Romanian Association for
Information Security Assurance

# PROCEEDINGS
# OF
# THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume IX
eISSN 2393-0837


CyberCon Romania
2022


THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

# PROCEEDINGS
## OF
## THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume IX

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


**CyberCon Romania**
**2022**


# 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**: https://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

## EDITORIAL COUNCIL CHAIRMAN

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

## INTERNATIONAL ADVISORY BOARD

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

Professor **Angelica BACIVAROV**, PhD
University Politehnica of Bucharest, Romania

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

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

**Viorel GAFTEA**, PhD
Romanian Academy, Romania

Professor **Fabrice GUERIN**, PhD
ISTIA, University of Angers, France

**Angela IONIȚĂ**, PhD
Research Institute for A.I., Romania

**Cristian PAȚACHIA - SULTĂNOIU**
Orange, Romania

Professor **Daniela-Elena POPESCU**, PhD
University of Oradea, Romania

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

Assoc. Prof. **Eduard-Cristian POPOVICI**, PhD
University Politehnica of Bucharest, Romania

Professor **Răzvan RUGHINIȘ**, PhD
University Politehnica of Bucharest, Romania

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

Assoc. Prof. **Emil SIMION**, PhD
University Politehnica of Bucharest, Romania

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

Professor **Sandeep TIWARI**, PhD
Amity University, India

Professor **Dănuț TURCU**, PhD
"Carol I" National Defence University, Romania

Professor **Ton van der WIELE**, PhD
Erasmus University Rotterdam, Netherlands

## ORGANIZING COMMITTEE

**Sabina-Daniela AXINTE**, PhD
University Politehnica of Bucharest, Romania

**Larisa GĂBUDEANU**, PhD
Babeș-Bolyai University, Romania

**Ioan-Cosmin MIHAI**, PhD
"Al. I. Cuza" Police Academy, Romania

**Gabriel PETRICĂ**, PhD
University Politehnica of Bucharest, Romania

# TABLE OF CONTENTS

# AI and IoT Mapping and the Transition to an Interconnected Cyber Defence and Intelligence Capabilities

**Joseph JONES[1], Angela IONIȚĂ, PhD[2], Ioan-Cosmin MIHAI, PhD[3]**
[1] OS2INT, Skive, Denmark
joseph.jones@os2int.com
[2] Romanian Academy
aionita@racai.ro
[3] Police Academy, Romania
cosmin.mihai@academiadepolitie.ro

**Abstract**

*This paper brings together authors from a diverse range of technical areas to discuss the evolving cyber threat landscape and how military forces, have transformed their capabilities to meet present-day operational challenges in cyberspace. The Internet of Things (IoT) is based on the premise that enough data can lead to new perspectives on processes and systems. With over 7 billion IoT devices connected today, experts expect that number to increase to 22 billion by 2025. They can be used to support decisions and new products and services, or they can lead to internal savings and new external revenue streams. Despite countless discussions and opinions on the definition of AI in its various facets, successful IoT implementation projects require major actors to play their part, but in conjunction with human experts to work with to make better decisions in cyberspace, improving the quality of human-machine team's actions in asymmetric operations. The Defence domain already looking at ways to organize better human-machine teams, which promise to boost individual and team performance, reduce threats to humans, enable new operating concepts, and ultimately boost national power.*

**Index terms:** AI, Decision-making, Human-machine teams, Hyperautomation, IoT

## 1. Introduction

In the digital age we are going through, we must be aware that the Internet of Things (IoT) is driving significant and impactful change across verticals markets. While IoT devices can be found throughout our homes, the number of IoT devices that are being deployed across industrial environments and defense is also growing simultaneously.

Each application is unique and may require different forms of IoT connectivity and it is important for organizations to understand and weigh the pros and cons of each technology before deploying to ensure they are receiving proper connectivity. IoT has become essential to create efficiencies and improve lives globally, and with this comes the need for organizations to pivot and adapt to technological advances to stay relevant, competitive, and effective.

According to [30] it is expected that by 2026, the global IoT market will reach a value of $1.4 billion. This growing adoption is said to be "*fueling the next industrial revolution of connectivity*," shifting the way industries and organizations approach processes and systems with efficiencies and downtime top of mind.

*"As IoT technology continues to evolve, businesses and organizations are progressing with it, taking advantage of the opportunity to develop more efficient and effective processes. While the "industrial revolution of connectivity" may be a work in progress, IoT technologies will continue to drive progress and change everywhere*." [30].

The most recognizable shift in the modern-day battlefield is that information became the most effective weapon of all and moving towards an interconnected cyber defence and intelligence capabilities. The situational awareness based on the collected information became the core of every operation. Information operations as a new domain entered the battlefield, the integrated network of sensors, weapon systems and platforms became force multiplier [6].

According to Statista [23], "*The total installed base of Internet of Things (IoT) connected devices is projected to amount to 75.44 billion worldwide by 2025, a fivefold increase in ten years*." (Fig. 1).

In the future, it is expected that operations will rely less on human soldiers and more on interconnected technology, leveraging advancements in embedded systems and machine intelligence to achieve superior defense capabilities. In the future of new concepts, new technologies, new tools, and processes appeared based on the concept of network-centric warfare.

Over time, several different terms have been introduced to describe the use of IoT technology for reconnaissance, environment surveillance, unmanned warfare, and other combat purposes. These terms include the Internet of Military Things (IoMT) [7], the Internet of Battle Things [20], and the Internet of Battlefield Things (IoBT).

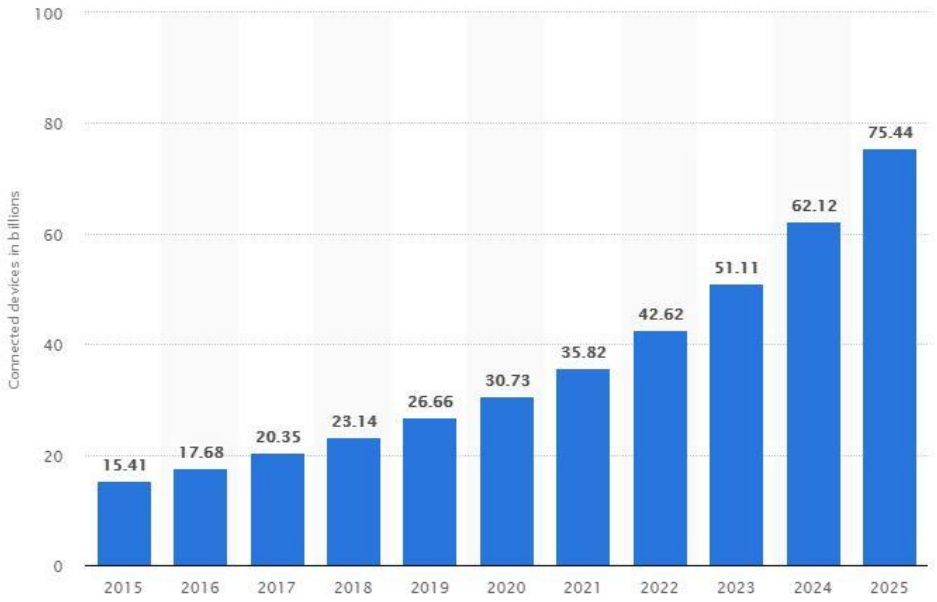



**Fig. 1.** Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025

One of the best visions of the future was made by Defense Secretary of USA, Lloyd Austin [22]: "*What we need is the right mix of technology, operational concepts and capabilities -- all woven together in a networked way that is so credible, flexible and formidable that it will give any adversary pause*" Austin said. "*We need to create advantages for us and dilemmas for them."*

## 2. Operational and intelligence decision-making in the evolution of Remote and Automated Systems (RAS)

Digital technologies lie at the heart of nearly every domain today. The automation and greater connectedness they afford have revolutionized the world's institutions - but they have also brought

risk e. g. in the form of cyberattacks. Threat intelligence is knowledge that allows you to prevent or mitigate those attacks. Rooted in data, threat intelligence provides context - like who is attacking, what their motivation and capabilities are, and what indicators of compromise in some systems to look for - that helps make informed decisions about security. "*Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject's response to that menace or hazard.*" [26].

For the image to be as close as possible to the real one, it is necessary firstly, for this section, to highlight what automation and automated system refers to.

Automation is making waves in many industries worldwide and encompasses a wide range of technologies including endpoint management, robotic process automation (RPA), artificial intelligence (AI) and machine learning (ML).

Without any doubts, the trends highlighted in Gartner's top ten strategic technology for 2021 [37] have an impact on all areas of life and goes beyond the automation provided by rigid programming models, and they exploit AI to deliver advanced behaviors that interact more naturally with their surroundings and with people. As predicted by Gartner, as the technology capability improves, regulation permits and social acceptance grows, autonomous things will increasingly be deployed in uncontrolled public spaces.

For a better understanding of the evolution and new trends, it would be good to go through a short history of autonomous military systems offered by literature. This short history tells us that autonomous military systems have been used by armed forces around the world for many decades. All of these can trace their past to as early as the First World War and their importance to the battlefields of the future is expected to grow exponentially.

Today they can be found performing various combat roles from search and rescue, explosive disarmament, fire support, reconnaissance, logistics support and, of course, lethal combat duties to name but a few. Many believe will see fully automated lethal autonomous systems soon potentially making the role of human soldier obsolete.

Despite other fears, it should be noted that many military vehicles with combat capability are prevented from being fully autonomous presently. This is by design to ensure there is some human input at times to ensure targets are not within restricted fire zones under the laws of war set out in the Geneva Convention [8].

In [25] there is a quick tour of the history of autonomous military systems (including remote controlled, semi- and fully-autonomous) and highlighted some interesting examples. But there is an enormous variety of autonomous military systems and, as such, it has not been possible to cover them all. Autonomous systems for the military, also called autonomous robots or remote-controlled drones, have had a surprisingly long and interesting history. Though they have come to prominence and large-scale use in recent years, their ancestors were first used during the First and Second World War and the Cold War that followed them.

Military autonomous systems are likely to grow in numbers and roles exponentially in the future as armies continue to develop and invest in this technology. Some military experts believe that not only will combat robots be a reality very soon but also that robots will outnumber actual service personnel in the U.S. Army by 2025.

Automation was highlighted in Gartner's published top ten strategic technology trends for 2020 [38]. One trend is what Gartner calls "*hyperautomation*" the combination of multiple machine learning, packaged software, and automation tools to deliver work, referring to all the steps of automation-discover, analyze, design, automate, measure, monitor and reassess. Understanding the range of automation mechanisms, how they relate to one another and how they can be combined and coordinated is a major focus for hyperautomation.

Another trend identified by Gartner is "*autonomous things."* [39]. These are physical devices that use AI to automate functions previously performed by humans. The most recognizable forms of autonomous things are robots, drones, autonomous vehicles/ships, and appliances. The main purpose of an automated system is to help speed up a process. Automated systems eliminate the need for human interference to complete a task. Tasks that are time-consuming or inconvenient are often incorporated into systems.

Automated Systems have key components that allow them to function properly including a control system, a way to interpret and distribute data and a human interface. Programmable logic allows the system to process data and control it. Automated systems have been incorporated into production lines and machines for years. Several industrial domains use automated systems to increase production and reduce costs. An example is the computer industry where there are many tasks that do not require constant human attention. Software can be used to complete several different tasks and automatically post the results. Bots can be programmed to click objects on the screen, send messages at preset times or interact on social networks using artificial intelligence. Another common example is an ATM, which can process banking transactions without a teller.

According to Kaseya [40] in different stages of their evolution automation technologies refers to a simple three-level hierarchy presented in Fig. 3.

Another trend identified by Gartner refer to *multiexperience.* Through 2028, the user experience will undergo a significant shift in how users perceive the digital world and how they interact with it. Conversational platforms are changing the way in which people interact with the digital world. Virtual reality (VR), augmented reality (AR) and mixed reality (MR) are changing the way in which people perceive the digital world. This combined shift in both perception and interaction models leads to the future multisensory and multimodal experience.

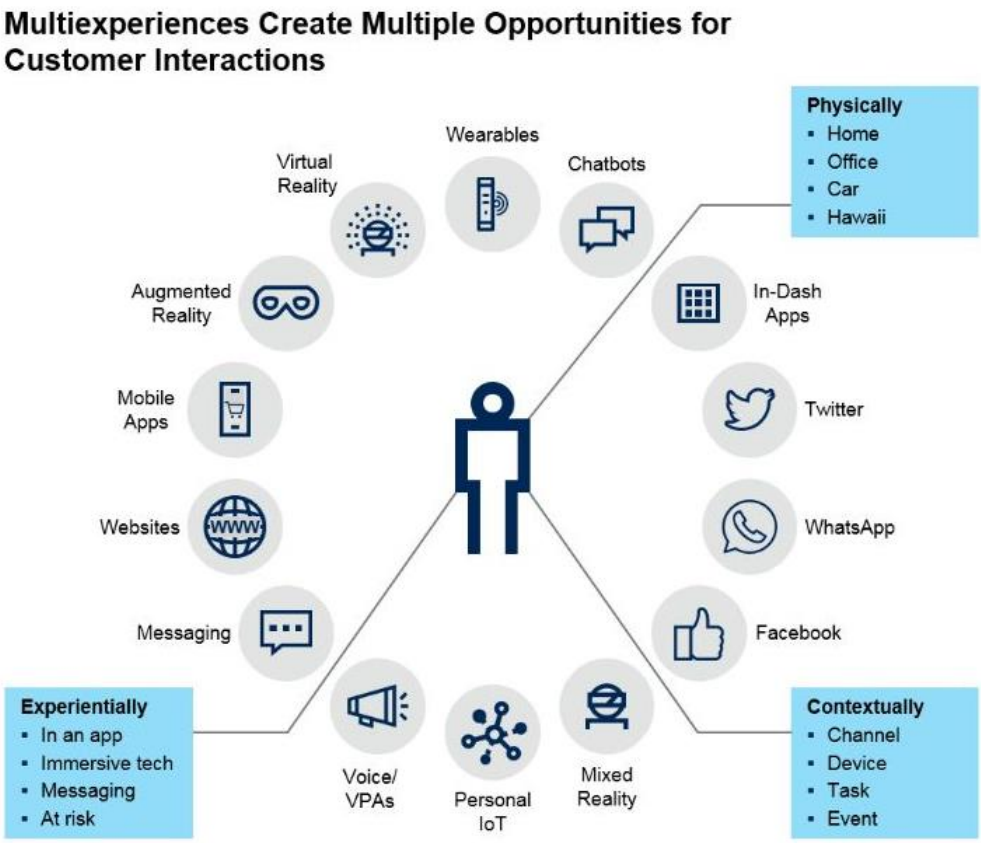



**Fig. 2.** Opportunities created by multiexperiences
Source: Gartner, 2020

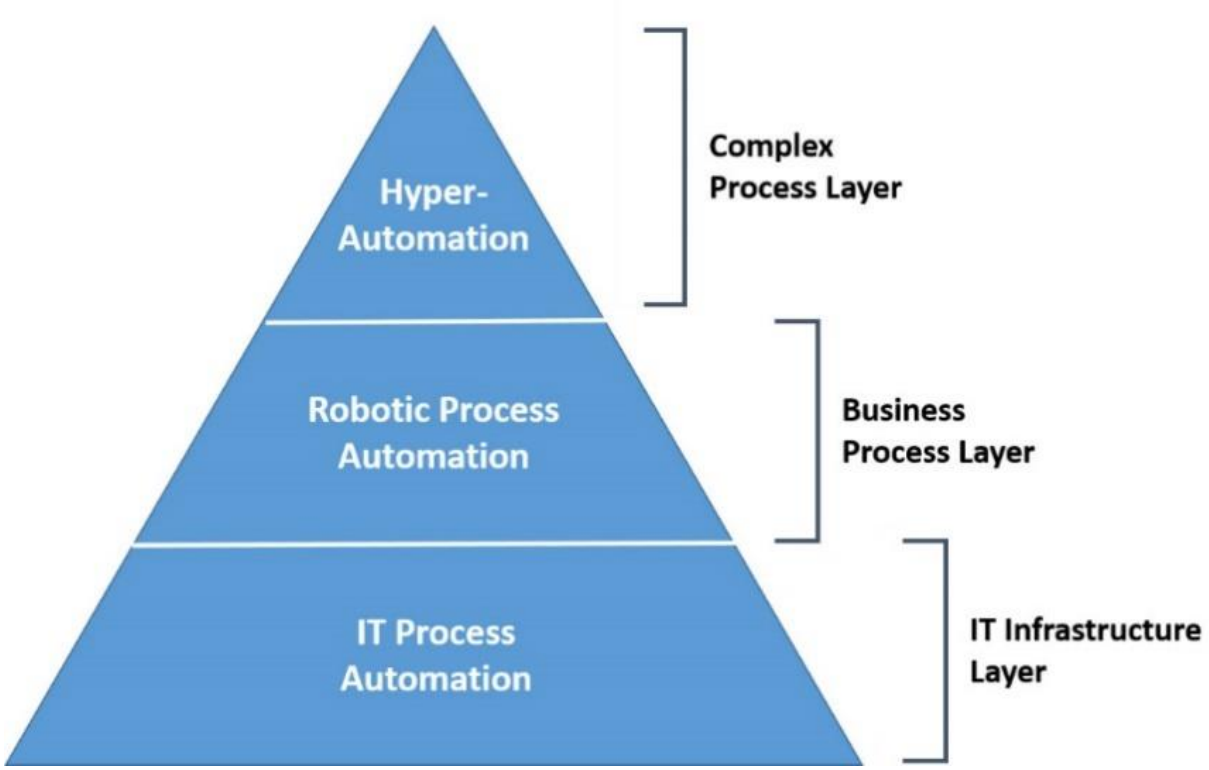
Through 2023, Gartner expects four key aspects of the *democratization* trend to accelerate, including democratization of data and analytics (tools targeting data scientists expanding to target the professional developer community), democratization of development (AI tools to leverage in custom-developed applications), democratization of design (expanding on the low-code, no-code phenomena with automation of additional application development functions to empower the citizen-developer) and democratization of knowledge (non-IT professionals gaining access to tools and expert systems that empower them to exploit and apply specialized skills beyond their own expertise and training).
Democratization is focused on providing people with access to technical expertise (e.g., ML, application development) or business domain expertise (for example, sales process, economic analysis) via a radically simplified experience and without requiring extensive and costly training. "Citizen access" (e.g., citizen data scientists, citizen integrators), as well as the evolution of citizen development and no-code models, are examples of democratization.

Over the next 10 years increasing levels of physical and cognitive *human augmentation* will become prevalent as individuals seek personal enhancements. This will create a new "consumerization" effect where employees seek to exploit their personal enhancements - and even extend them - to improve their office environment.

