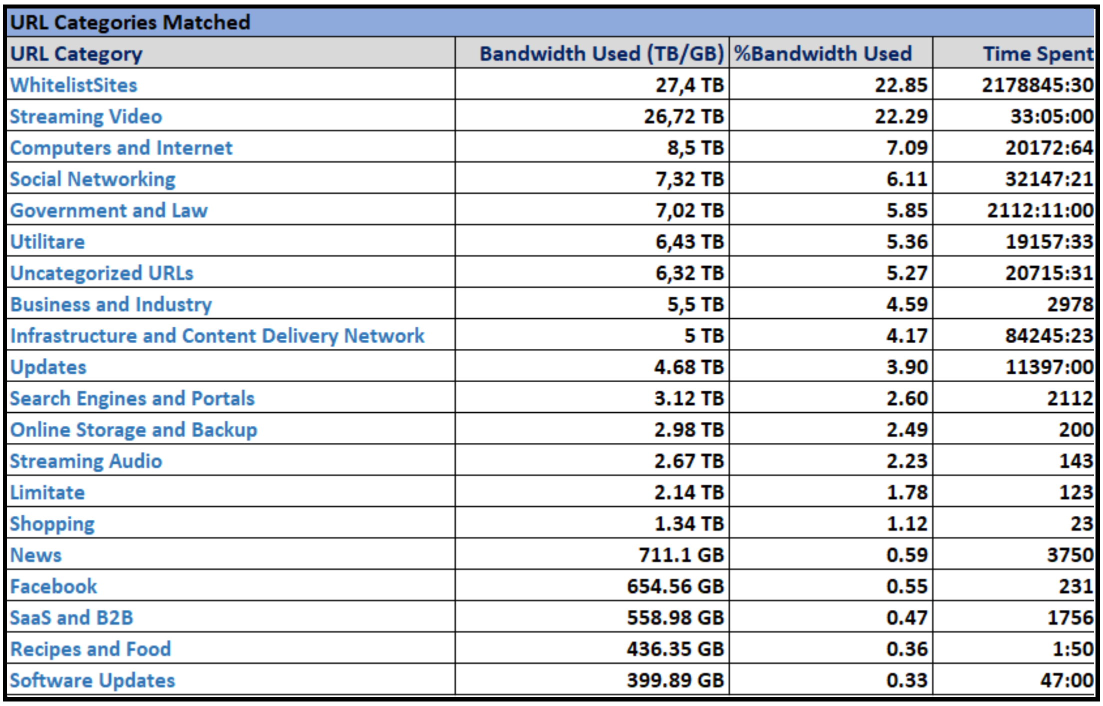
a. Analysis of data traffic between networks (LAN, WAN, Internet) – performed at the router level;

b. Using a Squid proxy log analyzer configured at the proxy server level.

3.1. Analysis of data traffic between networks (LAN, WAN, Internet) – performed at the router level

Monitoring network equipment is critical to ensuring optimal performance, detecting and preventing network problems, and maintaining security.

At the level of the organization under analysis, the top 20 positions in descending order, from the point of view of generated traffic, look like this (Figure 1):



URL Categories Matched			
URL Category	**Bandwidth Used (TB/GB)**	**%Bandwidth Used**	**Time Spent**
WhitelistSites	27,4 TB	22.85	2178845:30
Streaming Video	26,72 TB	22.29	33:05:00
Computers and Internet	8,5 TB	7.09	20172:64
Social Networking	7,32 TB	6.11	32147:21
Government and Law	7,02 TB	5.85	2112:11:00
Utilitare	6,43 TB	5.36	19157:33
Uncategorized URLs	6,32 TB	5.27	20715:31
Business and Industry	5,5 TB	4.59	2978
Infrastructure and Content Delivery Network	5 TB	4.17	84245:23
Updates	4.68 TB	3.90	11397:00
Search Engines and Portals	3.12 TB	2.60	2112
Online Storage and Backup	2.98 TB	2.49	200
Streaming Audio	2.67 TB	2.23	143
Limitate	2.14 TB	1.78	123
Shopping	1.34 TB	1.12	23
News	711.1 GB	0.59	3750
Facebook	654.56 GB	0.55	231
SaaS and B2B	558.98 GB	0.47	1756
Recipes and Food	436.35 GB	0.36	1:50
Software Updates	399.89 GB	0.33	47:00

Fig. 1. Top 20 positions in descending order, in terms of traffic generated

As percentages, these data are represented in the following graph (Figure 2):

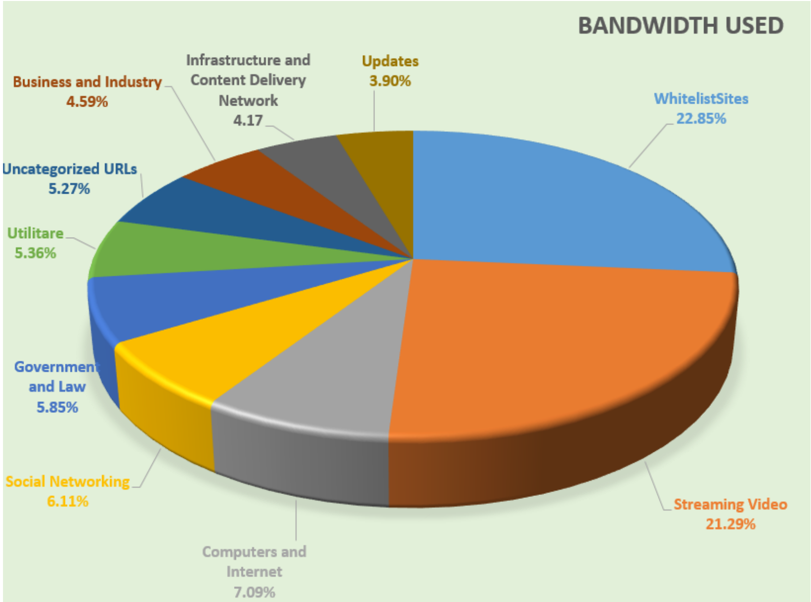


Fig. 2. Graphic representation of the values regarding the generated traffic

The conducted study revealed the following trends in the use of the Internet by users:

- Professional Activities: Access to information relevant to the performance of work duties.
- Media Content Consumption: Watching videos, participating in video conferences or listening to music.
- Accessing government websites and legislation.
- Social Media Interaction: Navigating social media platforms for communication and interaction.
- Email Management: Checking and replying to emails.
- Searching for Personal Information and Online Shopping: Using the Internet to search for information of personal interest or to make online purchases.

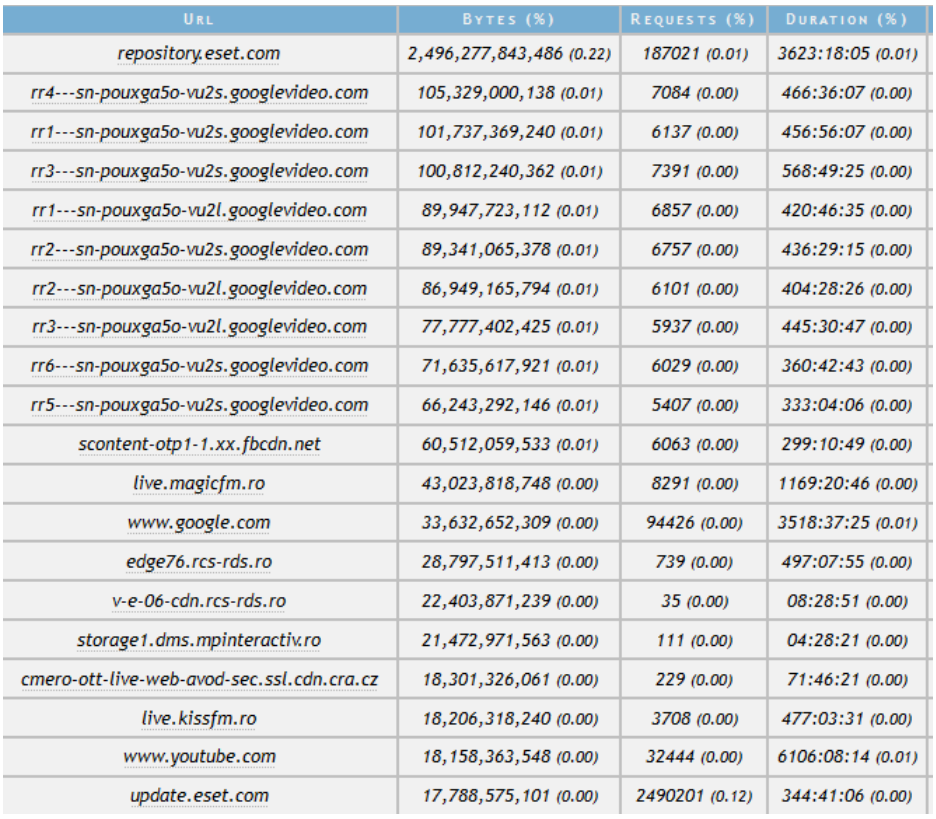
3.2. At the proxy server level

At the organization level a proxy server is configured and a network **cache (Squid**) is used to handle HTTP, HTTPS and FTP traffic, used to improve network performance and improve security. Squid is also used for **traffic filtering purposes, access monitoring** and **temporary storage of frequently accessed resources** (cache), to reduce latencies and network load.

Traffic monitoring was done by using the SquidAnalyzer software [7], installed on the proxy server within the organization. This software is a Squid proxy log analyzer and report generator with statistics on times, hits, bytes, users, networks, URLs and domains. Statistical reports are geared towards user and bandwidth control.

SquidAnalyzer uses flat files to store data and does not require SQL, SQL Lite or Berkeley databases. This log parser is incremental.

The analysis of network traffic generated at the level of the organization (August-October 2024) was carried out from the perspective *of relevance and use of network resources.* The top 20 most accessed web addresses in terms of traffic (total amount of data transferred) are shown in Figure 3.



URL	BYTES (%)	REQUESTS (%)	DURATION (%)
repository.eset.com	2,496,277,843,486 (0.22)	187021 (0.01)	3623:18:05 (0.01)
rr4---sn-pouxga5o-vu2s.googlevideo.com	105,329,000,138 (0.01)	7084 (0.00)	466:36:07 (0.00)
rr1---sn-pouxga5o-vu2s.googlevideo.com	101,737,369,240 (0.01)	6137 (0.00)	456:56:07 (0.00)
rr3---sn-pouxga5o-vu2s.googlevideo.com	100,812,240,362 (0.01)	7391 (0.00)	568:49:25 (0.00)
rr1---sn-pouxga5o-vu2l.googlevideo.com	89,947,723,112 (0.01)	6857 (0.00)	420:46:35 (0.00)
rr2---sn-pouxga5o-vu2s.googlevideo.com	89,341,065,378 (0.01)	6757 (0.00)	436:29:15 (0.00)
rr2---sn-pouxga5o-vu2l.googlevideo.com	86,949,165,794 (0.01)	6101 (0.00)	404:28:26 (0.00)
rr3---sn-pouxga5o-vu2l.googlevideo.com	77,777,402,425 (0.01)	5937 (0.00)	445:30:47 (0.00)
rr6---sn-pouxga5o-vu2s.googlevideo.com	71,635,617,921 (0.01)	6029 (0.00)	360:42:43 (0.00)
rr5---sn-pouxga5o-vu2s.googlevideo.com	66,243,292,146 (0.01)	5407 (0.00)	333:04:06 (0.00)
scontent-otp1-1.xx.fbcdn.net	60,512,059,533 (0.01)	6063 (0.00)	299:10:49 (0.00)
live.magicfm.ro	43,023,818,748 (0.00)	8291 (0.00)	1169:20:46 (0.00)
www.google.com	33,632,652,309 (0.00)	94426 (0.00)	3518:37:25 (0.01)
edge76.rcs-rds.ro	28,797,511,413 (0.00)	739 (0.00)	497:07:55 (0.00)
v-e-06-cdn.rcs-rds.ro	22,403,871,239 (0.00)	35 (0.00)	08:28:51 (0.00)
storage1.dms.mpinteractiv.ro	21,472,971,563 (0.00)	111 (0.00)	04:28:21 (0.00)
cmero-ott-live-web-avod-sec.ssl.cdn.cra.cz	18,301,326,061 (0.00)	229 (0.00)	71:46:21 (0.00)
live.kissfm.ro	18,206,318,240 (0.00)	3708 (0.00)	477:03:31 (0.00)
www.youtube.com	18,158,363,548 (0.00)	32444 (0.00)	6106:08:14 (0.01)
update.eset.com	17,788,575,101 (0.00)	2490201 (0.12)	344:41:06 (0.00)

Fig. 3. The top 20 most accessed web addresses in terms of traffic

The total amount of bytes transferred for each URL (web page) was analyzed. As you can see, the first place is the updates of the antivirus solution (Eset). During the analyzed period, the traffic that the antivirus solution updates generate is approximately 2.5 TB, being approximately 24 times higher than that of the next accessed page (Figure 4).

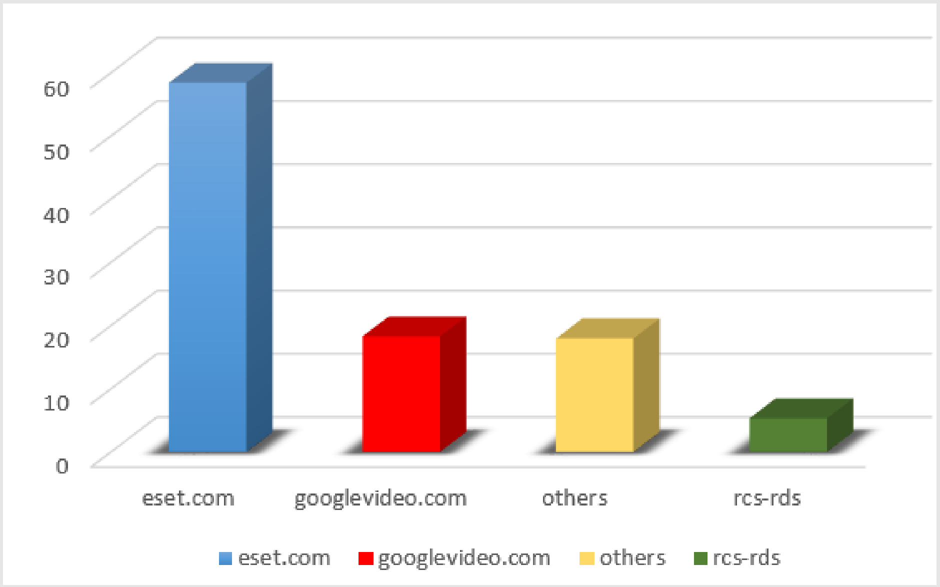
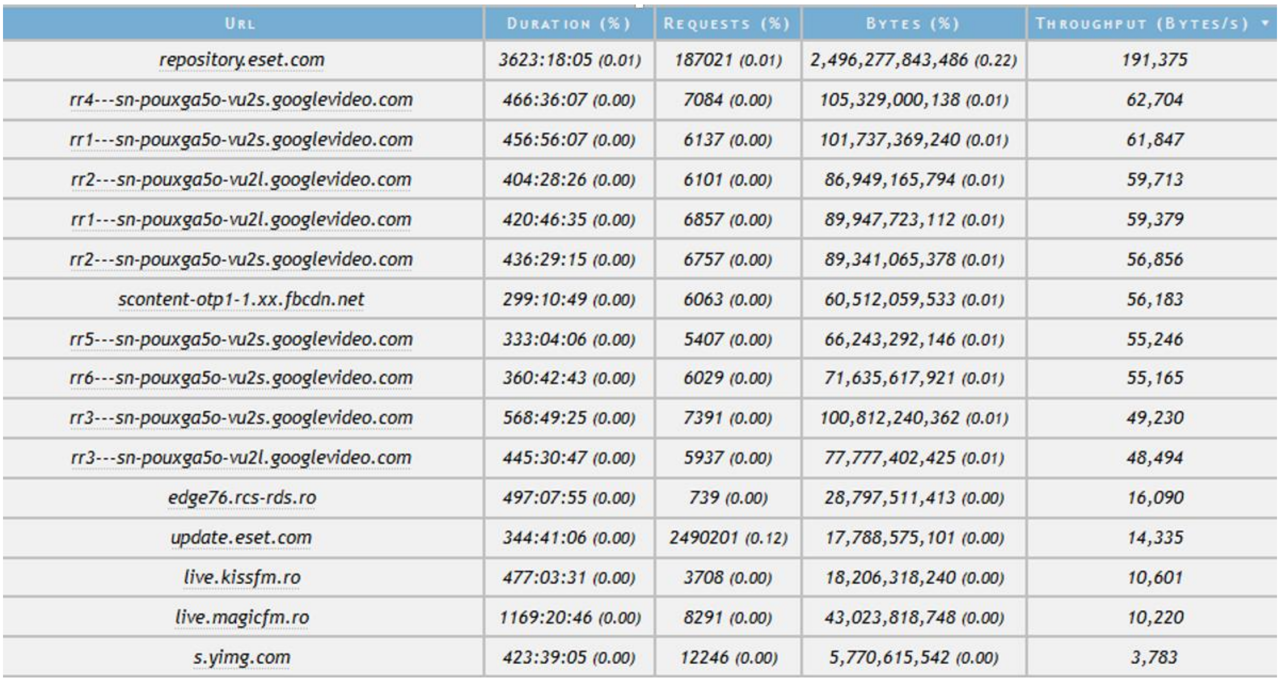


Fig. 4. Total amount of bytes transferred for each URL

Time spent by users on web pages:

The sites on which users spent the most time were identified by analyzing URLs with high throughput, indicating sites of high interest or abnormal activity (Figure 5).