Human augmentation explores how technology can be used to deliver cognitive and physical improvements as an integral part of the human experience.

Another trend focused on *transparency* and *traceability* and refer to a range of attitudes, actions and supporting technologies and practices designed to address regulatory requirements, preserve an ethical approach to use of AI and other advanced technologies, and repair the growing lack of trust in companies. As organizations build out transparency and trust practices, they must focus on three areas:

(1) AI and ML;
(2) personal data privacy, ownership, and control; and
(3) ethically aligned design.



| IT Process Automation | Robotic Process Automation | Hyperautomation |
|---|---|---|
| The foundational layer of all automation technologies is the automation of IT processes. This involves the automation of routine IT tasks and workflows (e.g., server maintenance, software patch management and software updates and includes auto-remediation of IT incidents and associated service tickets). | RPA is the business process layer. In RPA, simple, repeatable rules are followed by "bots" or virtual systems to automate manual computing steps or simple business processes.<br>Research firm Gartner predicted that the global robotic process automation (RPA) market revenue will reach $1.89 billion in 2021 - an increase of 19.5 percent from 2020. | Hyperautomation brings together artificial intelligence/machine learning (AI/ML) tools with RPA to enable the automation of complex business processes.<br>Hyperautomation can lead to real digital transformation of the business. As one of the top 10 strategic trends of 2021 touted by Gartner (https://youtu.be/s3rlYW cwdDY), the idea of hyperautomation is to automate "anything" that can be automated.<br>Implementing hyperautomation requires streamlining entire processes, getting rid of legacy applications, and enforcing lean, optimized, and interconnected processes. |
| There are some benefits of IT Process Automation: reduced human error (Automating IT processes ensures there is accuracy in every step and reduces the chances of errors occurring), increased IT operational efficiency (IT process automation frees up IT technicians to work on more challenging tasks and strategic), higher system uptime (auto-remediation of incidents means that problems are resolved faster, and systems and services have higher availability). | Among benefits of RPA are cost-effectiveness, improved productivity and quality of work, better decision making.<br>Challenges with RPA count: scalability (unless the appropriate implementation processes are chosen with RPA, scaling can become an issue) and enabling end-to-end automation (RPA tools may be insufficient for complex processes and in such cases, may break down these processes into simpler tasks that can be automated with RPA or progress to hyperautomation). | Among benefits of Hyperautomation are: End-to-end automation (starting from process discovery to measuring return-on-investment (ROI), all of this can potentially be automated), significant transformation (when every part of a complex process is automated, the whole operation can be transformed).<br>There are some challenges with Hyperautomation. The major challenge with hyperautomation is automating complex processes. Grappling with process complexity can cause frustration and increase implementation costs |

**Fig. 3.** Hierarchy of Automation Technologies (adopted from [10])

It is important to perceive that we cope with significant shift from the centralized model of most public cloud services and that will lead to a new era in cloud computing: the era of *distributed cloud* (the distribution of public cloud services to different locations while the originating public cloud provider assumes responsibility for the operation, governance, updates to and evolution of the services).

According Gartner [39], another area is represented by *practical Blockchain* which remains immature for enterprise deployments due to a range of technical issues including poor scalability and interoperability.

AI and ML will continue to be applied to augment human decision making across a broad set of use cases. While this creates great opportunities to enable hyperautomation and leverage autonomous things to deliver business transformation, it creates significant new challenges for the security team [41] and risk leaders with a massive increase in potential points of attack with IoT, cloud computing, microservices and highly connected systems in smart spaces. *Security and risk leaders* should focus on three key areas - protecting AI-powered systems, leveraging AI to enhance security defense, and anticipating nefarious use of AI by attackers.

On the second, it must clarify what is *Operational Intelligence* (OI) and how it works, and which are OI benefits and challenges. OI is an approach to data analysis that enables decisions and actions in different, including business, operations to be based on real-time data as it is generated or

collected. Typically, the data analysis process is automated, and the resulting information is integrated into operational systems for immediate use by specialists.

OI applications are primarily targeted at front-line workers who, hopefully, can make better-informed decisions or take faster action on issues if they have access to timely intelligence and analytics. In addition, OI can be used to automatically trigger responses to specified events or conditions.

What is now known as OI evolved from operational business intelligence, an initial step focused more on applying traditional Business Intelligence (BI) querying and reporting. OI takes the concept to a higher analytics level, but operational BI is sometimes still used interchangeably with operational intelligence as a term.

In most OI initiatives, data analysis is done in tandem with data processing or shortly thereafter, so workers can quickly identify and act on problems and opportunities in different operations. Deployments often include real-time intelligence systems set up to analyse incoming data, plus real-time data integration tools to pull together different sets of relevant data for analysis.

Today, the cybersecurity industry faces numerous challenges - increasingly persistent and devious threat actors, a daily flood of data full of extraneous information and false alarms across multiple, unconnected security systems, and a serious shortage of skilled professionals.

Some specialised people try to incorporate threat data feeds into their network, but do not know what to do with all that extra data, adding to the burden of analysts who may not have the tools to decide what to prioritize and what to ignore.

Everyone can benefit from threat intelligence. Cyber threat intelligence is widely imagined to be the domain of elite analysts. It adds value across security functions for organizations of all sizes.

When threat intelligence is treated as a separate function within a broader security paradigm rather than an essential component that augments every other function, the result is that many of the people who would benefit the most from threat intelligence do not have access to it when they need it.

Security operations teams often prove routinely unable to process the alerts they receive - threat intelligence integrates with the security solutions already use, helping automatically prioritize and filter alerts and other threats. Vulnerability management teams must more accurately prioritize the most important vulnerabilities with access to the external insights and context provided by threat intelligence. And risk analysis and other high-level security processes could be enriched by the understanding of the current threat landscape that threat intelligence provides, including key insights on threat actors, their tactics, techniques, and procedures, and more from data sources across the web.

A cyber threat intelligence solution can address each of these issues. The best solutions use ML to automate data collection and processing, integrate with existing solutions, take in unstructured data from disparate sources, and then connect the dots by providing context on indicators of compromise (IoCs) and the tactics, techniques, and procedures (TTPs) of threat actors.

Threat intelligence is actionable - it is timely, provides context, and can be understood by the people in charge of making decisions.

Stream processing systems and big data platforms can also be part of the OI picture, particularly in applications that involve large amounts of data and require advanced analytics capabilities. In addition, various Information Technology (IT) vendors have combined data streaming, real-time monitoring, and data analytics tools to create specialized operational intelligence platforms.

As data is analyzed, organizations often present operational metrics, key performance indicators (KPIs) and insights to the workers in interactive dashboards that are embedded in the systems they use as part of their jobs; data visualizations are usually included to help make the information easy to understand. Alerts can also be sent to notify users of developments and data points that require their attention, and automated processes can be kicked off if predefined thresholds or other metrics are exceeded.

Between the benefits of OI implementations there is the ability to address operational issues and opportunities as they arise -- or even before they do, as in the case of predictive maintenance. OI also empowers workers to make more informed -- and conceivably better -- decisions on a day-by-day basis. Ultimately, if managed successfully, the increased visibility and insight into operations can lead to higher revenue and competitive advantages over rivals.

But there are also challenges. Building operational intelligence architecture typically involves piecing together different technologies, and there are numerous data processing platforms and analytics tools to choose between, some of which may require new skills. High performance and sufficient scalability are also needed to handle the real-time workloads and large volumes of data common in OI applications without choking the system.

The *threat intelligence* belongs three dimensions (Fig. 4): **strategic** (broader trends typically meant for a non-technical audience), **tactical** (outlines of the tactics, techniques, and procedures of threat actors for a more technical audience), **operational** (technical details about specific attacks and campaigns).


**Fig. 4.** The three dimensions of threat intelligence (adopted from [42])

*Strategic threat intelligence* [43] provides a broad overview of an organization's threat landscape. It is intended to inform high-level decisions made by decision makers - as such, the content is generally less technical and is presented through reports or briefings. Good strategic intelligence should provide insight into areas like the risks associated with certain lines of action, broad patterns in threat actor tactics and targets, and geopolitical events and trends.

Policy documents from nation-states or nongovernmental organizations, news from local and national media, industry- and subject-specific publications, or other subject-matter experts, white papers, research reports, and other content produced by security organizations there are as many common sources as possible of information for strategic threat intelligence.

Producing strong strategic threat intelligence starts with asking focused, specific questions to set the intelligence requirements. It also takes analysts with expertise outside of typical cybersecurity skills - in particular, a strong understanding of socio-political and business concepts.

Although the final product is non-technical, producing effective strategic intelligence takes deep research through massive volumes of data, often across multiple languages. That can make the initial collection and processing of data too difficult to perform manually, even for those rarefied analysts who possess the right language skills, technical background, and tradecraft. A threat intelligence solution that automates data collection and processing helps reduce this burden and allows analysts who do not have as much expertise to work more effectively.

*Tactical threat intelligence* [44] outlines the tactics, techniques, and procedures (TTPs) of threat actors. It usually includes technical context and is used by personnel directly involved in the defence, such as system architects, administrators, and security staff.

Reports produced by security vendors are often the easiest way to get tactical threat intelligence. Look for information in reports about the attack vectors, tools, and infrastructure that attackers are using, including specifics about what vulnerabilities are being targeted and what exploits attackers are leveraging, as well as what strategies and tools that they may be using to avoid or delay detection.

Tactical threat intelligence should be used to inform improvements to existing security controls and processes and speed up incident response. Because many of the questions answered by tactical intelligence are unique and need to be answered on a short deadline - for example, "*Is this critical vulnerability being exploited by threat actors targeting my industry present in my systems?"* - having a threat intelligence solution that integrates data from within own network is crucial.

*Operational intelligence* [45] is knowledge about cyber-attacks, events, or campaigns. It gives specialized insights that help incident response teams understand the nature, intent, and timing of specific attacks.

Because this usually includes technical information - information like what attack vector is being used, what vulnerabilities are being exploited, or what command and control domains are being employed - this kind of intelligence is also referred to as technical threat intelligence. A common source of technical information is threat data feeds, which usually focus on a single type of indicator, like malware hashes or suspicious domains. But if technical threat intelligence is strictly thought of as deriving from technical information like threat data feeds, then technical and operational threat intelligence are not totally synonymous - more like a Venn diagram with huge overlaps. Other sources of information on specific attacks can come from closed sources like the interception of threat group communications, either through infiltration or breaking into those channels of communication.

Consequently, there are a few barriers to gathering this kind of intelligence: **access**, **noise**, **obfuscation.**

*Threat intelligence* solutions that rely on ML processes for automated data collection on a large scale can overcome many of these issues when trying to develop effective operational threat intelligence. A solution that uses natural language processing, for example, will be able to gather information from foreign-language sources without needing human expertise to decipher it.

Thirdly, in [9] it is argued that AI will change decision-making in the defence and security arena in four principal ways. First, by enabling 'cognitive manoeuvre' the use of predictive analytics to enable much earlier intervention. Second, by forcing humans to take themselves 'out of the loop' for decision-making by out-performing them in an increasing number of domains. Third, by providing advice that is correct, but difficult to explain. Fourth, in the short term, by driving unprecedented rigour into decision-making processes, forcing decision-makers to be much more explicit about the mental models on which they are basing decisions, to enable comparison with automated analytics.

## 3. AI-development and conflict

The global artificial intelligence market size is expected to reach $169,411.8 million in 2025, from $4,065.0 million in 2016 growing at a CAGR of 55.6% from 2018 to 2025. Artificial intelligence has been one of the fastest-growing technologies in recent years [45]. AI is being used in every industry and is projected to be a core skill for the future. Artificial Intelligence represents a huge opportunity across virtually every sector. It has already proven to be disruptive, but it is anticipated that it will be much more widespread over the next few years. The professionals differentiate between an objective nature and a subjective character of conflict. Nature of conflict describes what conflict is and character of conflict describes how it is fought. Nature of conflict may be violent, interactive between opposing wills and fundamentally political. Conflict's character is influenced by technology,

law, ethics, culture, methods of social, political, and military organization and other factors that change across time and place. Character of conflict changes as much as professionals organize themselves to fight conflicts.

It has been not appreciated the changes in how conflict was tackling or in the character of conflict. Future development and deployment of human-machine teams and autonomous weapons systems represents such a shift in the character of conflict.

In near future in autonomy and machine learning it is expected significant advance, to include the emergence of robots working together in groups and as swarms. New and powerful robotic systems will be used to perform complex actions, make autonomous decisions, provide intelligence, surveillance, and reconnaissance, coverage, and speed response times over wider areas of the globe. Professional organizations must plan now for this new era of conflicts. Governments must be prepared for the political, strategic, and ethical dimensions of this shift in the character of conflicts.

Major technological breakthroughs that could occur in robotics as well as information, cognitive, and material sciences are, by themselves, truly revolutionary. Applications of AI have the potential to change the very nature of conflicts. At the strategic level, this could affect e.g., how the armed forces organize ground forces, how it fights and what types of major weapon systems it will need. At the operational and tactical levels, enemy's AI capabilities could dictate specific weapon systems design, the development of new types of units to address his AI capabilities and how brigade to squad level units conduct tactical operations [36].

But some questions remain:

- should the technology develop the way it is expected to, removing a man from the loop could allow machine conflict to be fully unleashed?
- AI so radically changes everything so that war itself may not resemble what it has been for the entirety of human history?

From this point of view, at the present state of development AI technologies are considered immature. Modern unmanned aircraft in service can operate autonomously but cannot yet execute the sorts of complex missions that manned equivalents can achieve. Land robots are clumsy on uneven terrain. Concepts fail to deliver significant breakthroughs in autonomous decision making. There is considerable wariness that the hype and publicity surrounding deep learning will not pan out as dramatic breakthroughs.

The present developments of AI technologies in military domain have not reached the level when it can be said that it would change the nature of war. In fact, it is in a nascent state of development. However, the scenario is changing fast. Despite best efforts, no nation-state can ever be fully prepared for the character of the next war. As such, potential military applications of emergent technology should not be viewed as a panacea for the chaos, friction, and chance that will continue to define war in the future. Regardless of the possibilities offered by technological advances, success in the next conflict is likely to be just as reliant on human genius.

Today, we are at a major inflection point, one in which technology is reshaping the way conflicts are tackling [13]. "*The future of warfare will be shaped by the role of smaller drones; robots on the battlefield, offensive cyberwar capabilities, extraordinary surveillance capabilities both on the battlefield and of individuals, greater reliance on special operations forces operating in non-conventional conflicts and militarization of the space"*. [24].

There are arguments that AI has the potential to go beyond shaping the character of conflict and change the nature of conflict itself because conflicts it is expected to be fought by robotic systems, not people. AI has the potential to engage in planning and decision making that were previously human endeavours.

The character of conflicts changes together with the tools that become available and how they influence the ways professionals organize themselves to fight conflicts. AI is one of the major developments of our time. ML and particularly the implications that go with it, is shaking up many

aspects of how things do, allowing us to deploy AI software where previously used a human or a more inefficient process. Sometimes this is to the consternation of people, particularly those who worry about AI systems and machine intelligence taking over human jobs, or perhaps the sci-fi scenario of AI being intelligent and organized enough to overrule humans. AI systems have the potential to increase the speed with which countries can fight. Even if humans are still making final decisions about the use of lethal force, fighting at machine speed can dramatically increase the pace of operations.

There are several applications of AI currently in development or are at early stages. The neural networks can utilize imagery databases and classify scenes, allows for a more accurate assessment of specific locations. The processing power that is possible with narrow AI systems [47] have the potential to increase the speed of data analysis. Image recognition can achieve faster, more accurate results than humans can achieve today.

AI and ML can also help in that information gathering and decision-making process.

Successful implementation of AI might lead to new concepts of operation that could influence force structure and force employment, or how professionals organize themselves and plan operations. One possibility is the use of large numbers of smaller platforms for different operations, known as swarms. The algorithms and control systems designed to enable 'swarming' already there are in different sectors and in academia. Expensive, high quality platforms could become vulnerable to swarms of sensors and lower-cost weapons platforms that are effectively networked together. AI could thus help bring quantity back into the equation in the form of large numbers of robotic systems.

Another potential application for AI that could shape the character of conflict is coordination through layers of algorithms that work together to help manage complex operations. AI could accelerate trends that challenge these long running force structure imperatives, such as the need to defeat adversaries with advanced anti access, area denial (A2/AD) networks with tolerable costs.

All the modern armed forces face the same challenge. According to [24] despite spending billions in upgrading existing capabilities, very few of these platforms were designed to seamlessly integrate AI or partner with autonomous robotic systems. This means retrofitting is required, making emergent technology an integration problem. It is also likely to take significant time and effort for the professionals to adapt entrenched command and control approaches to absorb the shock generated by the introduction of artificial intelligence and autonomous systems [17]. AI, autonomous machines are almost certain to create new integration challenges.

According to [24] "*despite some rapid advances in AI development, it is estimated that it could take until 2060-2070 for it to reach the level of maturity required to satisfy many imagined military purposes*."

## 4. Human-machine teams in future asymmetric operations

In a study done by Center for Strategic and Budgetary Assessments (CSBA) and Mick Ryan (Australian Army) it stands out: "*By the middle of the 21st century, ground forces will employ tens of thousands of robots, and the decisions of human commanders will be shaped by artificial intelligence. Although the future is impossible to predict, trends in technology and warfare make this a near certainty. Military organizations must plan now for this new era of warfare. Governments must be prepared for the political, strategic, and ethical dimensions of this shift in the character of war."* [32]

Many governments and organizations have attempted to identify prevailing trends that will drive or influence strategy and national policy. Likewise, military organizations around the world are studying the changing character of war to inform force structure and procurement decisions. The uncertainty of the future security environment leads to more confusion and no precise predictions of the future. Prudence demands that governments and military organizations outline a range of expected future scenarios based on prevailing trends to inform their planning.

Assessments of the future security environment from Canada, the United States, the United Kingdom, Australia, and New Zealand [48, 49, 50, 51, 52, 53, 54] refers to several common themes and significant changes in demographics and urbanization, geopolitics, economics, the role of the state, the diffusion of power, climate, and resources. Also, emerging, and disruptive technology are forecasted. It is expected that these will not only affect the policy and strategy of nations but will also drive changes in the character of war and future ground force operations.

As mentioned in a Science and Technology Options Assessment Study [55]: "*in the EU there are currently many ongoing efforts towards the improvement of cybersecurity."* The mentioned study concludes that the use of a cybercapability maturity model is necessary for the coherent monitoring and further development of cybercapacities in the Common Security and Defence Policy (CDSP). *"Modelling is important, not only for covering all aspects of cybersecurity, but also for monitoring the maturity of efforts and diverting resources to the areas that need it most. In the CSDP context, there are additional factors that need to be considered for the protection of military and civilian missions, personnel, and infrastructures. The geographical dispersion of CSDP missions beyond the EU borders, the global nature of the threat agents, hybrid threats and the protection of deployed assets from cyberattacks are all challenges that require attention*."