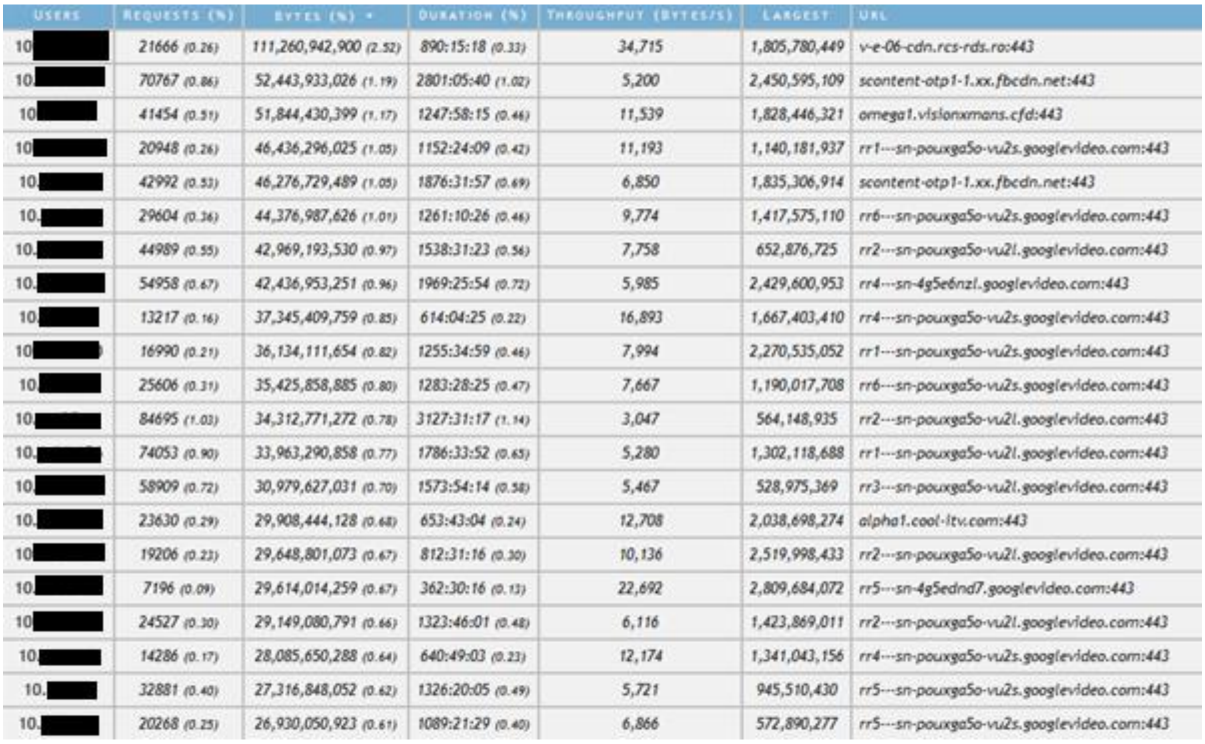
URL	DURATION (%)	REQUESTS (%)	BYTES (%)	THROUGHPUT (BYTES/S) ▾
repository.eset.com	3623:18:05 (0.01)	187021 (0.01)	2,496,277,843,486 (0.22)	191,375
rr4---sn-pouxga5o-vu2s.googlevideo.com	466:36:07 (0.00)	7084 (0.00)	105,329,000,138 (0.01)	62,704
rr1---sn-pouxga5o-vu2s.googlevideo.com	456:56:07 (0.00)	6137 (0.00)	101,737,369,240 (0.01)	61,847
rr2---sn-pouxga5o-vu2l.googlevideo.com	404:28:26 (0.00)	6101 (0.00)	86,949,165,794 (0.01)	59,713
rr1---sn-pouxga5o-vu2l.googlevideo.com	420:46:35 (0.00)	6857 (0.00)	89,947,723,112 (0.01)	59,379
rr2---sn-pouxga5o-vu2s.googlevideo.com	436:29:15 (0.00)	6757 (0.00)	89,341,065,378 (0.01)	56,856
scontent-otp1-1.xx.fbcdn.net	299:10:49 (0.00)	6063 (0.00)	60,512,059,533 (0.01)	56,183
rr5---sn-pouxga5o-vu2s.googlevideo.com	333:04:06 (0.00)	5407 (0.00)	66,243,292,146 (0.01)	55,246
rr6---sn-pouxga5o-vu2s.googlevideo.com	360:42:43 (0.00)	6029 (0.00)	71,635,617,921 (0.01)	55,165
rr3---sn-pouxga5o-vu2s.googlevideo.com	568:49:25 (0.00)	7391 (0.00)	100,812,240,362 (0.01)	49,230
rr3---sn-pouxga5o-vu2l.googlevideo.com	445:30:47 (0.00)	5937 (0.00)	77,777,402,425 (0.01)	48,494
edge76.rcs-rds.ro	497:07:55 (0.00)	739 (0.00)	28,797,511,413 (0.00)	16,090
update.eset.com	344:41:06 (0.00)	2490201 (0.12)	17,788,575,101 (0.00)	14,335
live.kissfm.ro	477:03:31 (0.00)	3708 (0.00)	18,206,318,240 (0.00)	10,601
live.magicfm.ro	1169:20:46 (0.00)	8291 (0.00)	43,023,818,748 (0.00)	10,220
s.yimg.com	423:39:05 (0.00)	12246 (0.00)	5,770,615,542 (0.00)	3,783

Fig. 5. Sites on which users spent the most time

It is noted that, in this case, the first place is occupied by the web page called by the services that ensure the perimeter protection of users (antivirus server).

Top 20 users with the most activity:

Users with the highest number of requests (total time spent online and URLs accessed) are identified (Figure 6).



USERS	REQUESTS (%)	BYTES (%) ▾	DURATION (%)	THROUGHPUT (BYTES/S)	LARGEST	URL
10[redacted]	21666 (0.26)	111,260,942,900 (2.52)	890:15:18 (0.33)	34,715	1,805,780,449	v-e-06-cdn.rcs-rds.ro:443
10.[redacted]	70767 (0.86)	52,443,933,026 (1.19)	2801:05:40 (1.02)	5,200	2,450,595,109	scontent-otp1-1.xx.fbcdn.net:443
10[redacted]	41454 (0.51)	51,844,430,399 (1.17)	1247:58:15 (0.46)	11,539	1,828,446,321	omega1.visionxmans.cfd:443
10[redacted]	20948 (0.26)	46,436,296,025 (1.05)	1152:24:09 (0.42)	11,193	1,140,181,937	rr1---sn-pouxga5o-vu2s.googlevideo.com:443
10.[redacted]	42992 (0.53)	46,276,729,489 (1.05)	1876:31:57 (0.69)	6,850	1,835,306,914	scontent-otp1-1.xx.fbcdn.net:443
10.[redacted]	29604 (0.36)	44,376,987,626 (1.01)	1261:10:26 (0.46)	9,774	1,417,575,110	rr6---sn-pouxga5o-vu2s.googlevideo.com:443
10.[redacted]	44989 (0.55)	42,969,193,530 (0.97)	1538:31:23 (0.56)	7,758	652,876,725	rr2---sn-pouxga5o-vu2l.googlevideo.com:443
10.[redacted]	54958 (0.67)	42,436,953,251 (0.96)	1969:25:54 (0.72)	5,985	2,429,600,953	rr4---sn-4g5e6nzl.googlevideo.com:443
10.[redacted]	13217 (0.16)	37,345,409,759 (0.85)	614:04:25 (0.22)	16,893	1,667,403,410	rr4---sn-pouxga5o-vu2s.googlevideo.com:443
10[redacted]	16990 (0.21)	36,134,111,654 (0.82)	1255:34:59 (0.46)	7,994	2,270,535,052	rr1---sn-pouxga5o-vu2s.googlevideo.com:443
10.[redacted]	25606 (0.31)	35,425,858,885 (0.80)	1283:28:25 (0.47)	7,667	1,190,017,708	rr6---sn-pouxga5o-vu2s.googlevideo.com:443
10[redacted]	84695 (1.03)	34,312,771,272 (0.78)	3127:31:17 (1.14)	3,047	564,148,935	rr2---sn-pouxga5o-vu2l.googlevideo.com:443
10.[redacted]	74053 (0.90)	33,963,290,858 (0.77)	1786:33:52 (0.65)	5,280	1,302,118,688	rr1---sn-pouxga5o-vu2l.googlevideo.com:443
10[redacted]	58909 (0.72)	30,979,627,031 (0.70)	1573:54:14 (0.58)	5,467	528,975,369	rr3---sn-pouxga5o-vu2l.googlevideo.com:443
10.[redacted]	23630 (0.29)	29,908,444,128 (0.68)	653:43:04 (0.24)	12,708	2,038,698,274	alpha1.cool-itv.com:443
10[redacted]	19206 (0.23)	29,648,801,073 (0.67)	812:31:16 (0.30)	10,136	2,519,998,433	rr2---sn-pouxga5o-vu2l.googlevideo.com:443
10[redacted]	7196 (0.09)	29,614,014,259 (0.67)	362:30:16 (0.13)	22,692	2,809,684,072	rr5---sn-4g5ednd7.googlevideo.com:443
10[redacted]	24527 (0.30)	29,149,080,791 (0.66)	1323:46:01 (0.48)	6,116	1,423,869,011	rr2---sn-pouxga5o-vu2l.googlevideo.com:443
10[redacted]	14286 (0.17)	28,085,650,288 (0.64)	640:49:03 (0.23)	12,174	1,341,043,156	rr4---sn-pouxga5o-vu2s.googlevideo.com:443
10.[redacted]	32881 (0.40)	27,316,848,052 (0.62)	1326:20:05 (0.49)	5,721	945,510,430	rr5---sn-pouxga5o-vu2s.googlevideo.com:443
10.[redacted]	20268 (0.25)	26,930,050,923 (0.61)	1089:21:29 (0.40)	6,866	572,890,277	rr5---sn-pouxga5o-vu2s.googlevideo.com:443

Fig. 6. Identifying users with the highest number of requests

User level detail:

Table 1. User level detail

No.	Department	Computer IP	Username	The most visited sites
1	Department 1	10. [redacted]	User 1	www.digionline.ro, www.temu.com
2	Department 2	10. [redacted]	User 2	www.youtube.com, www.facebook.com
3	Department 3	10. [redacted]	User 3	live.magicfm.ro, cmero-ott-live-web-avod-sec.ssl.cdn.cra.cz
4	Department 1	10. [redacted]	User 4	www.youtube.com, play.google.com, googlevideo.com
5	Department 1	10. [redacted]	User 5	chat.facebook.com, play.google.com
6	Department 2	10. [redacted]	User 6	www.youtube.com, googlevideo.com
7	Department 3	10. [redacted]	User 7	www.youtube.com
8	Department 3	10. [redacted]	User 8	live.streamtheworld.com, www.youtube.com
9	Department 2	10. [redacted]	User 9	www.youtube.com, play.google.com
10	Department 2	10. [redacted]	User 10	www.youtube.com, play.google.com
11	Department 2	10. [redacted]	User 11	www.youtube.com, play.google.com
12	Department 1	10. [redacted]	User 12	www.youtube.com
13	Department 2	10. [redacted]	User 13	www.youtube.com
14	Department 3	10. [redacted]	User 14	www.youtube.com, cool-eTV.net
15	Department 3	10. [redacted]	User 15	play.discomix.ro, www.youtube.com
16	Department 2	10. [redacted]	User 16	www.youtube.com, play.google.com
17	Department 1	10. [redacted]	User 17	www.youtube.com, play.google.com
18	Department 1	10. [redacted]	User 18	www.youtube.com, play.google.com
19	Department 2	10. [redacted]	User 19	www.youtube.com, facebook.ro
20	Department 2	10. [redacted]	User 20	www.youtube.com

4. Conclusions

Cyber threat analysis within the organization highlights a dynamic and complex cyber security landscape. Amidst the intensification of cyber attacks globally, it is important to adopt proactive and preventive measures to protect the integrity of the IT infrastructure and reduce the potential impact of attacks.

The paper proposed web traffic analysis from the perspective of bandwidth optimization for professional activities. This helps maintain a balance between operational needs and IT security.

Protecting electronic services that access the Internet becomes essential in preventing cyber attacks and protecting personal and organizational data.

Data traffic analysis also proves to be essential to understand user behavior in order to implement appropriate security measures appropriate to the organizational security culture.

References

[1]. https://therecord.media/major-russian-banks-ddos-attack-ukraine

[2]. https://www.bleepingcomputer.com/news/security/hamster-kombats-250-million-players-targeted-in-malware-attacks/

[3]. https://community.virginmedia.com/t5/Security-matters/Latest-Phishing-News-24-07-2024/td-p/5547441

[4]. https://www.bleepingcomputer.com/news/security/new-eldorado-ransomware-targets-windows-vmware-esxi-vms/

[5]. https://therecord.media/ransomware-group-volcano-demon-lukalocker

[6]. https://www.cve.org/

[7]. https://squidanalyzer.darold.net/

The Importance of Combating Fake News and Its Impact in the Digital Age

Gabriel-Virgil TAUBER[1], Sergiu-Adrian VASILE[2]
[1] University Cooperation and Public Relations Office, "Al. I. Cuza" Police Academy, Bucharest, Romania
gabriel.tauber@academiadepolitie.ro
[2] Border Police Department, "Al. I. Cuza" Police Academy, Bucharest, Romania
sergiu.vasile@academiadepolitie.ro

Abstract

In an era of massive digitization and technologization, information represents the quintessence of success on all levels and in all fields. With a major power and influence in achieving success, disinformation, however, gains in the last period of time more followers who, through different methods and means, manage to manipulate and control different social categories in order to achieve the intended goal. There is currently a risk that a piece of information (fake news) will cause harm and damage not only at the individual level but also at the macro level, destabilizing order and national security. As we will show in this article, with the help of artificial intelligence, with the help of each individual, among cooperation at the international level and among an education appropriate to the century in which we live, we can hope to counteract and diminish this phenomenon that it can also have geopolitical consequences and more.

Index terms: fake news, digitization, misinformation, vulnerabilities, cooperation, integrated solutions

1. Introduction to the phenomenon of Fake News

Although the name disinformation has existed throughout history, the term "fake news" has become much more well-known in the last decade, with the explosion of social media platforms. These technologies enable the rapid and widespread dissemination of information, including false information, often without verification or true context.

As always, in order to be able to describe a phenomenon, we must first start from the definition of the term Fake news, a term that represents those false or misleading information presented as legitimate news. They are intentionally created to mislead or manipulate public opinion, often for financial, political or ideological purposes.

Fake news can manifest itself in various forms, such as sensational headlines, completely fabricated articles, conspiracy theories or distorted interpretations of real events.

In order to be able to answer the question "Why is fake news dangerous" we need to bring to attention some well-founded reasons, such as the erosion of public trust, social and political polarization, the impact on elections and democracy, the spread of disinformation in public health crises and last but not least the economic challenges.

In the following, we will try to briefly exemplify each individual reason in order to create an overview of the phenomenon itself.

Thus, Fake news can destabilize the public's trust in traditional mass media on the one hand and in democratic institutions on the other. Once trust is damaged, people become more susceptible to misinformation and less likely to believe accurate information.[1]

All this misinformation contributes, without exception, to the polarization of society by fueling divisions and tensions between different social and political groups. They often promote a different view of reality, reinforcing prejudices and exacerbating conflicts.[2]

Moreover, they can influence the results of the elections by disseminating false information about the candidates or the policies led by them, thus creating massive disinformation that can affect the citizens' elections.

Not long ago, during the COVID-19 pandemic, fake news led to the propagation of conspiracy theories and mass misinformation about vaccines and public health measures. This had, without any doubt, a direct impact on public behavior, putting lives and public health at risk.[3]

And in the field of international relations, fake news can spread disinformation that affects the perceptions of some states about other nations. In some cases, governments or non-state actors use fake news as part of information warfare to destabilize other countries or to influence public opinion in the context of international conflicts.

Last but not least, also in the economic field, Fake news can have a significant impact, destabilizing the financial markets or affecting the reputation of companies.

2. The origin and evolution of Fake News

The origin and evolution of fake news has been talked about over time, this phenomenon not being a new one. Their roots can be traced deep into history. We can also find such an example during the Roman Empire when the emperor Octavian Augustus used disinformation campaigns to discredit his political rival, Mark Antony.

Moreover, in the 19th century, the tabloid presses frequently used fake or exaggerated news to attract readers and increase sales. One such example is "The Great Moon Hoax" of 1835, when a New York newspaper published false articles about the discovery of life on the moon, which led to a massive increase in the newspaper's circulation.[4]

With the advent of the Internet and social media, this phenomenon has grown in scale and become more sophisticated and easier to spread. The Internet has allowed the creators of fake news to reach the global audience much more quickly and safely, including a much lower cost. Thus, with the help of social networks, they have reached the spread of fake news much faster due to their algorithmic structure, which prioritizes content that generates engagement, even if the news is false or misleading.

Regarding the role of digital platforms and modern technology, it has played an extremely important role in amplifying the phenomenon of fake news given that the algorithms of social media platforms are designed to maximize the time users spend on the platform, often promoting sensational content or controversial, which frequently includes fake news. The use of bots and fake accounts also contributes to the quick spread of misinformation.

[1] Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, 31(2), pp. 211-236.

[2] Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe report.

[3] Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), pp. 1146-1151.

[4] https://aeon.co/videos/bat-people-on-the-moon-what-a-famed-1835-hoax-reveals-about-misinformation-today accessed on 20.05.2024.

3. Measures to combat Fake News by law enforcement and public safety authorities

Public order and safety authorities, through specialized structures of course, play an extraordinarily important role in combating the fake news phenomenon, through a series of measures that include monitoring, regulation and law enforcement. Combating disinformation is essential to maintaining public order, national security and the protection of citizens.

Authorities can deploy advanced digital surveillance systems to monitor online content and detect fake news in real time that has the potential to cause panic or destabilize public order. These artificial intelligence (AI) technologies can analyze large volumes of data to identify patterns and sources of misinformation.[5] This way the Police and other law enforcement agencies can work with social platforms to quickly flag problematic content and request its removal.

Another essential aspect of combating fake news is educating the public, meaning that public order and safety authorities can launch information campaigns in order to raise citizens' awareness of the risks associated with fake news, but also to provide them with tools to recognize disinformation.

Of course, these campaigns can include the distribution of informative materials, the organization of interactive workshops as well as the use of traditional and digital technology to reach a large audience. The aim is to improve citizens' media literacy and reduce their vulnerability to misinformation.[6]

Furthermore, the authorities are encouraged to work more closely with schools and universities to integrate media education into the school/university curriculum, thereby training younger generations to identify and reject false information.

In some cases, however, spreading fake news can constitute a crime, especially if it endangers public order or national security. In this case, the Police can investigate and sanction individuals or groups who intentionally create and distribute fake news with the aim of manipulating public opinion or destabilizing social order. These actions may include arrests, fines and other legal measures.[7]

There are of course also countries that have passed specific laws that criminalize the creation and spread of fake news, especially in the context of elections, pandemics or other crises. Law enforcement authorities must enforce these laws and work with other institutions to protect informational integrity.[8]

Regarding international collaboration to combat disinformation, public order authorities must find solutions to collaborate internationally to combat fake news. In this sense law enforcement agencies from different countries can share information, best practices and strategies to combat disinformation, helping each other identify and neutralize sources of fake news.

Moreover, by engaging in international initiatives, such as working groups within international organizations, it can increase the responsiveness of national authorities to the global phenomenon of disinformation.[9]

Thus, by undertaking such measures, society can be protected from the negative impact of fake news and thus a better, safer climate can be maintained. Effective collaboration between various entities and the use of technology are the keys to success in this battle.

[5] Graves, L. (2018). Understanding the Promise and Limits of Automated Fact-Checking. Reuters Institute for the Study of Journalism.

[6] Hobbs, R. (2017). Create to Learn: Introduction to Digital Literacy. Wiley.

[7] Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, 31(2), pp. 211-236.

[8] Lazer, D. M. J., Baum, M. A., Grinberg, N., & others. (2018). The science of fake news. Science, 359(6380), pp. 1094-1096

[9] Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe report.

4. The impact of Fake News on society and public health

It is important to emphasize that Fake news can have a significant impact both on society and on public health, thus generating both short-term and long-term consequences, consequences that can affect social stability, public health and trust in institutions.

In terms of declining trust in institutions and the media, Fake news undermines public trust in traditional media and democratic institutions.

When false information is presented as truth and is widely spread, the public becomes confused and skeptical of any source of information, including credible sources.

This phenomenon can lead to a crisis of confidence in society, where citizens no longer know what to believe in, something that can certainly affect social cohesion and political stability.[10]

Moreover, Fake news contributes to social and political polarization by fueling divisions between different ideological, ethnic or religious groups.