According to [32] *although there are many trends, three key areas of change will most likely affect future ground forces the most: geopolitics, the changing nature of work, and the disruptive impact of robotics and AI.*

All these tendencies are interdependent and potentiate each other so that e.g., the change in the global civilian labour market will eventually affect military personnel management models. New technologies will permit the automation of many tasks currently performed by humans. As automation and AI allow civilian business leaders to place humans in different kinds of work, so too will military personnel planners be forced to think anew about the recruiting and employment opportunities of a new global workforce approach. It is likely to drive the creation of new military personnel models and in turn the designing of new ground force structures. This, along with the disruptive technologies of robotics, AI, and human augmentation could enable new operating concepts.

In addition to expected future geopolitical changes and new global approaches to workforce structures, the potential applications of robotics and AI will drive their military employment. The professionals will be necessary to pay attention to few aspects to describe the key drivers for forces to develop their future human-machine organizations. It is estimated that the teaming humans with robotic and AI capabilities can boost national military power and can improve individual and team performance while reducing threats to humans; military forces could employ robots on future asymmetric operations as an ethical preference; in their turn, future adversaries will use these technologies; robots and AI can improve all institutional and support functions of those forces.

The world is facing unprecedented effort in the development and adopting of AI and ML and undoubtedly recent advances in artificial opened a new universe of opportunities in asymmetric operations. Tasks once believed to mandate human intervention have since been surpassed by machine execution.

Problems once computationally complex infeasible can now be solved in near real-time. It still struggles to understand how to apply AI and ML in a safe, practical, and usable way.

One of the greatest challenges that slow down the use of AI/ML is how to fit the human and machine together. Human-Machine Teaming (HMT) is the concept at which humans and machines intersect and work together toward a common goal. For this partnership to be successful, it is need better insight, context, and explainability - not only for the human to understand the machine, but also reciprocally, for the machine to understand the human. The strengths and weaknesses of both the human and as well as machine must be identified so that it can be understand how the human and machine should communicate, reconcile differences, and agree on a conclusion. In other words, it

must be very well understood how to establish and maintain a common area between people and machines to achieve operational goals [1].

Another approach is by understanding how humans interact with different levels of automated technology [34]. While not all automation will meet the criteria for intelligent teammates, across asymmetric operations such as cyber defense many automated components are limited forms of adaptable automation; that is, they have low adaptability (they are all or none; on or off), or the adaptability is overly time consuming [33]. According [19] it is known in other applications that the development of a more intelligent, responsive, and contextualized teammate, or adaptive automation system, may offer a set of advantages. However, to date, there has been limited exploration of these types of systems as cybersecurity [3].

One of the questions refer to what does it mean for humans and machines to work together effectively on complex analytic tasks? Is human-human teaming the right analogue for this kind of human-machine interaction? Recent works [15], focuses on what behaviors are necessary that allow next-generation intelligent assistants to provide context-sensitive, proactive support for human analytic work - especially as teammates in a cybersecurity asymmetric operational environment. Many of these requirements are like other analytic work: awareness and understanding of a user's current goals and activities, the ability to generate flexible responses to abstractly formulated needs, and the capacity to learn from and adapt to changing circumstances.

*To achieve these behaviors, intelligent teammates require processes of coordination and communication that are reminiscent of but distinguishable from those observed in human teams* [28]. Teams in cybersecurity operations, especially those in operations centers have specific dynamics that are affected as much by context as they are by the operational environment [29]. If anything, context is the most important challenge to overcome. As work on intelligent agents continues, raises awareness of an over-reliance on human-human teaming constructs and use 'teaming' as a model on which to guide the work in human-machine teaming rather than a set of rules to define it.

Concerning the challenges referring to how machines to understand to provide effective decision support to human, they must be built on cognitive and behavioral models. According to [12] some efforts in user-centered design for cybersecurity have effectively incorporated solutions for decision support needs derived from cognitive work or task analyses.

But all these can fail by not evolving to meet changing human decision-making needs. There are more requests for tools within the machine systems that track human behavior, particularly changes in behavior together with changes in tasks or goals, and then adapt machines to those changes.

Cognitive models could provide the needed solutions [4]. Because they are formal representations, they can be integrated with other intelligent computational algorithms to directly inform the machine about the user [21] and they can further translate machine analytics into human-interpretable actions or representations in an interface.

Integrating these functions, the cognitive models can help adapt the machine behavior to meet evolving human needs, including adapting information for faster decisions, mitigating workload and fatigue, and potentially even acting autonomously, when necessary, to maintain team performance [5].

Since 2013, in [11] it was remarked that many of today's cyberattacks are the result of employee susceptibility to phishing and spear phishing attacks. These cyber attackers exploit human cognitive biases and emotions that can overrule more rational decision-making. Some proponents of the dual process model believe that this less rational heuristic-based decision-making is the default decision-making process.

It may be that the framework described in [27] which tied automation to human information processing, can be extended to cyber kill chains. Combined with task analyses, on the attacker side can develop a better understanding of how humans use existing capabilities along the

"reconnaissance, weaponization, delivery, exploitation, installation, C2, and action" phases [18], and examine how AI could be coordinating and planning alongside the human. For defenders, AI could focus on elements of detection, denial, disruption, degradation, deception, and containment procedures, in addition to the utility of automation for managing updates and patching. Potential must be weighed and measured against foreseeable negative interactions. Ironic results of implementing automation, including creating more (not less) work for humans, failing to decrease required manpower, de-skilling operators, reducing awareness, contributing to accidents and loss of life, and general changing of operator skill and demands must all be considered [2], [35], [14]. In the future, HMT will likely play a larger role in cybersecurity as part of an expert cybersecurity HMT consistently evaluating the network for vulnerabilities. Machines can play a useful role as part of an expert cybersecurity team. However, machines may also play a role in working directly with the average employee to keep him/her safe from cyberattacks. Perhaps this HMT is designed primarily to support task work but can also help prevent cyberattacks by providing decision support.

As Nathan Bos mentioned in [28], a teammate also has the capability to become a liability. It can be extended this further to two specific types of attacks. For example, the important decision making resides in the human, while most of the information gathering and analysis rests within the machine, the combination is an HMT highly vulnerable to integrity attacks (a disruption in the information viewed by the agent), and availability attacks (a disruption of the general operational ability to interact with the teammate, and for the AI to do its work). Adversarial ML will further and uniquely exploit security done by machines. Careless AI teammates could create a cybersecurity irony of automation: a system added to strengthen security, weakens it.

What to do now? A common language and accurate representations will go a long way toward improving the system and human interactions with AI as Cleotilde Gonzalez point in [28]. The combinations of allocation decisions within future HMT are huge, and unfeasible to evaluate in masse [16] even for the kill chain ideas proposed. In [34] noted the best configurations will be through trial and error. Also, modelling, as Leslie Blaha remarks to [28]. Design of AI must avoid the history of ironies known to be fatal to man and mission.

## 5. Instead of conclusions

There is a great potential for IoT technologies to revolutionize modern warfare, leveraging data and automation to deliver greater lethality and survivability to the warfighter while reducing cost and increasing efficiency. The development and deployment of IoT technologies across the modern-day battlefield requires many challenges to be solved.

Major trends include artificial intelligence (AI), robotics, and the internet of things (IoT) to optimize defense operations and augment military efficiency. Today, conventional warfare is increasingly being replaced by hybrid approaches that also combine cyber warfare and other frontiers. Emerging military technology trends are changing the battlefield in four aspects-connectivity, lethality, autonomy, and sustainability. Connectivity solutions address concerns about how combatants detect and locate their adversaries, communicate with each other, and direct operations.

Future research will need to prove that there are correct models in human decision making in asymmetric operations, especially in cybersecurity, so that they can be incorporated into existing machines and show how machine analytics and cognitive models are integrated. Several additional questions continue to arise regarding the degree to which cybersecurity can be addressed and understood.

In [28] noted that applied behavioral research in cybersecurity could be a focal point of research much more than it currently is. While large sums of money are being spent on both technology and personnel in this area, there has been relatively little research with any behavioral component.

From Nathan Bos vantage point [29], there are three high potential and under-researched topics:

- Information search. The observations of cyber defenders show that information search is a basic activity for many tasks beyond incident response. According to [31] search patterns do not necessarily resemble hypothesis-driven search patterns but are often better characterized as information foraging.
- Judgement with uncertainty and risk. Some systems have been conceptualized such that machines provide intelligence while humans perform the higher-order task of assessing risk, providing judgment, and making decisions under uncertainty. This arrangement is rapidly being re-negotiated, however, as new systems automate risk assessment, and make decisions according to rules both learned and inferred.
- Workforce development. The urgent need for a cyber workforce has led to many undocumented initiatives in recruitment, selection, training, and retraining. This could be a generational problem in educational research if it were understood as such. Of particular interest is the topic of retraining. This happens when staff from quite different specializations are retrained in cybersecurity and when busy professionals try to keep up with an unusually fast-moving field and simultaneously manage the moving interface between human cognition and intelligent tools.

## References

[1] Baber, C., Cook, K., Attfield, S., Blaha, L. M., Endert, A., & Franklin, L., 2018, A conceptual model for mixed-initiative sensemaking. ACM SIGCHI Sensemaking Workshop.

[2] Bainbridge, L., 1983, Ironies of automation. Automatica, 19(6), 775-779.

[3] Ben-Asher, N., Oltramari, A., Erbacher, R., & Gonzalez, C., 2015, Ontology-based Adaptive Systems of Cyber Defense. International Conference on Semantic Technology for Intelligence, Defense, and Security, 34-41.

[4] Blaha, L. M., 2018, Interactive OODA processes for operational joint human-machine intelligence. NATO IST-160 Specialist's Meeting: Big Data and Military Decision Making. Bordeaux, France.

[5] Blaha, L. M., Fisher, C. R., Walsh, M. W., Veksler, B. Z., & Gunzelmann, G., 2016, Real-time fatigue monitoring with computational cognitive models. International Conference on Augmented Cognition, 299-310.

[6] Bognár E. K., 2018, Possibilities and security challenges of using IoT for military purposes, Hadmérnök (XIII) 1II (2018), https://www.researchgate.net/publication/336253176_Possibilities_and_security_challenges_of_using_IoT_for_military_purposes, accessed on April 30, 2021.

[7] *GovTribe, 2017, "Internet of Battlefield Things (IoBT) Collaborative Research Alliance (CRA)". April 5, 2017.*

[8] Davison, Neil, 2018, "Autonomous weapon systems under international humanitarian law", https://www.icrc.org/en/document/autonomous-weapon-systems-under-international-humanitarian-law, accessed on April 1, 2022.

[9] Dear, Keith, 2019, Artificial Intelligence and Decision-Making, RUSI Journal, 29 November 2019Emmitt, John, 2021, The Evolution of Automation Technologies, https://www.kaseya.com/blog/2021/02/16/the-evolution-of-automation-technologies/, accessed on April 1, 2022.

[10] Emmitt, John, 2021, The Evolution of Automation Technologies, https://www.kaseya.com/blog/2021/02/16/the-evolution-of-automation-technologies/, accessed on April 1, 2022.

[11] Evans, J. B. & Stanovich, K. E. (2013). Dual-process theories of higher cognition: Advancing the debate. Perspectives on Psychological Science, 8, 223-241.

[12] Franklin, L., Pirrung, M., Blaha, L., Dowling, M., & Feng, M., 2017. Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design. IEEE Symposium on Visualization for Cyber Security, 1-8.

[13] Freedberg Jr., Sydney J., 2017, "War without Fear: DepSecDef Work on How AI Changes Conflict," Breaking Defense, May 31, 2017.

[14] Gutzwiller, R. S., Clegg, B. A., & Blitch, J. G., 2013, Part-task training in the context of automation: Current and future directions. American Journal of Psychology, 126(4), 417-432.

[15] Haimson, C., Paul, C. L., Nebesh, B., Joseph, S., & Rohrer, R., 2019, Do we need "teaming" to team with a Machine? HCI International Workshop on Human-Machine Teaming.

[16] Hancock, P., Mouloua, M., Gilson, R., Szalma, J., and Oron-Gilad, T., 2007, Provocation: Is the UAV Control Ratio the Right Question? Ergonomics in Design, 7, 30-31.

[17] Hoffman, F. G., 2017, Will War's Nature Change in the Seventh Military Revolution?, Parameters 47(4) Winter 2017-18Kott, Alexander; Swami, Ananthram; West, Bruce (December 25, 2017). "The Internet of Battle Things". Computer. 49 (12): 70-75.

[18] Hutchins, E., Cloppert, M., and Amin, R., 2011, Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. International Conference on Information Warfare & Security, 113-125.

[19] Kaber, David B., 2018, A conceptual framework of autonomous and automated agents, Theoretical Issues in Ergonomics Science, 19(4), 406-430.

[20] Kott, Alexander; Swami, Ananthram; West, Bruce, 2017, "The Internet of Battle Things". Computer. 49 (12): 70-75, December 25, 2017.

[21] Lebiere, C., Jentsch, F., and Ososky, S., 2013, Cognitive models of decision-making processes for human-robot interaction. International Conference on Virtual, Augmented and Mixed Reality, 285-294.

[22] Liebermann, Oren, 2021, Lloyd Austin, Defense secretary lays out vision of future in first major speech, CNN Updated 0049 GMT (0849 HKT) May 1, 2021, https://edition.cnn.com/2021/04/30/politics/defense-secretary-lloyd-austin-speech/index.html, accessed on May 1, 2021.

[23] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[24] Mallick, P. K., 2019, Is AI Changing the nature of War?, https://www.vifindia.org/article/2019/january/18/is-artificial-intelligence-changing-the-nature-of-war, accessed on April 2, 2022.

[25] McFadden, C., 2018, A Brief History of Military Robots Including Autonomous Systems, https://interestingengineering.com/a-brief-history-of-military-robots-including-autonomous-systems, accessed on April 2, 2022.

[26] McMillan, Rob, "Definition: Threat Intelligence", Technology Research, May 16, 2013, accessed April 2, 2022.

[27] Parasuraman, R., Sheridan, T.B. and Wickens, C.D., 2000, A model for types and levels of human interaction with automation. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 30(3), 286-297.

[28] Paul, Celeste Lyn, Leslie Blaha, Nathan Bos, Robert S. Gutzwiller, 2019, Opportunities and Challenges for Human-Machine Teaming in Cybersecurity Operations, Proceedings of the Human Factors and Ergonomics Society 2019 Annual, available at:

https://www.researchgate.net/publication/334836878_Opportunities_and_Challenges_for_Human-Machine_Teaming_in_Cybersecurity_Operations, accessed on April 1, 2022.

[29] Paul, C. L., 2014, Human-centered study of a Network Operations Center: Experience report and lessons learned. ACM CCS Workshop on Security Information Workers, 39-42.

[30] Pégulu, Marc, 2021, How the Internet of Things is Shifting the Digital Age, https://www.rtinsights.com/how-the-internet-of-things-is-shifting-the-digital-age/, accessed on April 2, 2022.

[31] Pirolli, P. and Card, S., 1999, Information foraging, Psychological Review, 106(4), 643-6.

[32] Ryan, Mick, 2018, Human-Machine Teaming for Future Ground Forces, https://csbaonline.org/research/publications/human-machine-teaming-for-future-ground-forces, accessed on April 2, 2022.

[33] Scerbo, M. W., 1996, Theoretical perspectives on adaptive automation. In R. Parasuraman & M. Mouloua (Eds.), Automation and Human Performance: Theory and Applications. Mahwah, NJ: Erlbaum, 37-63.

[34] Sheridan, T. B., 2017, Comments on "Issues in human-automation interaction modeling: Presumptive aspects of frameworks of types and levels of automation" by David B. Kaber. Journal of Cognitive Engineering and Decision Making, 12(1), 25-28.

[35] Strauch, B., 2017, Ironies of automation: Still unresolved after all these years. IEEE Transactions on Human-Machine Systems, 48(5), 419-433.

[36] CRS Report R45178, Artificial Intelligence and National Security, by Daniel S. Hoadley and Nathan J. Lucas and Peter Singer; "Getting to Grips with Military Robots," The Economist, January 25, 2018; and Aaron Mehta, "AI Makes Mattis Question Fundamental Beliefs About War," C4ISRnet.com, February 17, 2018.

[37] Gartner Top Strategic Technology Trends for 2021, https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for- 2021/.

[38] Gartner Identifies the Top 10 Strategic Technology Trends for 2020, https://www.gartner.com/en/newsroom/press-releases/2019-10-21-gartner-identifies-the-top-10-strategic-technology-trends-for-2020).

[39] Gartner Says AI Augmentation Will Create $2.9 Trillion of Business Value in 2021, https://www.gartner.com/newsroom/press-releases/2019-08-05-gartner-says-ai-augmentation-will-create-2point9-trillion-of-business-value-in-2021.

[40] Kaseya® is the leading provider of IT and security management solutions for managed service providers (MSPs) and small to medium sized businesses (SMBs), www.kaseya.com.

[41] Gartner Top Strategic Technology Trends for 2021, https://youtu.be/s3rlYWcwdDY.

[42] CTIPs: What is Cyber Threat Intelligence and how is it used? (https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf, accessed on April 2, 2022.

[43] The Recorded Future Team, September 13, 2018, How Strategic Threat Intelligence Informs Better Security Decisions, https://www.recordedfuture.com/strategic-threat-intelligence/.

[44] The Recorded Future Team, September 19, 2018, How Tactical Threat Intelligence Helps Identify the Enemy, https://www.recordedfuture.com/tactical-threat-intelligence/.

[45] The Recorded Future Team, September 25, 2018, How Operational Threat Intelligence Blocks Attacks Before They Happen, https://www.recordedfuture.com/operational-threat-intelligence/.

[46] Artificial Intelligence Market Statistics: 2025, https://www.alliedmarketresearch.com/artificial-intelligence-market.

[47] Ben Dickson, 2020, What is artificial narrow intelligence (Narrow AI)?, https://bdtechtalks.com/2020/04/09/what-is-narrow-artificial-intelligence-ani/#:~:text=Narrow%20AI%20is%20the%20umbrella%20term%20that%20encompasses,that%20falls%20outside%20their%20problem%20space%2C%20they%20fail.

[48] Ministry of Defence (MOD) UK, Global Strategic Trends-Out to 2045 (Shrivenham, UK: Development, Concepts and Doctrine Centre, June 30, 2014).

[49] MOD UK, Future Operating Environment 2035 (Shrivenham, UK: Development, Concepts and Doctrine Centre [DCDC], December 14, 2015).

[50] David T. Miller, Defense 2045: Assessing the Future Security Environment and Implications for Defense Policy Makers (Washington, DC: Center for Strategic and International Studies, November 2015).

[51] Directorate of Future Land Warfare, Future Land Warfare Report (Canberra: Australian Army Headquarters, 2014).

[52] Army General Staff, Future Land Operating Concept 2035: Integrated Land Missions (Wellington, NZ: Headquarters New Zealand Defence Force, 2017).

[53] Vice Chief of Defence Force, Australia, Future Operating Environment 2035 (Canberra: Commonwealth of Australia, 2016).

[54] Canadian Department of National Defence, Designing Canada's Army of Tomorrow: A Land Operations 2021 Publication (Kingston, Canada: Directorate of Land Concepts and Designs, 2011).

[55] Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU., 2017, European Parliamentary Research Service Scientific Foresight Unit (STOA) PE, ISBN 978-92-846-1058-7.

# On Digital Diplomacy. Key Issues

**Mihai SEBE**
European Studies Unit, European Institute of Romania, Bucharest, Romania
mihai.sebe@ier.gov.ro

**Abstract**

*The current paper intends to be a foray into the aspects related to digital diplomacy. It presents the main working definitions and key legislative aspects as well as the Romanian case study, what have we done and what needs to be done.*

**Index terms:** cyber diplomacy, digital diplomacy, digital foreign policy, e-diplomacy, terminology

## 1. Introduction

The impact of technology on our day-to-day activities has been debated thoroughly in the last years. If on the issues related to economy, industry, trade and so on there are a lot of studies and analyses one the impact on politics and general way of doing things in the public sector there are still under-researched areas. One such area is the impact of the technology on diplomacy and the current paper tries to provide a short tentative answer on the current state of affairs.

## 2. Key digital policy issues and terminological clarifications

The last couple of years have witnessed the linguistic expansion of the word „-cyber" or „-e" or „-digital" in various combinations, each of them sometimes more exotic than the other. However, several definitions stand up, each of them being more or less similar in form.

Thus, one first concept used is that of "e-diplomacy" seen as „the use of the web and ICT to help carry out diplomatic objectives" [1]. Another more extensive definition is that provided by Tutt (2013) of the "e-diplomacy" seen as: "the virtual conduct of public diplomacy, using digital information and communications technology (ICT), namely cyber-tools such as Social Media (Twitter, Facebook, Youtube, etc.), in order to communicate and to project a nation' s image into both the national and international public sphere." [2].

As for digital diplomacy, a more generic version is that from the MacMillan Dictionary (2018) „the use of the internet to achieve diplomatic goals" [3]. These definitions refer to the general use of digital tools by diplomats and foreign ministries and not a specific diplomatic policy *per se*.

Another concept that has appeared relates to the diplomacy of cyberspace that is defined as cyber-diplomacy. „Cyber-diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests concerning cyberspace. Such interests are generally identified in national cyberspace or cybersecurity strategies, which often include references to the diplomatic agenda. Predominant issues

on the cyber-diplomacy agenda include cybersecurity, cybercrime, confidence-building, internet freedom and internet governance." [4]

This definition is better suited for the purposes of this section as it relates to the European Union approach as expressly stated in the 2016 EU Global Strategy (EUGS), which expressly describes what it wants through cyber-diplomacy: "The EU will be a forward-looking cyber player, protecting our critical assets and values in the digital world, notably by promoting a free and secure global Internet. We will engage in cyber diplomacy and capacity building with our partners and seek agreements on responsible state behavior in cyberspace based on existing international law. We will support multilateral digital governance and a global cooperation framework on cybersecurity, respecting the free flow of information." [5]

In order to have this cyber capacity and confidence-building with partners, that are key for cyber-diplomacy, we need to have a series of building blocks referred by Lațici [6] from Pawlak's works [7]:

- Developing and building the resilience of institutions able to respond to and recover from cyber threats.
- Securing diplomatic commitments to uphold an open, free, and safe cyberspace.
- Promoting inclusive growth and the sustainable development of digital infrastructure; improving digital markets and securing a safe online economy.
- Developing cyber defence strategies to protect military networks, assets and defence institutions. [6]

Furthermore, OSCE has advanced into this territory of confidence-building measures that help cyber-diplomacy by issuing in 2016 a series of 16 recommendations through its Decision no. 1202 [8]. Cyber diplomacy is perceived at the EU level as a key toward de-escalation of conflicts because "only a long-term cyber diplomacy coordinated at the European level could help to bring about security in Europe and avoid conflict escalation." [9].

## 3. Between tradition and innovation

Given the limited space of this section I would focus briefly on the cyber-partnerships that the EU has. It all starts from what Tikk (2020) sees as the fundamental "European conviction that states' actions in cyberspace as in any other domain, must be guided and governed by international law" [10]. For that purpose special attention is given to the development of the cyber aspects related to the EU partners. As such many of the EU strategic partnerships have developed also a cyber-dialogue component that, according to Renard (2018), varies depending on the countries in question. "(…) the EU's cyber partnerships aim not only for bilateral cooperation but also for 'reflexive' results (whereby the EU aim to develop its cyber and diplomatic agency) and 'structural' results (whereby bilateral partnerships aim to strengthen the multilateral fabric and global internet governance)" [11].

A similar topic was discussed with the African Union and is mentioned in the February 2020 Joint Communique: "They also stressed the critical role of cybersecurity and trust in the digital age and agreed to focus on and enhance capacity in privacy and data protection." [12]. A similar topic was mentioned in the August 2019 ASEAN-EU Statement on Cybersecurity Cooperation who "underscore our commitment to promote an open, secure, stable, accessible and peaceful information and communication technology (ICT) environment, consistent with applicable international and domestic laws. We intend to strengthen our cooperation on cyber issues." [13].

One still complicated issue is the future cyber cooperation with the United Kingdom following Brexit. Although UK is one of the top countries in the world as regards the issues of cybersecurity

there are still aspects that are unclear. However, one important positive aspect is that the 2020 Political declaration setting out the framework for the future relationship between the European Union and the United Kingdom mentioned the need for a strong dialogue in this area. "The United Kingdom and the Union will establish a cyber dialogue to promote cooperation and identify opportunities for future cooperation as new threats, opportunities and partnerships emerge" [14]

## 4. Developing an active cyber diplomacy and a digital foreign policy. Case studies

At the EU level, one document that stands apart is the 2015 Council Conclusions on Cyber Diplomacy which stipulates that the EU and the Member States should have a "coherent international cyberspace policy that promotes EU political, economic and strategic interests and continue to engage with key international partners and organizations as well as with civil society and the private sector" [15]. The document then goes on and provides a series of key recommendations that should be implemented by the Member States.

This would be further supplemented in October 2017 by a series of implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities. These guidelines can be divided in:

- Preventive measures: Cyber confidence and capacity building abroad, awareness-raising activities of EU cyber policies.
- Cooperative measures: Political and thematic dialogues or EU diplomatic démarches.
- Stability measures: Official statements by EU leadership, Council conclusions, diplomatic engagements in international forums and démarches.
- Restrictive measures (sanctions): Travel bans, arms embargos, freezing of assets [16].

EU support for Member States' lawful responses should they fall victim to a cyber act: including in the case of invoking the EU's mutual assistance clause, Article 42 (7) TEU and the solidarity clause, Article 222 TFEU. NATO Allies can also invoke Article 5 [6].

As regards Romania we need to use the same distinction from the beginning of the section. For the "e-diplomacy" aspects we need to mention a series of projects in the consular area that envisaged to create an integrated digital system of travel documents management (E-PASS), an electronic portal for obtaining visas (E-VIZA), a travel app of the MFA and so on. [17] [18]

Concerning the proper cyber-diplomacy actions, Romania has been a constant supporter of all of the EU measures taken in area related to cyber-security or cyber-diplomacy and has been in line with the EU decisions. The active involvement of Romania was duly noticed by the other Member States and in December 2020 Bucharest was chosen to host the European Cybersecurity Competence Center, described as "a future hub to distribute EU and national funding for cybersecurity research projects across the bloc" [19].

The Romanian MFA is in charge of the cyber diplomacy and coordinates from the political level the issues related to cybersecurity [20]. Also, it is active at the UN, NATO and OSCE level on issues linked to the cyber domain [21].

One of the most recent diplomatic interventions of Romania in cyber affairs is the April 2021 statement of support toward the United States in condemning the cyber-attacks on SolarWinds Orion platform, which also reaffirms Romania's position on regulating the cyberspace: "The Romanian MFA reaffirms its commitment to continue cooperating at international level in order to prevent such disrupting activities, by promoting an international framework for responsible state behavior in the cyberspace, based on the implementation of international law." [22].

This was followed months later by a new statement condemning the malicious cyber activities against Microsoft Exchange Server and the cyber campaign conducted by APT40 Group. It once more reiterates the Romanian principles regarding cyberspace: "Romania expresses its concern regarding any form of hostility and irresponsible behavior in cyberspace. Romania also reaffirms its firm commitment and involvement in supporting European and international enhanced efforts to prevent, discourage, deter and respond to such destabilizing actions, in accordance with the international framework for responsible state behavior in cyberspace, based on the application of international law.

Promoting and protecting the global, open, free, stable and secure cyberspace as well as the protection of intellectual property represents a major objective in sustaining the economic, society and security development at the international level, with respect for democratic values and rules-based order." [23].

A special mention should be given to the first Romanian Presidency of the Council of the European Union (1 January - 30 June 2019) where we can mention that "thanks to RO PRES, the Council of the EU set up a framework that would allow for the first time the EU to impose sanctions on individuals or entities responsible for cyber-attacks" [24].

Later on these initial ideas and initiatives took a new life as they were synthetized and given an official form in the new Romania's Cybernetic Security Strategy 2022 – 2027. In order to consolidate Romania's role worldwide, Romania want to have a worldwide engagement toward "promoting the notion of a global, open, stable and secure cyberspace, where human rights, fundamental freedoms and the rule of law are fully applied." Moreover this document provides a first, official definition of what cyber-diplomacy is: "diplomatic action aimed at promoting, supporting, defending and protecting, through international dialogue and cooperation with partner countries and international organizations, a global, open, free, stable and secure cyberspace, in which human rights, fundamental freedoms and the state fully applies to social welfare, economic growth, prosperity and the integrity of a free and democratic society and contributes to conflict prevention, mitigation of cyber security threats and greater stability in international relations". This ambitious plan in the area of cyber-diplomacy meant to consolidate Romania's standing in the international digital arena will imply for 2023 the creation of a high level diplomatic representation position [25].

## 5. Conclusion

In the end of this preliminary expose on cyber-diplomacy one thing is clear - the cyberspace has become a major part of the international relations and the majority of states have adopted cyber strategies and dedicated resources and staff to pursue their objectives in the cyber space. Cyber-diplomacy is only going to get more and more present in the day-to-day diplomatic activity as a cyber-international society is building up. What makes it so special is that it is a sector in a permanent construction as the technical realities and the day-to-day social dynamics are on a constant move.

Cyber-diplomacy role should be to strive to build confidence between the actors in the cyber space from an aggressive, strategic lead action toward a more peaceful co-existence defined by rules and norms: "in practical terms, at the moment the cyber-world still needs work to ensure adherence to international law and norms of responsible behavior - otherwise it's pure anarchy" [4].

In this author opinion, given the above mentioned information, we are now going beyond seeing the cyber-diplomacy as just a theoretical exercise or as a concept analyzed by academics alone. Cyber-diplomacy is now a day to day reality that goes beyond the sole institutions responsible with the classical diplomacy. It is becoming a collaborative activity that requires a whole-of-society approach and new ways of doing things and of communicating them. In the cyber-area we are all becoming in

a way cyber-citizens / cyber-diplomats responsible of our own actions and promoting a safe space, where the human rights and the liberties of all must be respected. Cyber-diplomacy is no longer a theoretical construct but a daily reality.

## References


[1] Fergus Hanson (March 2012), Revolution @State: The Spread of Ediplomacy, Lowy Institute for International Policy, https://www.brookings.edu/wp-content/uploads/2016/06/03_ediplomacy_hanson.pdf.

[2] Tutt, Alexander (2013). E-Diplomacy Capacities within the EU-27: Small States and Social Media [Master's Thesis]: https://www.grin.com/document/274032.

[3] MacMillan Dictionary (2018). Digidiplomacy: https://www.macmillandictionary.com/dictionary/british/digiplomacy.

[4] Barrinha, André & Thomas Renard (2017) Cyber-diplomacy: the making of an international society in the digital age, Global Affairs, 3:4-5, 353-364, DOI: 10.1080/23340460.2017.1414924.

[5] A Global Strategy for the European Union's Foreign and Security Policy (2016): https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

[6] Lațici, Tania (2020). Understanding the EU's approach to cyber diplomacy and cyber defence. European Parliament: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937EN.pdf .

[7] Pawlak, Patryk (2018). Operational Guidance for the EU's international cooperation on cyber capacity building, European Union Institute for Security Studies: https://op.europa.eu/en/publication-detail/-/publication/508a8d73-a426-11e8-99ee-01aa75ed71a1/language-en/format-PDF/source-117729241.

[8] Decision no. 1202 OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies (2016). OSCE: https://www.osce.org/files/f/documents/d/a/227281.pdf.

[9] Bendiek, Annegret (2018). The EU as a Force for Peace in International Cyber Diplomacy. SWP, Berlin, Germany: https://www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf.

[10] Tikk, Eneken (2020). International Law in Cyberspace: Mind the gap: https://eucyberdirect.eu/content_research/international-law-in-cyberspace-mind-the-gap/.

[11] Renard, Thomas (2018): EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain, European Politics and Society, DOI: 10.1080/2374 5118.2018.1430720.

[12] 10th African Union Commission - European Commission Meeting - Joint Communique (29 February 2020): https://ec.europa.eu/commission/presscorner/detail/en/statement_20_365.

[13] ASEAN-EU Statement on Cybersecurity Cooperation (2019): https://asean.org/storage/2019/08/ASEAN-EU-Statement-on-Cybersecurity-Cooperation-FINAL.pdf.

[14] Political declaration setting out the framework for the future relationship between the European Union and the United Kingdom (2020/C 34/01): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2020.034.01.0001.01.ENG.

[15] Council Conclusions on Cyber Diplomacy (February 2015): https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

[16] Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (2017), https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf.

[17] Ministry of Foreign Affairs of Romania (2021a). Proiecte în domeniul consular [Projects in the consular area]: https://mae.ro/node/29926.

[18] Ministry of Foreign Affairs of Romania (2021b). Proiecte din fonduri europene [Projects from European funds]: https://mae.ro/node/35750.

[19] Cerulus, Laurens, Leonie Cater & Vincent Manancourt (in press) (2020). Bucharest to host new EU cyber research hub. Politico: https://www.politico.eu/article/bucharest-to-host-eus-new-cyber-research-hub/.

[20] Ministry of Foreign Affairs of Romania (2021c). Rolul MAE în domeniul securităţii cibernetice pe plan naţional [The MFA role in the area of cyber security on the national arena]: https://mae.ro/node/28366.

[21] Ministry of Foreign Affairs of Romania (2021d). Problematica securităţii cibernetice în cadrul organizaţiilor internaţionale şi implicarea României ca membru al acestora [The question of cyber security within the framework of the international organizations and Romania's involvement in its capacity as a member]: https://mae.ro/node/28369.

[22] Ministry of Foreign Affairs of Romania (2021e). The Romanian Ministry of Foreign Affairs joins the United States in condemning the cyber-attacks on SolarWinds Orion platform: https://mae.ro/en/node/55404.

[23] Ministry of Foreign Affairs of Romania (2021f). The Romanian Ministry of Foreign Affairs joins the international demarches of condemning the malicious cyber activities against Microsoft Exchange Server and the cyber campaign conducted by APT40 Group: https://mae.ro/node/56228.

[24] The Romanian Presidency of the Council of the European Union. Results, 2019, https://www.romania2019.eu/wp-content/uploads/2017/11/Brosura-200x210-bilant-ENG.pdf.

[25] The Romanian Government, Decision no. 1321 of 30 December 2021 concerning the approval of Romania's Cybernetic Security Strategy for the period 2022 – 2027, and also of the Action Plan for the implementation of Romania's Cybernetic Security Strategy, for the period 2022 – 2027, https://legislatie.just.ro/Public/DetaliiDocumentAfis/250128.

# At the Intersection of Interests and Objectives in Cybersecurity

**Mircea Constantin ȘCHEAU[1], Mihai Daniel LEU[2], Cătălin UDROIU[3]**
[1] Phd, Constanta Maritime University, University of Craiova, Romania
mircea.scheau@cmu-edu.eu, mircea.scheau@edu.ucv.ro
[2] Threat Researcher, Farscope Information Consulting, Romania
daniel.leu2810@gmail.com
[3] Hybrid Cloud Specialist, Stefanini EMEA, Romania
udroiu_catalin@yahoo.com

**Abstract**

*The exponential increase in the advancements registered across all sectors of the information technology field gave a new, ever-expanding dimension to the idea of protesting against national governments by introducing political activism into cyberspace. Despite the apparent noble objectives, there is a thin line between hacking as a form of protest against the established order and cyber-criminal activity that can cause financial or material prejudice against organizations. This aspect outlines several dimensions of hacktivism which will be brought into discussion. Another interesting characteristic in hacktivist psychology is the pursuit of "digital clout" as a way to measure success: the more notorious a group becomes, the more attention it will get from the press alas the more successful it is. Even though it is a clear distinction between financially motivated threat actors and hacktivists, some shifts were observed in the cyber threat spectrum in the very politically charged context of war, with different groups which had a history of financially motivated cybercrime, joining the cyber conflict and engaging in hacktivist campaigns either on the one side or the other.*

**Index terms:** cyber security, involvement, threat landscape

## 1. Introduction

The term "hacktivism" was introduced in the vocabulary back in 1990 by the group "Cult of the Dead Cow" and broadly encompasses hacking as a political act in the alleged fight for free speech and human rights. Even though hacktivism is not a definitive product of the recent years, with hacktivist campaigns being observed since as back as 1989, the exponential rate at which the technological expertise in the information and technology sector expanded arguably expanded the scope of protest movements by introducing the act of civil disobedience in the cyberspace.

The ever-expanding cyber threat landscape that we faced in recent years combined with the scenario in which threat actors can rapidly change the motives behind their campaigns increases the complexity of analysis and thus, a more solidified approach must be brought forward when discussing concepts such as hacktivism.

This paper aims to provide an overview on hacktivism by highlighting several dimensions of the concept as well as by presenting it through the example of one of the most popular hacker collectives in recent years. We will also tackle the issue of financing and bring into the discussion some key points on the problematic operational financing of hacktivist groups.