They are often designed to create strong emotions such as fear, hatred or anger, emotions that lead to the radicalization of opinions and the strengthening of prejudices.

One such study of the social impact of misinformation and the mechanisms by which rumors and fake news spread is done very well by C.R. Sunstein in his work "On Rumors: How Falsehoods Spread, Why We Believe Them, What Can Be Done. Princeton University Press".

As I mentioned before, Fake news can significantly affect the results of elections by manipulating the public about candidates and political issues. A disinformation campaign during an election race can distort public debate and prevent citizens from making informed choices. In the context of close elections, Fake news can be enough to tilt the balance in favor of one candidate or another, thus undermining the legitimacy of the democratic process.[11]

Regarding the impact of fake news on public health, of course, it has a particularly dangerous role, especially during crises, such as the COVID-19 pandemic.

Misinformation regarding the origins of the virus, the indicated treatments or the effectiveness of vaccines led to risky behaviors and positions, such as the refusal of some people to wear masks, the avoidance of vaccination or the use of scientifically unvalidated remedies.

But there are also effects on mental health, as misinformation can lead to anxiety, confusion and mistrust of official information, which can lead to stress and other mental health problems.

Another example from the period of the COVID-19 pandemic, refers to the fake news about the side effects of vaccines or about conspiracies related to the pandemic, news that amplified the feeling of insecurity and anxiety among the population.[12]

Such approaches to spread fake news can undermine the efforts of the authorities to manage the issue in a reasonable manner.

When a large part of the population does not strictly follow official recommendations due to misinformation, controlling the spread of disease and protecting public health becomes much more difficult.

Moreover, the rapid spread of fake news can create information overload, where accurate information is lost in the flood of misinformation, thereby reducing the effectiveness of public health messages.[13]

[10] Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, 31(2), pp. 211-236.

[11] Lazer, D. M. J., Baum, M. A., Grinberg, N., & others. (2018). The science of fake news. Science, 359(6380), pp. 1094-1096.

[12] **Pennycook, G., McPhetres, J., Zhang, Y., & others. (2020).** *Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy-nudge intervention. Psychological Science*, 31(7), pp. 770-780.

[13] Lewandowsky, S., Ecker, U. K. H., & Cook, J. (2017). Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era. Journal of Applied Research in Memory and Cognition, 6(4), pp. 353-369.

5. Conclusions and future perspectives in the fight against Fake News

It is true that as technology advances, it is expected that the phenomenon of Fake news will become even more complicated to combat.

As presented in a study on the impact of advanced technologies such as deepfakes on public perception and trust in news, in the future we will see an increasing use of artificial intelligence that will create fake content such as deepfake videos, auto-generated text and digitally altered images. These advanced technologies will make fake news much harder to spot and much more convincing.[14]

But as public platforms will improve the detection mechanisms of fake news, it is likely that its spread will move to private messaging platforms, where it is more difficult to monitor and combat, as well presented in the paper "The global organization of social media disinformation campaigns. Journal of International Affairs".[15]

This phenomenon of disinformation, however, will continue to be used as a strategic tool even in geopolitical conflicts, to influence international public opinion on the one hand, but also to destabilize rival countries.[16]

In the study "Winning the Information War: Techniques and Counter-strategies to Fake News in Russia and the West", we are presented with an exploration of how disinformation is used in geopolitical conflicts and how campaigns will become more sophisticated and coordinated.

A real challenge in this regard will be the tandem development of technologies to keep up with the evolution of Fake news. This will require continued and robust investment in artificial intelligence to detect disinformation. Furthermore, constant adaptation of the legal framework will be necessary to regulate new forms of disinformation and protect individual rights such as freedom of expression.

If we talk about combating disinformation, this will require a special approach for vulnerable communities that can be achieved through media education adapted to their needs but also through collaboration with local leaders to raise awareness.

Being a global problem, strengthening international cooperation in combating this phenomenon is essential and requires the sharing of information, the development of common strategies and the establishment of international standards.

But, of course not only the authorities play an essential role in combating disinformation. Each of us, at the individual level, has an important role in combating fake news.

As R. Hobbs presents us, in his work "Create to Learn: Introduction to Digital Literacy. Wiley" it is essential to check sources before sharing information, making sure it comes from credible and verified sources. This involves checking the author, the publication and the context in which the information was published.[17]

And critical thinking sometimes helps to objectively evaluate information as well as to recognize fake news. A more or less skeptical attitude towards sensational headlines as well as a careful analysis of the content are just a few essential aspects to prevent the spread of misinformation.

Last but not least, education is, if we can say so, the basis of our ability not to fall victim to Fake news. Through our participation in digital and media literacy courses and workshops we can improve our ability to identify and combat fake news. Continuing education in this area is crucial to keep up with new forms of disinformation.

[14] Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. Social Media + Society, 6(1)

[15] Bradshaw, S., & Howard, P. N. (2019). The global organization of social media disinformation campaigns. Journal of International Affairs, 71(1.5), pp. 23-32

[16] Lucas, E., & Pomerantsev, P. (2020). Winning the Information War: Techniques and Counter-strategies to Fake News in Russia and the West. Center for European Policy Analysis

[17] Hobbs, R. (2017). Create to Learn: Introduction to Digital Literacy. Wiley.

Regarding collective responsibility in the information age, we can only reinforce the fact that each of us is obliged to contribute to the creation of a culture of correct information, in which the distribution of verified and true information is a social norm.

As good attitudes to follow, it is important to remember that whenever we come across fake news, we must report it to the respective platforms for their removal. This can be considered a form of social responsibility that can help reduce the impact of misinformation.

Sources and bibliography

[1]. Allcott, H., & Gentzkow, M., "*Social Media and Fake News in the 2016 Election*", published in the Journal of Economic Perspectives, 2017.

[2]. Bradshaw, S., & Howard, P. N., "*The global organization of social media disinformation campaigns*", published in the Journal of International Affairs, 2019.

[3]. Graves, L., "*Understanding the Promise and Limits of Automated Fact-Checking*", published in the Reuters Institute for the Study of Journalism, 2018.

[4]. Hobbs, R., "*Create to Learn: Introduction to Digital Literacy*", published in Wiley, 2017.

[5]. Lazer, D. M. J., Baum, M. A., Grinberg, N., & others, "*The science of fake news*", published in the Science, 2018.

[6]. Lewandowsky, S., Ecker, U. K. H., & Cook, J., "*Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era*", published in the Journal of Applied Research in Memory and Cognition, 2017.

[7]. Lucas, E., & Pomerantsev, P., "*Winning the Information War: Techniques and Counter-strategies to Fake News in Russia and the West*", published in the Center for European Policy Analysis, 2020.

[8]. Pennycook, G., McPhetres, J., Zhang, Y., & others, "*Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy-nudge intervention*", published in the Psychological Science, 2020.

[9]. Vaccari, C., & Chadwick, A., "*Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news*", published in the Social Media + Society, 2020.

[10]. Vosoughi, S., Roy, D., & Aral, S., "*The spread of true and false news online*", published in the Science, 2018.

[11]. Wardle, C., & Derakhshan, H., "*Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*", published in the Council of Europe report, 2017.

[12]. https://aeon.co/videos/bat-people-on-the-moon-what-a-famed-1835-hoax-reveals-about-misinformation-today.

Assessing Web Security in E-Learning Systems

Denisa-Nicoleta MIHALACHE
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
denisa.mihalache@stud.etti.upb.ro

Abstract

The exponentially evolution of the internet and the increasing sophistication of cyber threats have made securing web servers and web applications a critical concern in today's digital landscape. This research explores the security vulnerabilities of e-learning platforms, particularly Moodle, and demonstrates practical exploitation methods to highlight the risks. A key focus is the development and deployment of a custom script to create a trojan virus leveraging the Right-to-Left Override (RLO) technique. This malware, disguised as a legitimate e-learning material, infiltrates the platform, lists system files, and injects malicious code into Python files, showcasing a high-impact threat vector.

Index terms: cyber-attacks, penetration testing, malicious software, trojan, e-learning security

1. Introduction

The rise of e-learning platforms has transformed the education landscape, providing students and educators with flexible, accessible, and scalable learning environments. By leveraging technologies such as Learning Management Systems (LMS), institutions can deliver courses, assignments, and interactive content seamlessly across the globe. Among these platforms, Moodle has emerged as one of the most widely adopted open-source solutions, enabling customizable and collaborative educational experiences.

However, the growing reliance on web-based platforms has made them attractive targets for cyberattacks. Threat actors exploit vulnerabilities in these systems to compromise sensitive user data, disrupt operations, or propagate malware. Security risks are further amplified as institutions integrate third-party plugins, rely on cloud hosting, and manage large volumes of user-generated content.

This research investigates the vulnerabilities inherent in e-learning platforms, with a focus on Moodle, and demonstrates the implications of a trojan virus attack. By simulating real-world exploitation techniques, such as leveraging the Right-to-Left Override (RLO) character for file obfuscation, the study highlights critical gaps in the security of web servers hosting such platforms. The findings aim to raise awareness about the importance of robust security practices and provide actionable insights to mitigate potential risks.

2. Security testing

Security testing is a critical process in evaluating the security of an application, identifying vulnerabilities and threats, and mitigating them effectively. It plays a key role in the Software Development Life Cycle (SDLC), allowing teams to discover security flaws before they escalate into serious attacks or breaches. By focusing on the integrity, confidentiality, and availability of systems, security testing helps to ensure that applications remain resilient against potential risks.

Security testing provides the advantage of early identification of flaws during the development process, ensuring that vulnerabilities are addressed before they can become expensive or complex to fix. It also prevents the delivery of insecure software that could lead to significant business risks such as compliance violations, legal issues, and reputational damage. In production environments, security testing enables organizations to quickly identify and address vulnerabilities, reducing the chances of exploitation. Furthermore, it encourages continuous improvement by uncovering new threats and enabling organizations to enhance their security measures [1].

Ethical hacking, or penetration testing, involves simulating the tactics of malicious hackers with full authorization to identify weaknesses and improve security defenses. Ethical hackers use the same tools and techniques as cybercriminals, but with the intent of identifying and fixing vulnerabilities rather than exploiting them [2].

White hat hackers, also known as ethical hackers, focus on helping organizations by identifying and fixing vulnerabilities to prevent attacks. Black hat hackers, on the other hand, exploit weaknesses for malicious purposes, often for financial gain or data theft. Gray hat hackers operate in an ethical gray area; although they identify vulnerabilities without permission, they typically notify the system owners of the risks, sometimes requesting a fee in exchange for details of the exploit [3].

Vulnerability scanning tools are widely used to identify weaknesses in operating systems and software, providing organizations with a clear picture of potential security risks. Penetration testing, or simulated attacks, is another valuable technique, allowing organizations to see how their systems would fare under real-world attack conditions and identify areas for improvement. Ethical hacking, often considered the cornerstone of proactive security, involves authorized attempts to break into systems to discover vulnerabilities before malicious actors can exploit them. Security auditing offers a systematic review of system configurations, software, practices, and environments to ensure compliance with industry standards and improve overall security [4].

3. Penetration testing approaches for Moodle

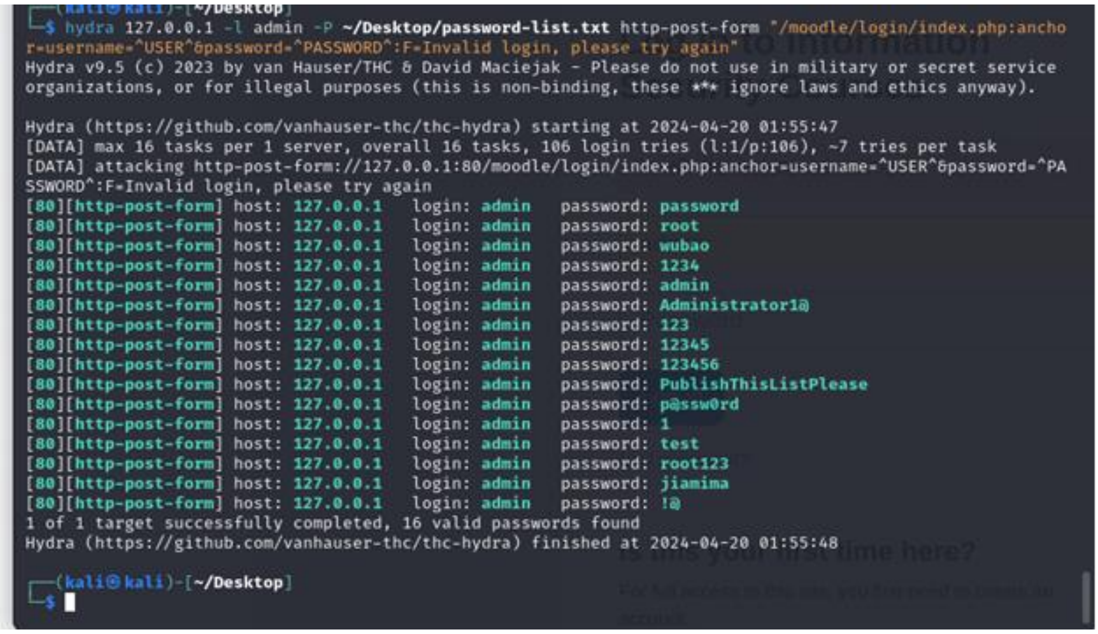
The objective of the penetration testing phase was to evaluate the security posture of the Moodle installation within an Apache2 web server environment. The testing environment was carefully constructed to ensure a secure and controlled setup for the research on improving web server security for Learning Management Systems (LMS). VMware Workstation 17 PRO for Linux was chosen as the platform for virtualization, offering enhanced security features such as snapshots for system restoration. Kali Linux was used as the operating system to leverage penetration testing tools, while Apache2 and MariaDB were installed as core components to host web applications and manage databases securely. Moodle, the selected LMS, was deployed to provide a practical testing environment, with a focus on securing both the server and application to mitigate potential security threats. The methodology involved systematic enumeration and analysis of the application’s endpoints, utilizing various reconnaissance tools. The testing process commenced with the reconnaissance phase using open-source tools such as Dirb, Gobuster, Ferox, and Burp Suite. These tools were employed to generate a comprehensive map of the web application and identify potential attack vectors.

The reconnaissance phase provided valuable insights into the application's surface area and potential attack vectors, establishing a foundation for further vulnerability analysis and exploitation efforts.

Next, the analysis of the website, without authentication, revealed an anomaly: course names and numbers were displayed without restrictions, and the author names of these courses were visible to any visitor. From a security perspective, the only information that should be visible to any visitor is the name of the learning platform. Exposing such details could facilitate various attacks, including social engineering and user impersonation. Additionally, Moodle should restrict the use of default usernames, such as "admin," as this information can be exploited for targeted attacks.

At this point, a brute-force attack attempt was carried out using Hydra, a parallelized login cracker that supports various attack protocols (Figure 1). To test this, a list of commonly used passwords for the "admin" username was required. Along with this, a list of common admin usernames was also created. Using Burp Suite's interception capabilities, I analyzed the behavior of the server when arbitrary data was entered into the login form. The intercepted HTTP form post revealed that a login token was assigned to each session, but this token was not crucial as a new one would be generated for each submission. The error message from the server helped in identifying valid credentials.

Out of 106 tested passwords, 16 were found to be valid, with "Administrator1@" being the correct one. This password, although meeting the minimum complexity requirements (8 characters, including upper and lower case letters, numbers, and special characters), was deemed too simplistic. This breach increases the severity of the vulnerability significantly.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra 127.0.0.1 -l admin -P ~/Desktop/password-list.txt http-post-form "/moodle/login/index.php:ancho
r=username=^USER^&password=^PASSWORD^:F=Invalid login, please try again"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-20 01:55:47
[DATA] max 16 tasks per 1 server, overall 16 tasks, 106 login tries (l:1/p:106), ~7 tries per task
[DATA] attacking http-post-form://127.0.0.1:80/moodle/login/index.php:anchor=username=^USER^&password=^PA
SSWORD^:F=Invalid login, please try again
[80][http-post-form] host: 127.0.0.1   login: admin   password: password
[80][http-post-form] host: 127.0.0.1   login: admin   password: root
[80][http-post-form] host: 127.0.0.1   login: admin   password: wubao
[80][http-post-form] host: 127.0.0.1   login: admin   password: 1234
[80][http-post-form] host: 127.0.0.1   login: admin   password: admin
[80][http-post-form] host: 127.0.0.1   login: admin   password: Administrator1@
[80][http-post-form] host: 127.0.0.1   login: admin   password: 123
[80][http-post-form] host: 127.0.0.1   login: admin   password: 12345
[80][http-post-form] host: 127.0.0.1   login: admin   password: 123456
[80][http-post-form] host: 127.0.0.1   login: admin   password: PublishThisListPlease
[80][http-post-form] host: 127.0.0.1   login: admin   password: p@ssw0rd
[80][http-post-form] host: 127.0.0.1   login: admin   password: 1
[80][http-post-form] host: 127.0.0.1   login: admin   password: test
[80][http-post-form] host: 127.0.0.1   login: admin   password: root123
[80][http-post-form] host: 127.0.0.1   login: admin   password: jiamima
[80][http-post-form] host: 127.0.0.1   login: admin   password: !@
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-20 01:55:48