## 2. Research Method

Francis, J. R. D. [1] identified several ways in which one can be shown original research, and according with those, some of the strongest points outlined by the authors in this paper are:

- Setting down a major piece of new information in writing for the first time.
- Giving a good exposition of another's idea.
- Continuing a previously original piece of work.
- Showing originality in testing somebody else's idea.
- Providing a single original technique, observation, or result in an otherwise unoriginal but competent piece of research.

In this study, the authors brought into the discussion conceptual issues on the multiple facets of hacktivism and presented the complexity of the threat actors that operate in this space through previously documented hacktivist campaigns. This research is a literature review on relevant hacktivism and cyberterrorism literature.

## 3. Concept analysis

Given that we can broadly define hacktivism as the act of using technology as a form of protest in a clash between two opposed views, we could see a strong parallel with the concept of hacking as it was defined in the work of Tim Jordan and Paul Taylor 2004 as “the imaginative re-appropriation of technology’s potential within countercultural and oppositional communities”. [2]

While the goals of financially motivated threat actors are more than often straightforward, having financial gains as the ultimate objective, a more substantiated analysis has to be conducted when trying to fit cyber activity into the specter of hacktivism as it being a broadly defined concept, can encompass several methods and objectives.

FirstLinePractitioners present in an article [3] some interesting dimensions of hacktivism that we think are worth bringing into the discussion. The first dimension is cyberterrorism: How significant should the damage caused by a hacktivist campaign be in order for the national and international authorities to classify it as cyber terrorism? To answer that we need to take note of how national and international bodies define cyberterrorism.

The North Atlantic Treaty Organization (NATO) defines cyberterrorism in Responses to Cyber Terrorism 2008 [4] as "a cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal".

The United States Federal Bureau of Investigation (FBI) defines cyberterrorism [4] as "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by subnational groups or clandestine agents".

Both of these definitions broadly explain cyberterrorism as a cyberattack ultimately motivated by an ideological goal that has the power to profoundly impact society. One can observe the general similarities between the concept of hacktivism and cyberterrorism as both basically revolve around computer hacking fueled sometimes by ideological objectives. The main and most distinctive difference is that hacktivism is generally conducted through non-violent means.

The second dimension of hacktivism that is worth bringing into discussion is cyberwarfare conducted by nation state actors. These threat actors are nation state affiliated and usually conduct their operations with the purpose of either intelligence gathering or disruption, depending on the national interests of the state that is sponsoring them. One good example, in which hacktivist objectives coincidentally (or not) aligned with the interests of a nation state, was the massive cyber-attack carried against Estonian infrastructure in 2007. The attack, which was also referenced by

FirstLinePractitioners in their report [3], was allegedly triggered by Estonia's decision to reallocate the Bronze Soldier of Tallinn monument, and consisted of a massive Distributed Denial of Service (DDoS) attack against the digital infrastructure of Estonia. It is very interesting to mention that a state affiliated youth group called "Nashi" claimed responsibility for this particular motivated cyber-attack.

In order to correctly outline the scope of hacktivism in the cyber threat activity spectrum we have to take into account several key points such as the motivation of the attack, the technical capabilities of the actor executing the attack, the type of goals and objectives set at the beginning of a campaign and, probably one of the most interesting, financing. We propose to discuss the aforementioned aspects in the context of one of the most well-known groups since the emergence of hacktivism as a concept.

## 4. The paradox of decentralization

Hacktivism, according to the general consent at a conceptual level, is viewed as a generally decentralized effort. But is this true entirely? In order to answer this question, we have to take a look at probably the most discussed / analyzed hacktivist movement in recent history.

Anonymous made their first appearance around the year 2003 on the popular image board 4chan. In the following years, the allegedly decentralized group continued to engage in cyber-attacks against several government agencies, government institutions as well as private sector organizations, campaigns through which Anonymous consolidated their identity as an international, leaderless, hacktivist collective. The Japanese cyber security company Trend Micro outlined in a report [5] some of the most notable cyber-attacks claimed by Anonymous affiliated groups in the timeframe 2011-2013 such as the 2011 Operation Tunisia in which Anonymous recruited Tunisian hackers to execute Distributed Denial of Service (DDoS) attacks against government digital infrastructure as part of the Arab Spring protest movement or the 2012 Distributed Denial of Service (DDoS) attack against payment services like Amazon, PayPal, Visa, and Mastercard in connection to the WikiLeaks scandal. Another notable incident recorded in the aforementioned timeframe was the 2011 arguably more sophisticated attack against the American geopolitics company Stratfor in which the attackers allegedly managed to exfiltrate 200 gigabytes worth of data.

Despite the apparent minimal funding and lack of a central command structure, the Anonymous idea was able to unite different hacker groups under a centralized, objective-based framework through which they executed various campaigns. Heather Suzanne Woods, M.A. argued [6] that "Anonymous rhetorically creates a hacktivist identity in order to constitute its audience as a collective, unified social movement". Arguably, the Anonymous collective, even though lacking central leadership, could easily rally multiple hacker groups under a centralized, objective-based, campaign against specific targets.

The aforementioned capability was again demonstrated in the most recent operations, which were initiated in 2022 and incorporated a number of cyberattacks executed by several Anonymous affiliated groups against targets from both private and public sectors. In Anonymous characteristic fashion, these cyber-attacks ranged in terms of their technical sophistication from massive Distributed Denial of Service (DDoS) campaigns aimed at causing disruption of service to the targets such as the attacks against websites considered well defensed, some ministries, state-controlled television networks, to more sophisticated attacks such as the alleged exfiltration of about 28 GB of sensitive documents from a central bank.

While the hacker groups that joined the cyber theater conflict were thoroughly documented by security researchers, perhaps the most interesting aspect was the involvement of high-profile threat actors, previously known for being financially motivated, into hacktivist campaigns, potentially

rallied by the media attention received by the call to cyber retaliation against one state, made by the Anonymous collective.

From a threat research perspective, the apparent swiftness through which threat actors switched their focus from purely financially motivated campaigns towards another motivated hacking should be taken into account when one is to analyze the true motives of a cyber threat actor and the nature of the cyber incident that they caused.

The means through which the actors finance their operations represents another interesting aspect that, while clear to define for common cyber criminals and nation state sponsored hackers, needs a more thorough analysis in case of threat actors that operate in the hacktivist sphere. We will continue to bring into the discussion some key ideas on the means through which hacktivists finance their operations and attack infrastructure.

### 4.1. From recognition to funding

As we already know, in the past there was little or no information about how the hacktivist groups are funded to carry out certain actions.

We may say that this is the first time when on the internet appears clear information about a hacktivist organization that is now funded, indeed, through crowdfunding, for a specific reason. Even if we all know that the main scope of hacktivists it's a motivation made by a cause that can be economical, political or social: from disclosing embarrassing information's about some celebrities or political figures, by warning companies about their inside vulnerabilities, by highlighting human rights, to intercepting and tracking groups whose ideologies they do not agree. Usually, these groups' main purpose is based on an ideological and altruistic motivation, such as freedom of speech or social justice. These groups usually disrupt services as a primary goal in order to bring attention to a political or social cause.

An international war incident triggered a huge increase of crypto donations to resistance groups and has raised over $4M in cryptocurrency since one state intensified its attacks.

As we all know, cryptocurrencies have never fulfilled their main purpose when they were launched as the quotidian currency for buying daily goods, or, at least not until today, even some companies adopted this kind of payment. Moreover, this method of payment, regulation-resistant even today, offers the possibility of sending large amounts of money anywhere in the world, including to a war zone in an anonymous format.

Cryptocurrency payments made to military and hacktivist groups aimed at countering aggression against states that fell victim to outside aggression had a sudden increase, especially in the second half of 2021.

Payments number to those organizations made using crypto coins like Bitcoin, Litecoin, Ether or other types of cryptocurrencies acquired through crowdfunding reached a cumulative value of more than $500.000 last year, compared with 2020, when the value was around 5.000 $ and less still in previous years.

This kind of donations had begun to increase rapidly in the 2$^{nd}$ half of 2021, when many hacktivist groups like Come Back Alive [8] managed to raise around to $200,000, and another group called Ukrainian Cyber Alliance received $100,000 worth of crypto [9] all after crowdfunding campaigns were promoted. Another group known as the Myrotvorets Center raised $237,000 but started to raise again with the actual events.

Activists have utilized these funds to buy goods or products such as: medical supplies, military equipment, or advanced technologies like drone-based reconnaissance, as well as funding the development of a facial recognition application with the main scope to identify mercenaries or spies.

These crowdfunded million dollars is just a small part of the total amount of funds obtained with the scope of defending that was managed to be tracked by cyber specialists, and hacktivism groups had to raise funds through more traditional means. The sudden increase of cryptocurrency

donations around the world demonstrates how borderless, often unregulated crypto payments could fund well-intentioned or less well-intentioned organizations involved in actual or future conflicts.

For most of these kinds of fundraising campaigns, payments through cryptocurrencies can represent a small part of the funds that these type organizations receive from donors. Most of the donations were received through traditional payment methods, such as online payments services or bank wires, says Elliptic, one of the most known companies in the crypto funding investigation field.

However, for cyber specialists, cryptocurrency has made its reputation as a robust and more popular alternative against traditional payments. In some cases, blockchain owners or financial institutions had closed accounts belonging to this kind of organization with the main scope as fundraising campaigns, but similar operation may not be validated also for crypto wallet. Cryptocurrency is also particularly suited to cross-border donations, allowing donors all around the world to sponsor hacktivist or cyberterrorist groups.

### 4.2. Cyber Weaknesses

In a recent report [7], even one of the most powerful states known for its reputation on cyber zone faced significant challenges in cyber operations in 2022, even if it's well known for its capabilities and high operational tempo.

Many of these challenges are not unique, but raise hurdles to further growth of that state's cyber operations. Like other government agencies, security services face challenges recruiting qualified personnel.

Private sector opportunities and rival agencies compete for talent, a problem that can be found all around the world these days. As noted, this often causes security services to outsource operations to civilian and criminal hackers.

Most powerful nation states are implying significant resources and time to achieve strategic cyber advantage to advance their national interests, intelligence-gathering capabilities, and military strength through espionage, disruption and theft.

The security of the services and information about the citizens and partners that the government agencies have is a challenge, the security of these data being paramount and being their responsibility.

Therefore, the importance of this data and essential services is besieged by cyber-attacks on their integrity, being targeted by persevering actors who use sophisticated techniques, but also by cyber criminals who try to earn a little in an easier way and less effort as possible.

It's critical for government networks to both do the basics in terms of cybersecurity and vulnerability management. As the speed of information technology gets more advanced day after day, thread actors and their used method of attack are getting more complex and sophisticated, but, by integrating and implementing up-to-date security policies, governments can more effectively secure their assets

## 5. Results and Discussions

According to a recent report published by Shimon Noam Oren [10], the year 2021 registered a noticeable increase in the complexity of cyber-attacks with an observed 125% increase in all threat types combined. As the cyber threat landscape continues to expand, so does the complexity behind the motivation, capabilities and objectives of the threat actors that operate in cyberspace. Given the aforementioned fact, the analysis efforts have to take into account all these developments when working towards the successful profiling of threat actors and towards their classification as either financially motivated, state sponsored or hacktivists.

While threat actors involved in hacktivist campaigns usually prefer to communicate through popular social media platforms, these last few months brought forward an interesting shift in the behavior of some actors which were previously observed mostly in the cyber underground on

cybercriminal forums or on chat groups hosted on different instant messaging applications. Those aforementioned actors, some of which were previously known to be mostly financially motivated, registered a sudden shift in motivation, getting involved in the ongoing hacktivist campaigns ignited by the current international context.

While we presented an overview on hacktivism and on the most recent shifts in cyber threat actors' motivation, influenced by world events, there are still several key points which need to be further elaborated in separate discussions if we are to further solidify a threat analysis model, such as the collection of huge amounts of data available across several communication channels used by threat actors as well as financing models associated with each type of cyber threat actor.

## 6. Conclusions

Even though, in its most basic form, we can simply define hacktivism as breaking into computer systems for political and social reasons or as a form of civil disobedience against the government, we must take into account the diverse and complex facets of hacktivism when researching groups that operate in this sphere. Aspects such as technical sophistication, campaign objectives as well as financing methods are paramount to the correct profiling of hacktivist cyber threat groups.

This paper also highlights the apparent paradox of decentralization that is mostly predominant in the cyber campaigns executed by the Anonymous hacking collective, which, despite the lack in a centralized form of leadership and command structure, was proven to be able to rally several hacking groups and individuals that operated across multiple sectors of the cyber threat landscape in seemingly well-coordinated, politically motivated campaigns.

## References

[1]. Francis, J. R. D. (1976) Supervision and examination of higher degree students, Bulletin of the University of London, 31: 3-6.
[2]. Hacktivism and Cyberwars: Rebels with a Cause. Tim Jordan and Paul Taylor, 2004.
[3]. "Hacktivism": about the origins, meaning and history of online Activism. FirstLinePractitioners. Available: https://www.firstlinepractitioners.com/hacktivism/.
[4]. Responses to Cyber Terrorism. Centre of Excellence Defence against Terrorism, 2008.
[5]. Hacktivism 101: A Brief History and Timeline of Notable Incidents. Trend Micro, 2015.
[6]. The Rhetorical Construction of Hacktivism: Analyzing the Anonymous Care Package. Heather Suzanne Woods, B.A., 2013.
[7]. Come Back Alive. Available: https://www.comebackalive.in.ua/.
[8]. NGOs turn to bitcoin to browdfund the Fight Against. Available: https://www.reuters.com/technology/crypto-donations-soar-groups-backing-ukraines-government-report-2022-02-08/.
[9]. CRS Report R45415, U.S. Sanctions on Russia, coordinated by Cory Welt; CRS Report R46616, Russian Military Intelligence: Background and Issues for Congress, by Andrew S. Bowen. Available: https://sgp.fas.org/crs/intel/R46616.pdf.
[10]. Cyber Threat Landscape Report 2022: Summary & Predictions. Available: https://www.deepinstinct.com/blog/2022-cyber-threat-landscape-report.

# Security Enhancements for Cloud Applications

**Ana-Maria DINCĂ[1], Sabina-Daniela AXINTE, PhD[2]**
Faculty of Electronics, Telecommunications and Information Technology,
University POLITEHNICA of Bucharest, Romania
[1] ana_maria.dinca@stud.etti.upb.ro
[2] axinte_sabina@yahoo.com

**Abstract**

*This study scrutinizes the cloud applications infrastructure and the associated vulnerabilities that could allow unauthorized access to users' accounts. The research is based on a Fault Tree Analysis that uncovers various security design flaws and their occurrence probabilities. For each undesirable event, a preventive mechanism is suggested and validated by the testing results, decreasing to a minimum the risk exposure of unauthorized access to users' sensitive data.*

**Index terms:** cybersecurity, cloud platform security, security augmentation, security by design

## 1. Context

Lately, cloud computing gained more and more popularity because of its broad spectrum of solutions and convenience, especially in the last couple of years. Since the pandemic started, companies started substituting their hardware equipment with cloud solutions, cutting costs and facilitating access to critical resources for the employees that shifted to remote work [1].

With an increase in cloud usage, the number of cybernetic attacks surged and consequently the number of data breaches has risen, as shown in the annual Verizon Data Breach Investigation Report (DBIR): "the number of data breaches showed a significant jump up from 3,950 confirmed data breaches in the 2020 report to 5,258 in 2021" [2].

According to the DBIR, the causes of data breaches in 2021 were related to a human component in 85% of the incidents, while 61% of breaches involved credentials, 13% implicated ransomware and only 3% of the breaches were built upon vulnerability exploitation [3]. The high percentage of data breaches, facilitated by the human component, can be explained by the rise in social engineering and phishing attacks; according to Cisco's 2021 Cyber Security Threat Trends report [4] phishing attacks can be accounted for 90% of data breaches. Users choosing vulnerable passwords to protect their personal data is another security exposure, induced by the human factor and responsible for inadvertently facilitating cybernetic attacks.

The human component caused a concerningly high percentage of data breaches that were confirmed in 2021, which indicates a need for augmented security training for employees and additional security mechanisms in order to boost the sensitive data protection.

## 2. Pre-requisites

This paper is proposing a research regarding security vulnerabilities that might emerge during the planning or design phases of the software development cycle. The study is conducted on a web application designed and developed as part of the graduation thesis and its intended end-users are the students attending the Faculty of Electronics, Telecommunications and Information Technology and

the faculty members such as teachers, assistants or administrative staff (IT administrators, secretaries). The application's purpose is to provide the schedule for its users for any requested date and to offer support with booking a classroom.

The functional flows were designed to accommodate various information access levels in accordance with different roles and specific permission groups, thus the functionalities differ in perspective between users. The main roles in the application are the following: administrators, teachers and students, each one having less access privileges that the previous ones.

One of the first dissimilarities between the functional flows can be observed during the registration flow, where the teachers and the administrators can begin their account initialization by themselves, but students need to previously be enrolled on the platform by an administrator or a teacher. After enrolling on the platform, the users receive an email that will contains a web address where they can set up their account password.

Once the account is activated and the users can access the application, they can fill in their additional data in order to be able to access their schedule and to find out where the classes take place. They are also able to see how they can get in touch with the faculty members - classroom, office, email address.

Users can also book classrooms for various activities such as an exam preparation or a group study; depending on the user's privileges, if they are a faculty member, they can book lecture halls or regular classrooms whilst students can only book regular classrooms.

Because the accounts created on the platform contain some of the users' personal information, a compromised account can lead to sensitive information exposure and, additionally, could result in material damage for certain scenarios, such as an attacker impersonating a student, booking a classroom and causing material damages; unsensitized fields in the application also represent a vulnerability considering that it can jeopardize the stored data.

In the following sections, the causes that put the users' accounts at risk will be analyzed in order to tighten security validations and to propose adequate solutions to prevent negative scenarios.

## 3. Fault Tree Analysis

Fault Tree Analysis (FTA) is used to compute the probability of an undesirable event, which can be utilized to compute the occurrence probability of an attacker to access users' sensitive data. One needs to determine the direct root causes for the top event and then, for each of the leading causes, to identify the specific triggering events.

For the FTA presented below there have been identified a total of 10 base events that can facilitate an attacker to gain unauthorized access to users' accounts. The first five events are scenarios that involve setting or resetting a user's password, which sends an email to the associated address, that contains an URL from where they can set a new password. This flow becomes vulnerable in case of previously compromised email accounts; the attacker has the possibility of setting the new password before the legitimate user gets the chance to, and therefore the ownership of the platform account will be lost.

The considered basic events and their associated probabilities are the following: user inserting an expired password - 42% [5], accessing an inactive account - 15%, user forgetting current password - 78% [6], consecutive failed login attempts in a short period of time - 30% and new platform account creation - 40%. The first four events are part of the main scenario where the user loses access to his account and sends a reset password request to the IT department, with a probability of 46%; an user enrolling on the platform is the other main scenario with a probability of 40%. Consequently, the combined probability of these scenarios equals to 16% because there is a reduced possibility that an user's email account has been compromised prior to receiving an access-providing email, more specifically, one in four email accounts are considered already compromised.

The following five events are directly related to the probability that the user chose a vulnerable password and their probabilities are the following: weak password - 64% [5], password reused between multiple accounts - 61% [5], password contains username or publicly available data such as name, age, pet's name - 60%, password leaked online after a cybernetic attack - 55% or user was a target of a phishing attack - 33% [7]. The combined probability of these scenarios is equal to 97% - a concerningly high percentage, which strengthens the necessity of protecting platform accounts enforcing strong passwords and implementing resilient and prompt security mechanisms to protect these accounts during an imminent cybernetic attack.

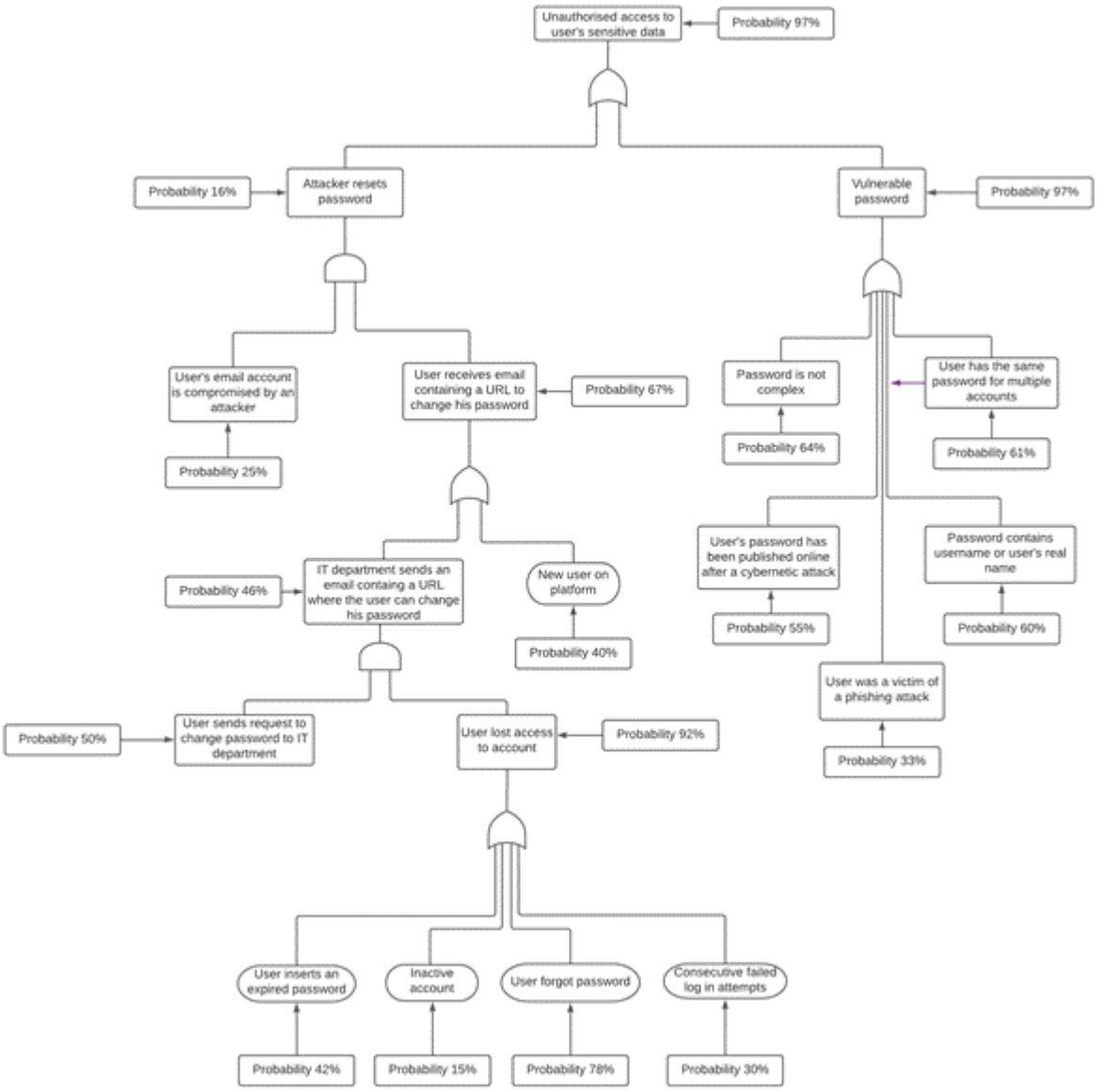



**Fig. 1.** Fault Tree Analysis

After the final computation, the possibility that users' sensitive data can be accessed by an attacker is up to 97%, which makes it imperative to introduce various security measures with the main goal of protecting the accounts created on the platform, their associated personal information, and mitigating the risk of the top event.

## 4. Security augmentation in design phase

Continuous improvement is a compulsory requirement in modern cloud architecture. Consequently, we focus on enhancing User Experience and strengthening security in an effort to keep

end-users both engaged and protected. The FTA previously presented stands as a step towards improving the platform, while the next organic one is proposing solutions for the identified problems.

The first issue to be tackled is the possibility that an attacker, who previously compromised the user's email account, is able to set a new password on behalf of the rightful owner and therefore restrict his access. This scenario can be entirely prevented by using two-factor authentication (2FA), which is an additional step to the traditional authentication: after providing the correct username and password combination, the user is asked to insert an one time password (OTP). An OTP is a fortifying layer of protection in order to secure the platform's accounts, that expires once it is used or after a fixed period a time, usually between five and ten minutes for OTPs sent via text messages, and one minute for OTPs generated using dedicated software applications. Also, if the OTP is sent via a text message and the token sent by the user is not an exact match, then it's invalidated and a new one is generated and sent to the user. However, when the OTP is generated by an application, the verification can be attempted multiple times in the one minute interval, which prompts to a small, but risk-exposing probability of bypassing the security layer.

The proposed implementation of 2FA on the platform relies on imposing phone number ownership verification for each platform account; when the user tries to set a new password, the identity will be confirmed only when the received code matches the one on the server. When several successive incorrect OTPs are being received, the account will be locked for a determined period of time and a warning email will be send to both the user and the IT department, informing that the account has been locked due to suspicious activity.

Another concerning problem identified by the FTA is the vulnerable passwords chosen by the user, given that complex password combinations are easy to forget, and that 53% of people rely on their memory to remember passwords [8]. First vulnerable category are the ones of low complexity that can be easily cracked, such as having less than 8 characters or consisting only of letters or numbers in a predictable order (E.g. "12345" or "qwerty"). The second circumstance is when it contains the username or any other personal information about that user that is publicly available and easy to uncover such as birthdate, spouse name, pet name, graduated college, workplace etc. Last situation when a password is believed to be weak is whether it is encountered on the online resources that contain credentials disclosed during cybernetic attacks [9] or extremely common passwords (E.g. "Password1", "Mypass1234", "Admin123", "Password1234").

The designed solution prevents the user from setting a compromisable password combines the resolutions for each of the described scenarios. At first, the passwords will be constrained to be of eight characters length, having at least one lowercase, at least one uppercase, at least one number and at least one special character. If the password passes this validation, it will be sent to the server in order to verify if it contains any trace of personal information associated to that account. If the password does not include predictable information, it will be compared against a database of stored passwords that were leaked online; the server will compute a percentage to decide how similar the combination chosen by the user is to any entry in the persisted data. If the percentage is smaller than 30%, the password is considered secure and associated with the account, the user is redirected to the home page. Otherwise, the password will not be set and the user will be informed which requirement was not fulfilled, followed by a suggestion based on that reason.

The password database for reference will be updated periodically or in case of major cybernetic attacks. Additionally, on the mentioned events, a script will be run, hashing any new entries and comparing them with the stored user passwords, and if any of them are a match, the associated accounts will be blocked and warning email notifications containing the quarantine justification and the URL for password reset will be sent.

From the user's experience perspective, requiring an OTP on each authentication is considered to be disruptive behaviour. Thus, it was opted for a less intrusive approach in the form of IP comparison between the last known one for that specific user, and the one from the current request.

If not identical, user will be prompted to the next screen to confirm his identity by typing in the OTP sent to the phone number associated to the account. If there will be more than three incorrect attempts from the user, the account will pe locked and emails will be sent to both the user and the IT department with the quarantine reason; the user will also be guided through the necessary steps to change the account password.

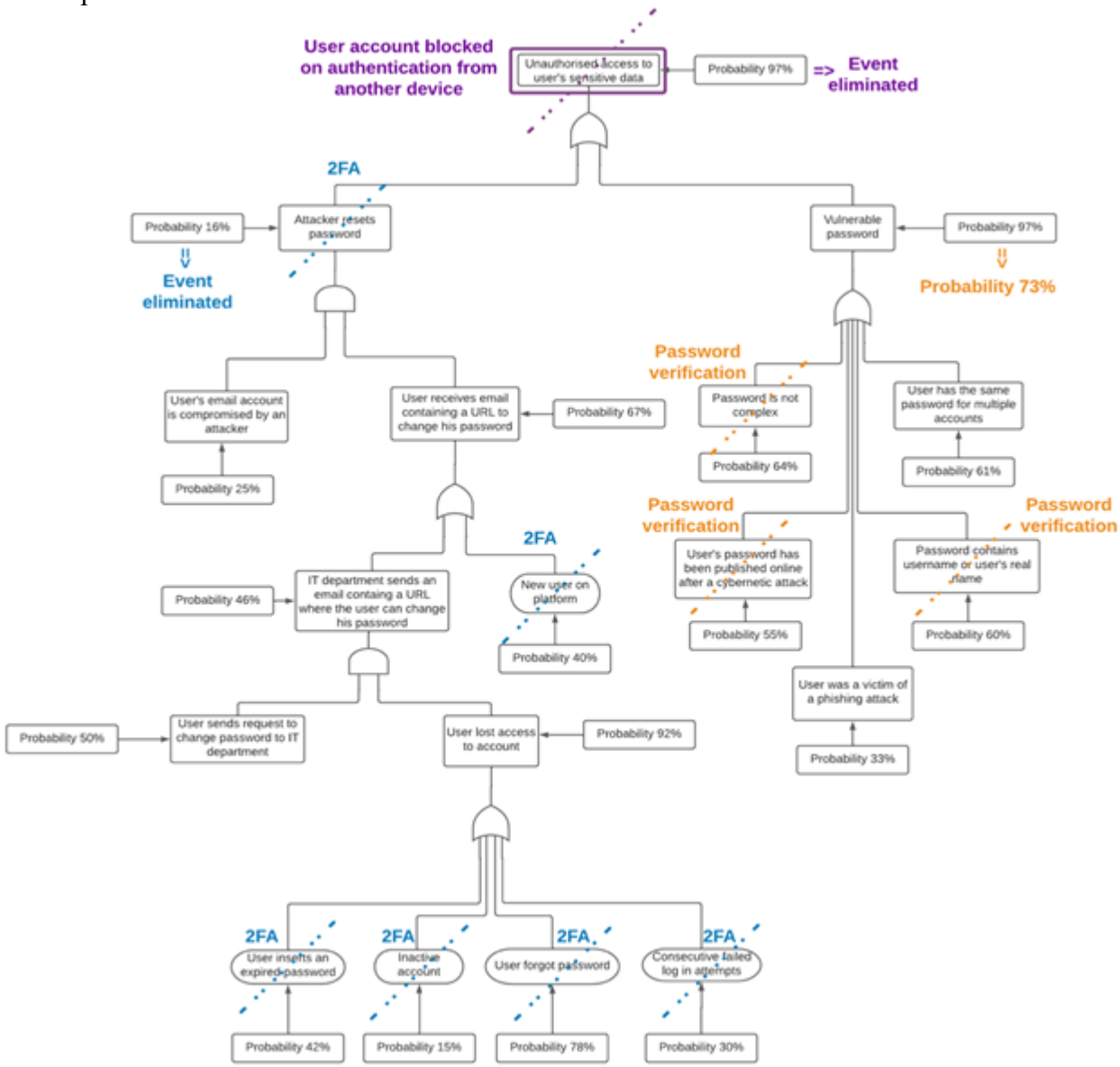



**Fig. 2.** Enhancement results

## 5. Conclusions

In the last couple of years there has been a significant increase in cybernetic attacks, as the COVID-19 pandemic has forced the business digitalization to spread all around the world. This has exposed hidden vulnerabilities in the cloud platform infrastructures and the inadequate investment in cybersecurity awareness training for employees, causing unwarranted "costs to the global economy of about $1 trillion — 50% more than predicted in 2018" [10].

This paper conducted a Fault Tree Analysis on a modern cloud platform and it revealed several design vulnerabilities that could leave users' personal data exposed to cybernetic attacks. The first issue was discovered in one of the most important business flows, set or reset password. The main cause is the large percentage of compromised email accounts and, if the reset password URL sent to such a compromised account, will allow an attacker to set the platform account password prior to the

user. The implemented solution was a 2FA integration, which confirms the user‘s identity. If there is suspicious activity, the account will be blocked and the user and the IT department will be notified, eliminating the possibility of an attacker to take control of a user’s account.

The second problem identified by the FTA was the usage of noncompliant passwords: low-complexity passwords, that are vulnerable on brute force attacks, predictable passwords that contain information that is publicly available or passwords that have been disclosed online during previous cybernetic attacks. The chosen prevention mechanism was to enforce a higher complexity for passwords, to identify any trace of personal data in the provided password and to compare it to a database containing previously leaked passwords. If the password passes all the checks, the user will be logged in and redirected to the home page. Consequently, the passwords protecting the planform accounts will be stronger and the possibility to be cracked is considerably diminished.

The third addressed vulnerably is the user impersonation by an attacker with the correct credentials. To cover this, the current IP address is compared to the last registered one, and if they do not coincide, the user will be asked to introduce a newly sent OTP. By comparing the IP addresses used to log in, the account owner’s identity is verified and suspicious connections are blocked.

Given the growing interest in cybersecurity, the exponential evolution of hacking tools and the free available documentation that facilitate the activity of both ethical and malicious hackers, platforms need to be prepared for cybernetic attacks and to implement preventive fail-safe mechanisms against phishing and social engineering attacks.

## References

[1] S. Mandal, D. A. Khan, "A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic," 2020 Int. Conference on Smart Electronics and Communication (ICOSEC), pp. 837-842, doi 10.1109/ICOSEC49089.2020.9215374, 2020.

[2] J. Carson, "3 Top Takeaways from the 2021 Verizon Data Breach Investigations Report," 29 06 2021. [Online]. Available: https://thycotic.com/company/blog/2021/06/29/verizon-data-breach-investigations-report-top-takeaways/. [Accessed 25.02.2022].

[3] Verizon, "Data Breach Investigations Report," 2021. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2021/. [Accessed 27.02.2022].

[4] C. Umbrella, 2021. [Online]. Available: learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list. [Accessed 27.02.2022].

[5] N. Lord, "Uncovering Password Habits: Are Users’ Password Security Habits Improving? (Infographic)," 2020. [Online]. Available: https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic. [Accessed 23.03.2022].

[6] L. Leuthvilay, "New Password Study by HYPR Finds 78% of People Had to Reset a Password They Forgot in Past 90 Days," 2019. [Online]. Available: https://blog.hypr.com/hypr-password-study-findings. [Accessed 23.03.2022].

[7] J. Lapienytė, "Top 5 industries that fall victim to phishing scams," 28.10.2020. [Online]. Available: https://cybernews.com/security/top-5-industries-that-fall-victim-to-phishing-scams/. [Accessed 23.03.2022].

[8] P.I. LLC, "resources.yubico.com," 2019. [Online]. Available: https://resources.yubico.com/53ZDUYE6/as/q3tmql-974v8g-g8llc3/Ponemon_2019_State_of_Password_and_Authentication_Security_Behaviors_Report.pdf. [Accessed 13.03.2022].

[9] Have I been pwned, https://haveibeenpwned.com. [Online]. [Accessed 01.04.2022].

[10] A. Lukehart, "2022 Cyber Attack Statistics, Data, and Trends," 04.01.2022. [Online]. Available: parachute.cloud/2022-cyber-attack-statistics-data-and-trends/. [Accessed 18.03.2022].

# From the Borderless Digital Chambers to Prison's Four Walls After Committing Personal Data Unlawful Acts

**Larisa-Mădălina MUNTEANU**
Data Protection Lawyer and Deputy Data Protection Officer, JS Information Governance Ltd, Peterborough, the United Kingdom
larisa@js-ig.com

**Abstract**

*This paper represents a concise comparative presentation of how and why can imprisonment be a penalty in different legal systems when committing cybercrimes that affect personal data. Yet, since personal data is closely linked to cybersecurity (especially in cases of non-compliance with regulatory standards), the subject matter herein will focus on the subsequent relationship between personal data and cybercrimes, but from a peculiar perspective - how impactful unlawful acts can be so as to result in criminal convictions. It relies, therefore, on a symbiosis of acknowledging where personal data sits in the cybercrimes' ecosystem and applying this to the most threatening cases identified by global regulators. In this context, the current research is contingent on mirroring the major legal models worldwide, based on which these offences are sanctioned with imprisonment. It is utterly thought-provoking to analyse how the contrasting legal provisions are driven by a common goal: preventing cybercrimes or, as the case may be, minimising their consequences. All these differences have, essentially, homogenous values at a foundational level. Particularly, that foundational level is the research core of this paper.*

**Index terms:** cybercrimes, electronic data, global legal systems, imprisonment, personal data protection

## 1. Introduction

Once upon a time, we used to write essays about how flying cars will be the most innovative development in the world, how robots will efficiently assist humans in daily tasks and how cities will be increasingly computerized. I was myself one of those essay makers. Contrastingly, now I wonder if these ideas and expectations were actually something worth waiting for. Nowadays, we might as well discuss about how life without computers would not be that deplorable.

Having these thoughts as premise, this paper will focus on the emergence of one of the negative consequences stemming from digitalisation - cybercrimes. However, the presentation will be shaped in the context of personal data, as the modern (non?) material assets. In this context, a different facet of cybercrimes will be shaped. This refers to regulatory frameworks implemented by regulators as preventive and corrective mechanisms, focusing on the most serious penalty - imprisonment.

Within the underlying research, it was easily concluded that electronic personal data is exposed to an extremely high risk when discussing cybercrimes. The reasons will be presented in the following sections. Also, this paper will put the basis of an illustrative perspective of personal data cybercrimes, in the light of different international legal systems. The purpose of this study is not to create a comprehensive list of how states around the world decide to 'discipline' individuals that do not comply with data protection laws, but rather to expand on how legislators act when serious unlawful

acts are committed. This is why, there might be cases when it would have been interesting to mention additional legal systems, but, for space and time concerns, limitations were necessary. Nonetheless, I am looking forward to preparing a more extended version of this study in the future.