┌──(kali㉿kali)-[~/Desktop]
└─$ █
```

Fig. 1. Password cracking using Hydra

Several vulnerabilities were identified, including Cross-Site Scripting (XSS) [5] in various parts of the Moodle interface and the clear-text transmission of passwords. These issues could further compromise the security of the platform and should be addressed promptly. Specific attack paths, such as those found in the "Grader Report," "Group Search," and "Announcements" sections, allow for the injection of malicious JavaScript, leading to potential theft of session cookies or redirection to malicious websites. The lack of encryption for password submission in the login and signup pages is another critical vulnerability, as it exposes passwords to interception, especially in unsecured network environments. Furthermore, the "username persistence" vulnerability was also noted on the login page, where the last valid username entered was retained, even if the user was invalid. This could be exploited by attackers to gain insights into valid usernames on the platform.

To demonstrate the severity of the security vulnerability, I opted for an attack strategy involving the insertion of a malicious virus into the system. Utilizing the administrative privileges previously obtained, I created a virus using the Python programming language. This virus was then uploaded onto the platform in the form of a trojan, disguised as a PDF course material, to illustrate the potential risks associated with unrestricted file upload vulnerabilities.

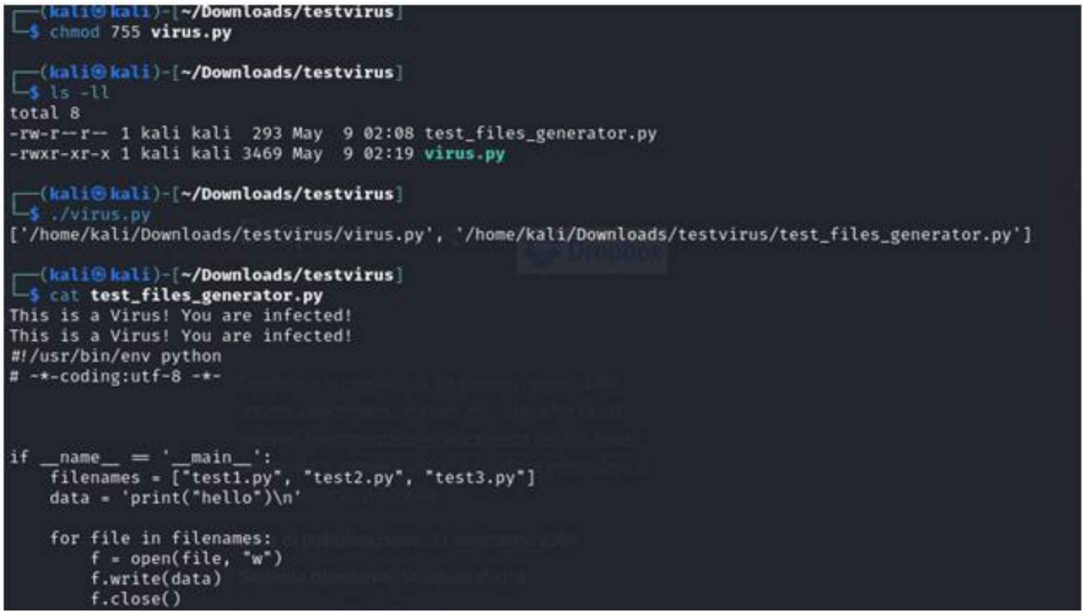
A virus is a type of malicious software (malware) [6] designed to infect files by injecting malicious data or code into them. The virus attempts to enumerate all files across directories and then injects the malicious payload into those files. Unlike worms, which propagate autonomously, this virus does not replicate by itself but continuously infects all files within the specified directories.

In this specific example, once the virus is executed it recursively searches through directories and identifies files with a specific extension (such as .py). For each file, it checks if it has already been infected by looking for a predefined infection string. If the file is not infected, the virus appends the malicious string at the beginning of the file's content. This payload does not replicate itself like a worm but instead continues to infect any new files it encounters within its directory search. The virus can infect numerous files, potentially compromising system integrity and security by modifying and spreading across the file system.

The virus specifically targets .py files because higher privilege accounts, such as system administrators, typically rely on Python for various administrative tasks and scripts. These accounts often have elevated access rights, which makes them a prime target for malware designed to exploit their permissions. By focusing on Python files, the virus takes advantage of the fact that these files are commonly present and frequently executed by privileged users. Once the virus infects these files, it ensures that it operates under the radar, leveraging the trust placed in administrative tasks that use Python scripts. As a result, the virus spreads quietly among the system's critical administrative operations, potentially allowing further exploitation of the compromised environment (Figure 2).

To execute the virus, a timer or a specific execution time can be defined, but in this demonstration, a timer was used for quicker testing. When the virus runs, it will enumerate files and infect those that meet the specified criteria.

To test the functionality of the virus, a controlled environment was created with several Python files in the same directory. Upon execution, the virus successfully inserted the infection message into the files, indicating that it was operating correctly.



```
┌──(kali㉿kali)-[~/Downloads/testvirus]
└─$ chmod 755 virus.py

┌──(kali㉿kali)-[~/Downloads/testvirus]
└─$ ls -ll
total 8
-rw-r--r-- 1 kali kali  293 May  9 02:08 test_files_generator.py
-rwxr-xr-x 1 kali kali 3469 May  9 02:19 virus.py

┌──(kali㉿kali)-[~/Downloads/testvirus]
└─$ ./virus.py
['/home/kali/Downloads/testvirus/virus.py', '/home/kali/Downloads/testvirus/test_files_generator.py']

┌──(kali㉿kali)-[~/Downloads/testvirus]
└─$ cat test_files_generator.py
This is a Virus! You are infected!
This is a Virus! You are infected!
#!/usr/bin/env python
# -*-coding:utf-8 -*-



if __name__ == '__main__':
    filenames = ["test1.py", "test2.py", "test3.py"]
    data = 'print("hello")\n'