Moreover, this paper will hopefully put an end to the existing misconception that the data protection laws prescribe only fines (and in secluded cases, warnings). This thesis is plainly wrong for a number of reasons, but the main one is that sometimes, imprisonment is the third possible penalty, as expanded in the following chapters.

## 2. Legal dimensions of cybercrimes

To begin with, it is essential to understand what cybercrimes are, before thoroughly analysing particular hypotheses of identifying them. According to the United Nations Office on Drugs and Crime, 'There is no international definition of cybercrime nor of cyberattacks'. Yet, the typical acts can be classified as it follows: 'i) offences against the confidentiality, integrity and availability of computer data and systems; ii) computer-related offences; iii) content-related offences; iv) offences related to infringements of copyright and related rights' [1]. Given the topic of this paper, the first category is the one of interest.

From a judicial perspective, the Directive on attacks against information systems pinpoints the statutory foundational level, on which it is built: the Convention on Cybercrime of the Council of Europe (the Budapest Convention) [2], labelling it 'the legal framework of reference for combating cybercrime, including attacks against information systems' [3]. Thus, it is worth underlining this Convention, which is also the first international framework with regards to regulating cybercrimes. However, since its preamble explains the underlying necessity of this treaty as to 'deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data', a strong connection with personal data protection emerges. Yet, when discussing personal data safeguarding in the European space, the instrument that will most frequently be put forward and weighed up is the General Data Protection Regulation (hereinafter GDPR) [4].

Nonetheless, these two instruments do closely overlap: the Budapest Convention intends to sanction cybercrimes, whilst the GDPR acts as risk-based approach guidance. At the same time, it was concluded that 'The points of overlap between the Budapest Convention and GDPR is that cybercrime will necessarily be conducted in abusing data in one way or another' [5, p. 70]. Yet, although they both regulate on collecting, disclosing data, the Convention covers more than personal data. Therefore, it is difficult to conclude which of the legal frameworks has more narrow practical applicability: the Convention safeguards computer data and traffic data (including, but not limited to personal data) [2, Ch. 1, Art. 1], whilst the GDPR protects personal data (including, but not limited to electronic data). Furthermore, the EU enforced a more specific instrument, for ensuring privacy and personal data protection are respected exclusively in digital networks: the E-Privacy Directive [6].

Similarly, the Digital Markets Act is expected to be enacted soon, imposing obligations on the core digital platforms in order to respect the GDPR, the E-Privacy Directive, the cybersecurity legislation, along with consumer protection and product safety [7, Art. 7 (1)]. By building the rationale in this way, it became more striking that these puzzle pieces are more than intertwined - they depend on each other for allowing extensive digital protection to online users. Also, the necessity of these instruments is more incontestable than ever, since the data produced digitally is expected to grow spectacularly to 175 zettabytes by 2025 [8]. Correspondingly, 'If cybercrime was a country in this context, it would have been the world's 13th largest economy measured by Gross Domestic Product (…)' [5, p. 64].

However, it is important not to glorify (cyber) security to an excessive as balance is the key. Believing otherwise would just lead to social and regulatory chaos, whilst people might get 'blind' by the obsessive illusion of exhaustively regulating the cyberspace, which is impossible. Eventually, just as Dwight D. Eisenhower stated in 1961, 'We will bankrupt ourselves in the vain search for absolute security' [9]. Although this principle was born from a political context which is inapplicable now, the essence must still be considered: pure and unlimited security is not a realistically achievable goal. Nevertheless, it is important to have flexible regulators that can keep up the pace with perpetrators' strategies and tools, especially in digital realms.

Even if personal data might not be the ending, it might be the means: cybercrimes might not focus on personal data, but rather financial data. However, perpetrators need personal data to gain access to the financial data. Another perspective is that if they have personal data, they can easily make assumptions as for sign-in credentials on relevant platforms.

## 3. Data breaches and other security incidents as cybercrimes

To continue, after understanding the meaning and limits of cybercrimes, the current section intends to expand and apply this foundation. Thus, as a principle, stealing information and unlawfully accessing or using data can easily become a main target for worldwide Criminal Laws. The most frequent such cases illustrate incidents concerning corporate confidential data or financial data. However, since personal data is briefly defined as information [4, Art. 4], how frequent is personal data a threatened actor? Usually, according to the UK Information Commissioner's Office (hereinafter ICO), cyber incidents are caused by human error [10] and can be quite frequent, affecting 'four in ten businesses' [11].

Nonetheless, it was concluded for a while now that when addressing '(…) broad cybercrimes, privacy and data protection become a value to be balanced against prosecuting the crime' [12, p. 68]. Consequently, impersonation is already prohibited by Criminal Laws (especially the frequent cases of using false IDs in order to obtain unfair advantages, even if punished under different names). Then, one may question, what is the difference between using a false ID in order to access the confidential area of a company and using false IDs online, for entering their confidential servers or databases of a company? It seems that more often than not, the offences having a component of personal data are 'taken' online nowadays - and online is very accessible, but also very dangerous. However, since personal data can be both in printed and electronic form, the framework should be a common one, as long as not otherwise mentioned.

On the other hand, unlawful acts concerning personal data are currently covered by data protection laws. That means they are not usually directly perceived as having a connection with the Criminal Law. Nonetheless, Recital 149 of the GDPR allows Member States 'to lay down the rules on criminal penalties for infringements of this Regulation', including with regards to the obligations stemming from enforcement of the GDPR at national level. Also, Art. 84 highlights the main requirement imposed on national legislators - the additional penalties to administrative fines must be 'effective, proportionate and dissuasive'.

In practice, in specific jurisdictions, because of the impactful effects produced, imprisonment was deemed as the suitable penalty. Consequently, a thin line connects the personal data concept with the Criminal Law realms. Even if more and more legal systems choose to 'activate' criminal liability for serious cases of non-compliance in personal data protection, it becomes more interesting to discuss which states included imprisonment as a penalty and in which conditions.

The applications will be discussed in the following section, focusing on the circumstances that can lead to an individual being subject to imprisonment. The chief reasons for this approach depend on the thought-provoking rationale lawmakers used in order to decide in favour of including this sanction in national regulations. The way this mechanism works is more than debatable, blooming on

a dichotomy of minimising the consequences and reshaping the individual: '(…) the aim of imprisonment is to reconstitute the prisoner's spatiotemporal world without causing avoidable collateral damage' and 'cannot be divorced from the characteristics of the societies in which they take root' [13, p. 46].

## 4. Models of global legal systems

Although a connection between imprisonment and data protection non-compliance seems to be a far reality for most readers, the truth is that legal systems do actually fancy this approach. However, the regulations are not homogenously structured worldwide. As a consequence, the following paragraphs will guide the audience towards observing, conceptualising and incorporating the major global models of how imprisonment is chosen as a suitable penalty for the most severe non-compliance acts in personal data protection. The three subchapters suggested below are following a logical order, based on the emphasis regulators placed on the system of penalties, meaning the legal consistency and precision of relevant regulations. Some countries do recognise the necessity of imprisonment as a punitive measure in certain impactful scenarios explicitly in their data protection laws related laws, whilst the others rely on legal interpretation, with varying degrees.

### 4.1. Explicitly included in the national data protection laws

In Germany, some acts referring to personal data might trigger criminal liability, if committed 'deliberately and without authorisation' - for example, transferring data to a third party or making it accessible for commercial purposes could lead to imprisonment up to three years. On the other hand, the intent aspect is altered if the processing is carried out without authorisation or by fraudulent acquiring of data, since imprisonment (up to two years) is an option only if the intent was to obtain payment in return or to enrich oneself or harm someone [14]. In reality, since many online perpetrators do carry out such illicit acts in exchange of money, the practical applicability of this legal provision is indisputable.

Italy is another eloquent example. The Personal Data Protection Code prescribes some cases in which imprisonment is the penalty prescribed by the law, yet the maximum period is 3 years. Should an individual provide false statements or 'submit forged records (…) in a proceeding before the Garante and/or in the course of inquiries' [15, Sect. 168], they might be subject to such conviction. The rationale for this might be the indubitable proof of contempt for the Italy's National Data Protection Authority. However, the minimum imprisonment period that can be set on an offender is 6 months - this is relevant for non-complying with the rules on traffic data, location data or unsolicited communications [15, Sect. 167 (1)]. In this context, it can be easily inferred that traffic data and location data have a special regime in comparison with other types of information. Should this mean the Italian legislator included them in a *de facto special category* that is worth implementing higher levels of data protection? The conclusion lays on a rather gray area. Based on the following paragraph [15, Sect. 167 (2)], it comes to light that disregarding the requirements established for sensitive data [15, Sect. 26] results in a less lenient sanction - imprisonment from 1 to 3 years under the condition that harm is caused. Consequently, traffic data and location data are treated differently (with more strictness) by the Italian Code, but that does not mean they become sensitive data or they supersede the 'privileged' regime of sensitive data.

In South Africa, the Protection of Personal Information Act [16], particular offences might result in imprisonment for up to 10 years. What is even more striking is that fines can be imposed simultaneously. So, whilst other systems apply the 'ne bis in idem' principle prohibiting such outcomes, South Africa explicitly allows the opposite. Nonetheless, it is important to note that the right not to be tried or punished twice is encompassed in the European Convention on Human Rights (ECHR) [17], explaining why South Africa followed a parallel approach. To exemplify, this is the

case if the concerned party 'hinders, obstructs or unlawfully influences the Regulator (…)' [16, Sect. 100] or 'fails to comply with an enforcement notice' [16, Sect. 103 (1)]. It can be concluded once again that cybercriminals might face serious consequences caused by their thoughtlessness in relation with Data Protection Authorities, highlighted by the Italian system as well.

### 4.2. Explicitly included in related laws

Contrastingly, in the United States, the main peculiarity is the inexistence of a unique data protection law. In reality, the US relies on different regulations and levels - both statal and federal. However, the Data Security and Breach Notification Act 2017 holds valuable information supporting this paper. It is prescribed that if security breaches are 'intentionally and willfully' concealed, the individual concerned is subject to a fine or imprisonment up to 5 years, or both, under the condition the damages have an economic nature of at least $1,000 [18].

In other states, personal data protection laws coexist with sector specific laws. In the United Kingdom, the specific laws on personal data protection (Data Protection Act 2018 and UK General Data Protection Regulation) do not establish any legal grounds permitting imprisonment in cases of non-compliance. However, ancillary statutory instruments do - within the Computer Misuse Act 1990, for example. Herein, Sect. 3ZA(6) prescribes that unauthorised acts causing or creating a significant risk or serious material damage can be convicted on indictment 'to imprisonment for a term not exceeding 14 years, or to a fine, or to both'. From a legal perspective, it is at least interesting to discuss how the 'ne bis in idem' principle is practically applied in this case, just as in the South Africa instance. The only reasonable solution would be to impose an administrative fine in addition to imprisonment, otherwise the ECHR's protection would not be relevant - as highlighted in Prina v Romania [19].

Other relevant prohibited criminal act is the unauthorised access with intent to commit or facilitate commission of further offences (s2), clarifying that in the UK system, cybercrimes' preparatory acts are explicitly punished as well. In practice, the Supervisory Authority (ICO), had issued the first prison sentence in 2018, relying on s1 of the Computer Misuse Act 1990, when the concerned individual used a password of someone else in order to access company's records, including personal data, and continued to do so even after working for another company [20]. Subsequently, the second conviction in ICO's history happened in 2021, for unauthorised access and unlawful transfers of personal data [21].

These cases could be referred to as a benchmark for the topic of this paper - they doubtlessly shape how the unlawful obtaining of personal data (prohibited by specific data protection legislation) was practically merged with more technical legislation (countering unauthorised acts and practices against computers). In this context, it becomes crystal clear that personal data assets are one of the most frequent targets when discussing cybercrimes.

On the other hand, the Data Protection Law in France [22] recently amended the Defense Code with regards to processing information about the military status of individuals and established the main sanctions in case of non-complying with the legal requirements set out in these provisions. These can be a fine or up to three years imprisonment, depending on the particular disregarded obligation (e.g. not informing the relevant minister of the processing, allowing access to third parties in prohibited instances etc.). Moreover, the French Criminal Code encompasses other cases in which overlooking personal data protection standards results in punitive effects, countering cybercrimes. In chapter VI, section V, imprisonment is one of the main penalties - e.g. for five years, as an alternative to a € 300,000 fine, if special categories of data are processed without data subject's consent [23, Art. 226-19] or if the collection of data was carried out using 'fraudulent, unfair or unlawful means' [23, Art. 226-18]. Furthermore, cybercriminals that make illicit transfers of personal data outside the European Union might be subject to these penalties too [23, Art. 226-22-1].

Also, Turkey is one of the most exceptional cases in terms of legal structure, from a data protection standpoint. The national Data Protection Law] establishes the main data protection principles, procedures, complaints, cases of administrative fines, but refers to the Criminal Code when it comes to 'crimes' [24, Ch. 5, Art. 17]. Consequently, according to these provisions, the toughest sanction is imprisonment from one to four years for unlawfully delivering, publishing or acquiring data to another person [25, Art. 136], whilst the opposite is imprisonment from six months to one year for failing to destroy data subject to a legal requirement [25, Art. 138]. However, an essentially interesting aspect is to be noted: committing any of these offences with regards to special categories of personal data does not constitute an aggravating circumstance since they follow the same legal regime [25, Art. 135 (2)], but taking advantage of one's position might be. To continue, the imprisonment period is increased by half if in the particular case, the law was broken 'by a public officer or due influence based on public office' or 'by exploiting the advantages of a performed profession and art' [25, Art. 137].

### 4.3. Implicitly included in related laws

In Romania, the National data protection law does not encompass imprisonment as a sanction. This fact is confirmed by the law establishing the Data Protection Authority, which states its powers rely on imposing fines and warnings. However, the Criminal Code [26] might be of interest in this context. In the Special Part, Chapter V of Title VII, called 'Offenses against security and integrity of computer systems and data', imprisonment is the principal penalty to be imposed (yet, in some cases, alternatively with fines). Since the legislator referred in these cases to computer data (in relation with unauthorised access or transfer, illegal interception, alteration etc.), it becomes crucial to acknowledge the exact meaning of this concept. Can personal data be included in computer data? Based on Art. 181 (2) of the General Part, the answer is positive and stands by the literal interpretation, easily applied in this case - shortly, computer data includes any data that can be processed by means of a computer system. In practice, this means that affecting electronic personal data in such circumstances lays the foundation of discussing about cybercrimes.

On the other hand, Art. 302 of the Criminal Code prescribes the cases of violating the privacy of correspondence, briefly defined as the unauthorised opening, stealing, destroying, keeping or revealing of correspondence addressed to another individual. In practice, there are numerous cases in which correspondence contains personal data (let alone that it already includes the contact details of both the sender and receiver) - it might even include photos, which are biometric data, and consequently included in the special categories of personal data. In such cases, it is crucial to understand that the effects, based on the spirit of the GDPR, are much more threatening for the data subject's rights and freedoms. Therefore, to conclude, the Romanian system has no explicit provisions for allowing individuals being sentenced with imprisonment for breaching their data protection obligation. Yet, this might be possible when personal data is structured in an electronic format, and when one of the conditions of one of the above offences are met.

Similarly, Brazil implemented the same system. The National Data Protection Law does not empower the National Authority to sentence individuals to imprisonment for such non-compliance acts, but the Criminal Code might be applied in this case [27]. Exactly as in the Romanian legal framework, the Criminal Code encompasses crimes committed against computer systems and more specific, information systems. One interesting aspect about the Brazilian legislation is that recently, a very specific punishable conduct is the 'fraud committed through social networks, telephone contacts, fraudulent e-mails, or any other similar fraudulent means by using information provided by the victim or by an error caused by a third party', subject to up to eight years of imprisonment and a fine. Aggravating forms include using a server outside of the country or having 'elderly or vulnerable' victims[27, Art. 171].

## 5. Conclusions

All in all, in the 'Era of Seeking for Privacy', personal data has become one of our most valuable assets. It was highlighted within this study that cybercrimes are closely linked to personal data, but this hypothesis remains valid primarily with regards to electronic personal data.

On the other hand, active involvement has been noticed from both private and public bodies, in a global movement towards protecting personal data and combating non-compliance acts and perpetrators. In my opinion, it seems that protecting electronic personal data is gaining more attention than ever.

However, offences were portrayed differently by worldwide regulators, yet discrepancies do depend on socio-cultural, political and even economic values. This resulted in a uniform perspective in some countries, proving the need to legislate on these matters for enforcing punitive and restorative justice. Contrastingly, the way penalties were regulated, structured and imposed was fluctuating. This paper planned to emphasise some of the legal systems around the world, classified from a data protection perspective, with the purpose of delimitating what regulators consider to be 'serious' offences. It can easily be inferred by any individual that although cybercrimes and electronic personal data are cohabitating in borderless realms, penalties are real and impactful.

To conclude, this brief written presentation was not intended to cover each structure legal systems use when sentencing individuals to imprisonment for personal data related cybercrimes, but to extend the reader's perspectives on the severity of this phenomenon. This is not a comprehensive study - it is rather food for thought, addressed to any reader interested in the legal dimensions of cybercrimes when personal data is at stake.

## References

[1]. Global Programme on Cybercrime, UNODC. Accessed Mar. 18, 2022. [Online]. Available: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

[2]. Convention on Cybercrime, opened for signature 23 November 2001, ETS No 185 (entered into force 1 July 2004).

[3]. Directive 2013/40/EU of the European Parliament and of The Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8 Recital 15.

[4]. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[5]. D. Wicki-Birchler, "The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?," Int. Cybersecurity. Law Rev., vol. 1, no. 1-2, Sept 2020, doi: 10.1365/s43439-020-00012-5.

[6]. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.

[7]. Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020) 842 final.

[8]. T. Coughlin, "175 zettabytes by 2025." Forbes.com. https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/?sh=3e648f075459 (Accessed Mar. 21, 2022).

[9]. J. N. Las Vegas, "LETTER: Eisenhower, spending and communism," in Las Vegas Review Journal, Sept. 2021. Accessed Mar. 12, 2022. [Online]. Available: https://www.reviewjournal.com/opinion/letters/letter-eisenhower-spending-and-communism-2438000/.

[10]. Kaspersky, "Human Factor in Corporate Cybersecurity," 2019. Accessed Mar. 28, 2022. [Online]. Available: https://media.kaspersky.com/en/enterprise-security/KL_Human%20factor_main%20threats_datasheet.pdf.