    for file in filenames:
        f = open(file, "w")
        f.write(data)
        f.close()
```

Fig. 2. Repeat access virus testing

The next phase involved turning the virus into a trojan. Trojans are highly dangerous forms of malware due to their ability to load other malware types, execute arbitrary commands, and compromise victim systems without detection. The virus, when deployed as a trojan, can operate covertly while spreading malware or executing harmful actions on the compromised system.

The trojan was disguised as a legitimate PDF file containing course materials. This method, known as **file obfuscation**, involves modifying the appearance of a file to make it seem like an innocuous document (e.g., a PDF) while in reality, it is an executable file.

To achieve this, the .exe file was uploaded to a public document upload platform (e.g., Dropbox), and the file's extension was manipulated using the **Right-to-Left Override (RLO)** technique [7].

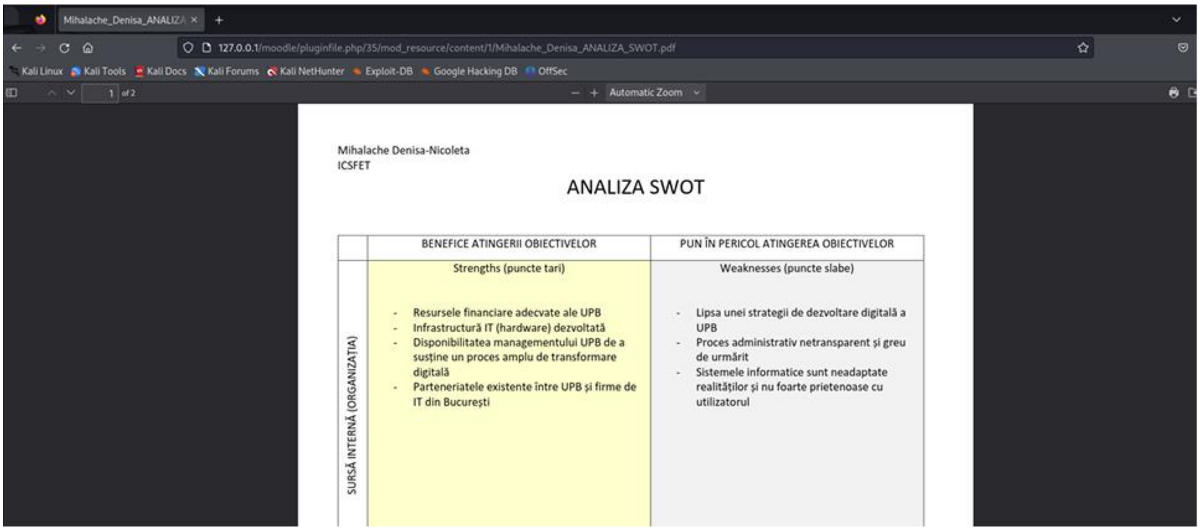
The use of Dropbox in the attack is essential for distributing the malicious file while bypassing security filters. Dropbox offers public, easy-to-share file hosting, making it harder for security systems to flag the file as suspicious. By uploading the disguised .exe file with a manipulated name using the Right-to-Left Override (RLO) technique, the attacker masks its true nature, making it appear as a benign document. The public, trusted nature of Dropbox increases the file's legitimacy, and the attacker can easily distribute the link via email or other platforms. This approach allows the attacker to reach multiple victims with minimal risk of detection.

Right-to-Left Override (RLO) technique exploits the way certain languages, like Arabic, are written from right to left. In most systems, file names are displayed left to right, but when the RLO character is inserted into a file name, it causes the system to interpret and display the file name in reverse order.

For example, the attacker might rename a file trojan.exe to something like trojan.pdf by inserting an RLO character before the .exe extension. This character effectively "reverses" the order in which the file name is displayed, making it appear as though the file ends with .pdf instead of .exe. In this case, the RLO character forces the system to read the file extension as .pdf, while the true file extension .exe is still present but hidden from view.

This manipulation makes the file appear as a benign PDF document when viewed by users or security software, but in reality, it is an executable file that can execute malicious code when opened. Since the file's extension is disguised, it bypasses user suspicion and may evade basic security checks that rely on extension names to determine the file's type.

When accessing a course material on Moodle, it appears as a file with a path such as file.pdf, which allows for the simultaneous loading of two URLs: one legitimate (for the course content) and one malicious (containing the virus). This is achieved through an AutoIt script that swaps the two URLs, redirecting the user to the malicious content while still displaying a legitimate appearance (Figure 3).



127.0.0.1/moodle/pluginfile.php/35/mod_resource/content/1/Mihalache_Denisa_ANALIZA_SWOT.pdf

Mihalache Denisa-Nicoleta
ICSFET

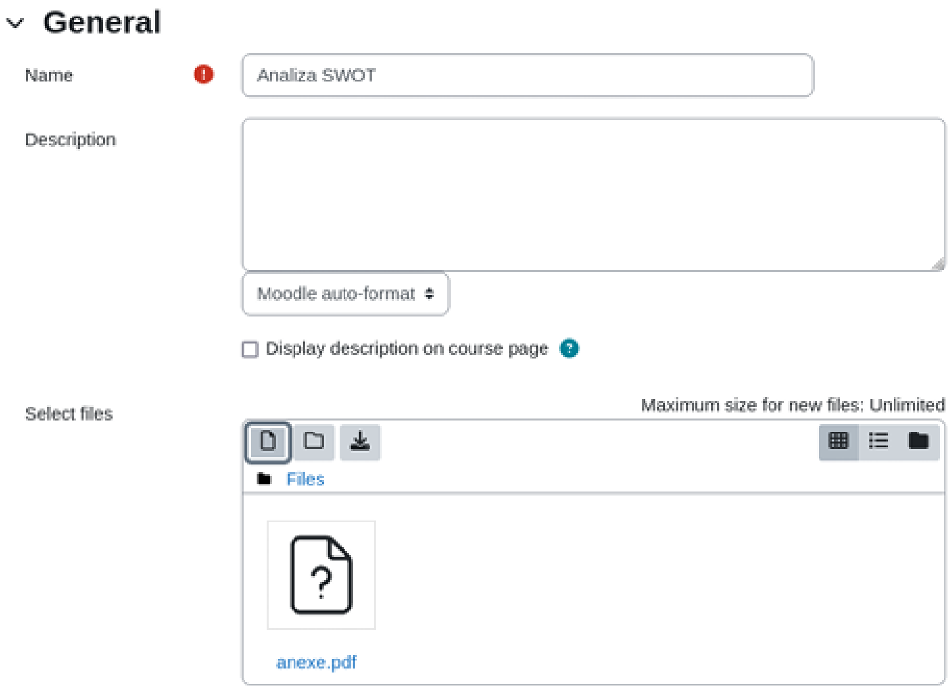
ANALIZA SWOT

	BENEFICE ATINGERII OBIECTIVELOR	PUN ÎN PERICOL ATINGEREA OBIECTIVELOR
SURSĂ INTERNĂ (ORGANIZAȚIA)	Strengths (puncte tari) - Resursele financiare adecvate ale UPB - Infrastructură IT (hardware) dezvoltată - Disponibilitatea managementului UPB de a susține un proces amplu de transformare digitală - Parteneriatele existente între UPB și firme de IT din București	Weaknesses (puncte slabe) - Lipsa unei strategii de dezvoltare digitală a UPB - Proces administrativ netransparent și greu de urmărit - Sistemele informatice sunt neadaptate realităților și nu foarte prietenoase cu utilizatorul

Fig. 3. Vulnerable URL

The script effectively manipulates the request, making the malicious file appear to be a harmless course material file. The AutoIt script automates this URL redirection, enhancing the attack's effectiveness and stealth. The script, saved as trojan.au3, automates this redirection. Additionally, to make the malicious file appear legitimate, the attacker converts the PDF icon into a .ico format, giving it a harmless appearance. The final executable, now appearing as a PDF, is then delivered to the victim, masking its true nature and increasing the likelihood of execution (Figure 4).

The trojan was renamed and uploaded to a platform where users could download it, such as an online course platform (Moodle), disguised as a legitimate course file. Upon downloading and executing the file, the trojan would begin its operation, infecting the system and potentially executing further malicious payloads, such as backdoors or additional malware.



General

Name: Analiza SWOT

Description:

Moodle auto-format

□ Display description on course page

Select files

Maximum size for new files: Unlimited

Files

anexe.pdf

Fig. 4. Uploading the malicious file "*anexe.pdf*"

4. Conclusion

The domain of web server and web application security is vast and continuously evolving, with new threats emerging regularly as technology advances.

Ethical hacking is vital because it simulates real-world attacks, helping organizations uncover vulnerabilities early in the process. By proactively testing systems, networks, and applications, organizations can address weaknesses before they are exploited by malicious actors, ensuring a stronger defense against potential threats. Integrating security testing into the development and operational phases is a strategic approach to maintaining the trust of customers and stakeholders while safeguarding data and systems from unauthorized access.

Malware threats continue to evolve, becoming more sophisticated and harder to detect. The research highlighted the limitations of current malware detection solutions, which often struggle to keep pace with the rapid development of new malware variants. By employing dynamic analysis techniques and behavior-based detection, the time required to identify and mitigate malware infections can be reduced. Sandbox environments, in particular, proved valuable for observing malware behavior in a controlled environment, allowing for more precise identification and prompt response. All software, including web servers and applications, must be updated with the latest security patches.

Password security is a fundamental aspect of web application security, yet many systems still rely on weak password storage mechanisms and inadequate password policies. The brute-force password cracking attack was demonstrated practically. Findings underscored the importance of adopting complex password storage and encryption mechanisms and implementing multi-factor authentication (MFA) to enhance security. Educating users on secure password creation practices is also crucial to reduce the risk of password cracking.

In conclusion, this research focused on the most prevalent attack vectors targeting widely utilized e-learning platform, addressing key security challenges. Progress in testing methods, attack replication, and comprehensive risk assessments offers a strong basis for enhancing the security of web applications. As cyber threats continue to evolve, sustained research and innovation will be crucial to preserving a secure and resilient web infrastructure.

References

[1]. S. Qadir and S. Quadri, "Information Availability: An Insight into the Most Important Attribute of Information Security," Journal of Information Security, 2015.

[2]. M. Walker, "Certified Ethical Hacker Exam Guide," SYBEX, 2012, pp. 48-55.

[3]. D. Ghimiray and O. Buxton, "Hacker Types: Black Hat, White Hat, and Gray Hat Hackers," 03 11 2023. [Online]. Available: https://www.avast.com/c-hacker-types. Accessed September 7, 2024.

[4]. R. Messier, C|EH - Certified Ethical Hacker - Study guide, SYBEX, 2023.

[5]. J. Grossman, R. Hansen, P. Petkov, A. Rage and S. Fogie, "XSS Attacks: Cross Site Scripting Exploits and Defense," in XSS Attacks: Cross Site Scripting Exploits and Defense, Syngress, 2007, pp. 67-75.

[6]. Malwarebytes, "Malware," [Online]. Available: https://www.malwarebytes.com/malware. Accessed October 15, 2024.

[7]. M. ATT&CK, "Masquerading: Right-to-Left Override," 14 10 2021. [Online]. Available: https://attack.mitre.org/techniques/T1036/002/. Accessed October 9, 2024.

Author Guidelines

As an author, you are kindly advised to follow the next instructions. Reading and understanding the requirements before submittal would ensure adherence to the International Conference on Cybersecurity and Cybercrime standards and would facilitate acceptance by the scientific reviewers.

1. Papers must be submitted in English having an even number of pages (minimum 4 pages). At least 50% of the last page should be occupied by text.
2. For papers writing it is recommended the use the text processor Microsoft Word and one of the template models found on the conference website. We will do the final formatting and all necessary format conversions of your paper.
3. The papers will be submitted using our online interface. Please do not send your papers by email.
4. The papers will be reviewed by two scientific reviewers, well-known in their domains of activity. Usually, it takes 1 to 3 months between the moment you finished your submission and a response is given by scientific reviewers.
5. The papers will be sent back to the authors for corrections if the figures, pictures, or tables are not contained in the text or if the reviewers require modifications or supplementary information.
6. The papers will be rejected if their scientific content is not adequate, if they don't contain original elements and if they are not properly written in English.
7. The bibliography must show the authors adequate documentation. At least 7-10 quality references should be cited.
8. Citation standard is IEEE. Please read the IEEE Citation Reference from the website: www.ieee.org/documents/ieeecitationref.pdf.
9. The whole responsibility for the calculation exactitude, experimental data, scientific affirmation, and paper translation belongs to the authors.
10. The authors will declare on their own responsibility that the article or parts of it were not published before in other journals.

More information: proceedings.cybercon.ro/index.php/ic3/author-guidelines

The Romanian Association for Information Security Assurance (RAISA)

The Romanian Association for Information Security Assurance (RAISA) is a professional, non-governmental, non-partisan political, nonprofit, and public benefit association.

RAISA AIM

The aim of the Romanian Association for Information Security Assurance is promoting and supporting information security activities in compliance with applicable laws.

RAISA VISION

The vision of the Association is to promote research and education in information security field and to contribute to the creation and dissemination of knowledge and technology in this domain. RAISA has a strong representation at the national level, bringing together professors and researchers from top universities and Romanian institutions, PhD, master's, and license students, as well as companies in the IT segment.

RAISA OBJECTIVES

To achieve the stated purpose, the Romanian Association for Information Security Assurance proposes the following objectives:

- Collaboration with the academic community from Romania or abroad in order to organize conferences, scientific seminars and workshops for presenting the development and implementation of effective measures to improve information security.
- Collaboration with research centers, associations, and companies from Romania or abroad, to organize informative events in information technology security field.
- To perform specific programs for education and training of personnel involved in electronic information management (data processing, storage, security).
- To ensure the dissemination of notice relating to existing vulnerabilities and nationally and internationally newly identified threats; to provide solutions for data restoration and policies to prevent and combat incidents based on the information provided by suppliers of software solutions.
- To publish scientific journals for university staff, PhD students or master's students, researchers, students, and other professional categories in the field of information security and cybercrime.
- To grant awards, scholarships, or sponsorships to people with outstanding merits in the field of information security.

Website: www.raisa.org
Email: contact@raisa.org

RAISA Members Benefits

RAISA MEMBERS

The Romanian Association for Information Security Assurance (RAISA) is an organization that consists of:

- **Founding members** - are individuals who have participated in the founding process of the Association, have agreed with the Statute of the Association at the date of establishment and are parts of the members' category, with all their rights. The founding members pay annual membership fee and have the right to deliberative vote during the General Assembly.
- **Members** - are individuals who have joined the Association after the date of establishment. The members pay annual membership fee and have all the rights, respecting the obligations stipulated in Statute of the Association. They have the right to deliberative vote during the General Assembly.
- **Honorary Members** - can be scientists, professors, cultural or religious personalities, valuable professionals, who have rendered outstanding services to the Association. They are exempted from contributions and their vote is advisory.
- **Collaborators/Volunteers** - anyone who wants to participate in Association activities without becoming a member. Their collaborations are on no-cost basis; they don't pay a membership fee and don't have the right to vote.

RAISA MEMBERSHIP BENEFITS:

- Free access to RAISA events.
- Discount to workshops and conferences supported by RAISA.
- Discount for professional courses organized by RAISA.
- Possibility to be involved in RAISA projects and campaigns, support offered for research.
- Free publishing for scientific articles in the International Journal for Information Security and Cybercrime (IJISC), indexed in international databases.
- Discount for books and scientific studies promoted by RAISA.
- The possibility of promoting the events on RAISA media channels:
    - www.securitatea-cibernetica.ro
    - www.securitatea-informatiilor.ro
    - www.criminalitatea-informatica.ro

Get the most from your membership!

www.raisa.org/raisa-members/