[11]. ICO, "Cyber Security Breaches Survey 2021," 2021. Accessed Mar. 28, 2022. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021.

[12]. M. G. Porcedda, "Data Protection and the Prevention of Cybercrime: The EU as an area of security?." 2012. Distributed by EUI Working Papers LAW 2012/25 [Online]. Available: http://hdl.handle.net/1814/23296.

[13]. I. O'Donnell, "The aims of imprisonment," in Handbook on Prisons, Y. Jewkes, B. Crewe, J. Bennett, Eds., London, U.K.: Routledge, 2016 pp. 39-54.

[14]. Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626), Part 2, Ch. 5. Sect. 42.

[15]. Personal Data Protection Code containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2021.

[16]. Act No. 4 Of 2013, Protection of Personal Information Act (POPIA).

[17]. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR), Protocol no. 7, Art. 4.

[18]. U.S. Senate, 115th Congress, 1st session (2017, Nov. 30). S.2179, Data Security and Breach Notification Act, Sect. 5 § 1041.

[19]. Prina v Romania (2020) ECHR 267.

[20]. J. Clark, S. Qureshi and A. Greaves, "UK: First prison sentence following ICO prosecution." DLA Piper. https://blogs.dlapiper.com/privacymatters/uk-first-prison-sentence-following-ico-prosecution/ (Accessed Mar. 29, 2022).

[21]. F. Fellowes and K. Barnes, "ICO Utilises the Computer Misuse Act to Impose Tougher Penalties for Unauthorised Access to Data." Squire Patton Boggs. https://www.consumerprivacyworld.com/2021/02/ico-utilises-the-computer-misuse-act-to-impose-tougher-penalties-for-unauthorised-access-to-data/ (Accessed Mar. 30, 2022).

[22]. Law n°2018-493 of 20 June 2018, on the protection of personal data.

[23]. French Criminal Code, 2005.

[24]. Law on the Protection of Personal Data No. 6698, 2016.

[25]. Turkish Criminal Code - Law Nr. 5237, 2004.

[26]. Law on the Criminal Code no. 286, 2009.

[27]. Decree-Law nº 2,848 of December 7th, 1940 (Brazilian Criminal Code).

# Healthcare Cybersecurity Vulnerabilities

**Ryan DRAKE[1], Evan RIDDER[2]**
[1] Arizona State University, United States
rdrake6@asu.edu
[2] Kansas State University, United States
eridder@ksu.edu

**Abstract**

*The healthcare industry sector is often considered a soft target for malicious actors. Having a large attack surface coupled with a focus directed toward patient care rather than security, often health organizations haven't taken the necessary precautions to secure patient data or access to medical devices within their infrastructures. As the severity and the associated costs of cyber-attacks on entities within healthcare organizations continue to escalate, an increased effort within this industry to mitigate the risks associated with these vulnerabilities is necessary. This study seeks to present the most common types of healthcare attacks and their mitigation methodologies. Additionally, a discussion of how compliance with the GDPR in the European Union and the HIPPA regulation in the United States can positively affect a healthcare organization's defensive posture.*

**Index terms:** Cybersecurity, GDPR, Healthcare, HIPPA, PHI, Privacy

## 1. Introduction

Beyond providing quality patient care, healthcare organizations must uphold ethical standards which include maintaining the privacy and confidentiality of patient health data [1]. To manage patient care, healthcare organizations process large amounts of sensitive data usually in the form of electronic health records which include patient personal health information (PHI), as well as financial and demographic data. This medical record data is a desirable target for cybercriminals as it is valuable for sale on the black market and it can be used for extortion purposes [2], [3]. Highlighting the extent of this issue, in 2021 over 45 million electronic medical records were stolen from healthcare providers in the United States. exposing sensitive patient personal, medical, and financial information [4].

Cybercriminals frequently attack medical providers due to the perception that the healthcare sector is a soft target [3]. Vulnerabilities in the healthcare sector can be attributed to many factors stemming from limited staffing resources, significant reliance on un-patched legacy systems which are no longer supportable, a large attack surface, and a lack of security awareness by care staff. [2], [3]. The number and complexity of attacks in the healthcare sector have risen over the last several years within the global community. As the severity and the associated costs of cyber-attacks on entities within healthcare organizations continue to escalate, an increased effort within this industry to mitigate the risks associated with these vulnerabilities is necessary [3].

This study seeks to present the most common types of healthcare attacks with mitigation strategies, along with a discussion of the concept of privacy in the context of the European Union's GDPR and the United State's HIPPA regulation.

## 2. Overview

As part of the ethical care of patients, the proper treatment of their personal and health-related data is essential. Privacy within the context of healthcare is associated with the handling of patient personal and healthcare data and is concerned with its collection, storage, processing, and use in a secure manner [1]. With the technological advances in the healthcare industry, patient-related data is recorded primarily in digital form and as such is vulnerable to information leakage due to unprotected information systems or through cyber attacks [2]. Care as to how these records are stored and processed, as well as securing the underlying IT infrastructure are fundamental steps necessary to reduce the risk of patient medical information leakage. However, as medical data is valuable to malicious actors, healthcare organizations provide attractive targets for an attack [3].

### 2.1. Personal Health Data

In the United States, more than 200 million patient records have been compromised since 2010 [4]. Most of these attacks were against electronic health records which contain patient personally identifiable information such as name, birthdate, addresses, and government identification numbers, however additional data such as medications, medical history, or test results can be part of this data [5]. Electronic health data is valuable on the black market as these stolen records usually contain a more complete identity profile beyond financial data. Health records often contain numerous aspects of demographic, financial, and potentially sensitive medical data which is appealing to the attacker since this PHI data can be sold and resold multiple times with stolen records often fetching $20 to $50 per record [5], [6], [7].

### 2.2. European Union - GDPR

The General Data Protection Regulation was enacted in 2018 in European Union (EU) as the main regulation that dictates the methods of how citizens' data is processed both in the EU and within its extraterritorial areas [8]. The GDPR applies to all data processing entities within the EU and as such, healthcare providers are also subject to the GDPR directives. GDPR compliance assists in the maintenance of privacy elements of healthcare data through regulations requiring strict compliance with patient consent rules for the collection, storage, and processing of personal data, eliminating patient consent by default [9]. Additionally, healthcare providers must adhere to the "right to be forgotten", allowing the patient to request their data be permanently deleted upon request. Security mitigations to maintain data security include encryption, the use of administrative, technical and physical controls, pseudonymization, redundancy, and intrusion protection mechanisms [8], [9].

### 2.3. United States - HIPPA

While the GDPR pertains to all business entities within the EU, the Health Insurance Portability and Accountability Act of 1996 (HIPPA) regulations only apply to healthcare providers within the United States. As opposed to the GDPR, HIPPA only applies to health care providers and processers within the United States and does not cover citizens outside of the bounds of the United States [10]. The HIPPA United States federal law protects the privacy of personal health information (PHI), giving rights to an individual regarding their data while imposing processing obligations to healthcare providers and processors. The basic principles of the HIPPA regulation include patient control of the release of their information, with strict boundaries put in place for the use and processing of PHI data. The use and processing of this data is for health purposes only and is not to be marketed or sold. Reasonable measures must be put in place to protect PHI from unauthorized access, disclosure, or use, where records can be either paper copies which must be physically located in locked areas, or electronic data records which must also be secured [6].

Similar to GDPR, healthcare providers within the United States must also comply with strict data security protocols and ensure compliance with the handling and disposal of PHI data. The HIPPA regulations are primarily centered around protecting patient records from a breach, however, HIPPA doesn't address the concept of patient consent to data use as GDPR does. Additionally, HIPPA does not give the consumer the right to data erasure as GDPR does, while both regulations have stringent penalties for organizations that violate the data processing and privacy laws [8], [9], [10].

## 3. Methods

As the healthcare industry remains an attractive target for cybercriminals, the identification of vulnerabilities associated with the healthcare industry and their associated mitigations can assist with the reduction of the risk associated with this industry silo. The methodology for this study included the following steps, identifying appropriate literature, the collection of data, the analysis and evaluation of the literature, followed by the categorization of the selected literature. The key terms "cybersecurity", "healthcare", "vulnerabilities", "GDPR" and "HIPPA" were used to search scholarly electronic databases which included PubMed, ProQuest, and Google Scholar. Additionally, websites associated with the reputable new sites were searched, as well as sites associated with the regulatory entities of GDPR and HIPPA. The literature review generated 57 sources, of which 9 were used as primary sources for evaluation and discussion. Exclusion and inclusion criteria were based upon the content of the abstract, level of research originality and the content of data presented. Broad themes of cyber vulnerabilities associated with healthcare emerged through the analysis and categorization of the reviewed literature which is discussed in Section 4.

## 4. Results

Four primary areas of the attack were identified through the literature review which include ransomware and malware, IT infrastructure, medical devices, and human-based exploitation which will be subsequently discussed.

### 4.1. Ransomware and Malware

Ransomware is a type of malicious software used by attackers to extort money from organizations. During a ransomware attack, the attackers first encrypt the target data to either block access or in some cases, exfiltrate the data. The attackers then message the organization with the monetary demands required to unlock the data [12]. These ransoms are usually paid in cryptocurrencies where the transactions are anonymous and non-reversible [2]. There is considerable debate as to if ransomware should be paid and if so, in what circumstances. Two issues concerning paying the ransomware are the incentivization of bad actors and the lack of guarantee that the attackers will honor their word [13]. Personal health data which has been encrypted by ransomware attackers should be assumed to be compromised, and as such would trigger breach notification obligations from a regulatory perspective [8], [9], [10].

As the most common attack mechanism for cybercriminals, ransomware attacks on the healthcare industry occur on a global scale [4]. The United States accounts for 60% of healthcare provider ransomware attacks followed by France, Brazil, Thailand, Australia, and Italy. Although these countries are the primary targets, other countries in the EU such as Germany and Romania have also had healthcare organizations such as hospitals, pharmacies, and medical centers attacked [11]. Some common malware associated with the ransomware attacks on healthcare entities includes Ryuk, DoppelPayer, LockBit, Hive, Maoloa, Phobos, WannaCry, Conti, Pysa, AstroLocker, Ragnarok, Vice Society, Groove, and CLoP [3], [4], [16], [11], [13].

### 4.2. IT Infrastructure Attacks

Large, complex data processing systems are required to manage healthcare ecosystems, and with that comes a large attack surface. Vulnerabilities in infrastructure elements such as firewalls, server applications, cloud storage, and processes can provide a means of attack to produce harm or exfiltrate sensitive data [6], [14]. As consumers interact with their health care providers over mobile and computer applications, ensuring web applications are hardened against attacks such as SQL injections or cross-site scripting is equally important [15]. Often infrastructure attacks provide the initial entry point for privilege escalation and subsequent takeover of systems to perform data exfiltration or for ransomware attackers [7].

Other attacks methods leverage vulnerabilities within the applications used by the medical staff such as the medical imaging and picture archiving and communications systems (PACS) used by the radiologists to evaluate various types of medical images obtained through patient CAT scans, MRIs, or ultrasound procedures [15]. Transmission of the images is done usually via DICOM, Digital Imaging, and Communications in Medicine which by default transmits messages in unprotected clear text that can be viewed through readily available packet analyzers such as WireShark [16]. Beyond obtaining the digital images, source and destination information used to further infiltrate the network can be obtained as well as sensitive patient healthcare information. Additionally, Health Level 7 (HL7) is set international standards which are used to promote the interconnectivity of medical devices from different vendors. Although HL7 version 3 is recommended level for use, many healthcare organizations are still using HL7 versions 1 and 2, which also by default transmit healthcare images, patient data, and network communications information in clear text by default which can lead to data leakage [15], [16].

### 4.3. Medical Device Vulnerabilities

As technology continues to be applied to the healthcare field, new medical devices which are both implanted, or wearable are becoming more available to a wider patient base. The ability to remotely monitor medical devices such as heart pacemakers or insulin pumps can potentially reduce the number of office visits while giving the patient greater control over their condition through the ability to better understand how their body is working [3]. Although these devices can provide improved patient care, their use does come with risks to their vulnerability to cyber-attack. Security vulnerabilities have been detected in implanted infusion pumps, cardiac pacemakers, and defibrillators, as well as the software used to access these types of devices. Frequently these devices were engineered and designed with the consideration of potential cyber-attack and often relied more on “security through obscurity” of proprietary protocols rather than a hardened attack surface [2]. The prevalent vulnerabilities include inadequate authentication mechanisms and access controls, with weak audit mechanisms. As many of these devices are similar to IoT there is frequently little storage with limited computational power and battery life. Attacks on medical devices can actively cause harm to patients by causing a malfunction of the device or through malicious device inputs or tampering with the device outputs. Attacks can also take place in the form of privacy loss due to data leakage of sensitive information [3], [7].

Beyond implantable devices, medical wearables also provide patients an ability to interact more directly with their health by allowing the continuous monitoring and recording of biometric data via the device sensors. These wearable devices can be compromised by pairing them between smartphone devices and virtual assistants [2.], [3]. As the FDA in the United States does not regulate smart devices used for medical purposes, the development of devices and apps are not subject to any restrictions which often can lead to serious privacy and safety issues [11]. Similarly, the European Union Medical Device Regulation (MDR) enacted in 2021 can view some types of wearables as borderline products where there is uncertainty over which regulatory framework applies [17].

### 4.4. Human-Based Exploitations

It is generally recognized that the human element presents the greatest threat to any organization either from malicious endeavors or through mistakes in configuration, lapses in security controls, or the unintentional introduction of malware through phishing campaigns [2], [5], [18]. The electronic data record is the chief target for malicious actors, who look for vulnerabilities within the systems used within the healthcare industry and its IT infrastructure or for exploitable human contacts contacted [6].

Security misconfigurations such as default passwords, improper configuration of firewalls, and server security or unsecured cloud databases provide an easy method for attackers to breach sensitive systems [3], [18]. With the plethora of available free vulnerability and penetration testing tools available, hackers can easily crawl through systems looking for open ports, default password configurations, or well-known vulnerabilities to exploit [2], [7].

Phishing uses targeted communications such as messaging or email to entice victims to either open an infected file or click on a malicious link to download malware. Phishing relies upon social engineering tactics to elicit a response from the victim to comply with the request, with the request often appearing to be from a trusted source such as the CDC, healthcare administrator, or IT staff [5], [18]. Once the file is downloaded or the malware installed from the malicious site, attackers can then continue their lateral movement and privilege escalation through the various systems to gain further footholds, leading to the exfiltration or encryption of that data to be used as ransom [13].

## 5. Discussion

Although an attack on medical devices themselves represents a way to directly impact patient care, the primary target for large-scale attacks is electronic data records that contain personal health information [4], [6], [11]. This data is attractive to the black market due to its longevity and multi-faceted nature which includes personal contact information such as addresses, government identification numbers, and financial records as well as medical information [6]. The securing of this information is an essential component of maintaining patient privacy and confidentiality. The application of compliance controls that are aligned with the GDPR and HIPPA regulations, coupled with the implementation of vulnerability mitigation strategies can enhance security protection efforts for healthcare providers.

### 5.1. Compliance

Regulatory compliance with the GDPR and HIPPA regulatory bodies provides a framework for healthcare organizations to apply security-based technical, administrative, and physical controls to provide security functions [19]. As part of the compliance process, healthcare providers must provide proof of the security controls they have in place, how they are operating, and depending upon the size of the organization an external verification must be done by a certified auditing company. Since there are strict fines for non-compliance to these security standards or if a breach occurs when basic security standards were not met, healthcare providers in both the United States and European Union countries are highly motivated to comply with the security requirements [8], [9], [10].

### 5.2. Mitigations

To mitigate the risks of unauthorized data disclosure or the tampering of devices, healthcare organizations must assume a zero-trust model for all systems and processes, with an assumption that their IT infrastructure could already be compromised. [20]. The central principle of zero-trust is that no device or network traffic should be considered trusted by default and with that, all traffic should be encrypted and subject to continuous monitoring to ensure the protection of data [21]. Beyond zero-trust enabling general cyber hygiene practices and security controls assists in protecting digital assets.

Industry-recommended cyber hygiene practices involve securing communications, protecting data, controlling access, proper authentication practices, ensuring patching is current, security training, and the implementation of security controls and data backups.[3], [5], [6], [7], [13], [14], [20], [21].

The securing of the communication system should be viewed from both an external and internal perspective. Externally the use of firewalls based upon the topology and use case is essential, coupled with the proper network architecture allowing for the segmentation of devices behind DMZs to help reduce the change of lateral movement of an attacker if a breach occurs. The use of intrusion detection systems (IDS) and intrusion protection systems (IPS) are also key to identifying possible attacks on the system [21]. Within the healthcare environment, data must be protected when in use, at rest, and in transit, and as such should be encrypted unless it is actively being processed [3], [6]. Storage systems, especially those on the cloud need to be encrypted and have access protections put in place [2]. Controls regarding access should be in place for both physical and data access, with strong authentication and authorization processes adhered to. It is crucial to maintain patch levels on all physical devices and software, as well as to be informed on emerging zero-day vulnerabilities such as Log.4 which could impact an organization's security posture.[21]. Staff training and mock drills help reduce the likelihood of unintentional internal security breaches through education regarding phishing and malware [5], [18].

Administrative security controls include enforcing least privilege where people are allowed access to only areas where they must have access to and no more, segregation of duties so that no one person can have unlimited access to a system, role, and rules-based access which allows for categorization of access privileges according to access requirements. Multi-factor authorization (MFA) should always be used if possible to help reduce the risk of stolen credentials being for system access [21]. Additionally, the strict management of any access or service account must be done. Beyond access control, the development of incident response plans is a central feature of the management of a data breach or cyber-attack, which should also include steps for disaster recovery if necessary. Backups should be monitored and periodically tested to ensure the ability to restore at set recovery objectives [2]. Detective security controls such as log collection and analysis vis SIEM systems are crucial elements to detect access attempts or potential breaches. Logs of servers, firewalls, gateways, and other communications must be monitored as well as the on the IDS and IPS devices. The scanning of emails and the use of data loss prevention technology should be used to assist in stopping scam emails before they reach the victim and data loss prevention software to stop the transmission of data that should not be shared [5]. Physical security controls should be put in place to ensure adequate protection of the data center and physical record access to only those who are authorized to do so [7]. Technical controls should include a wireless access policy that ensures that non-public access points are secured with WAP3 if possible [21]. Additionally, the use of anti-virus malware protection software should be mandatory for all end-user workstations and servers [20].

## 6. Conclusion

Traditionally, the healthcare sector has provided a soft target for malicious actors due to its broad attack surface and organizational priorities directed toward patient care rather than cyber security issues. Four general areas of cyber vulnerabilities were identified for the healthcare sector which included ransomware and malware, IT infrastructure attacks, medical device vulnerabilities, and human-based exploitations. These areas of attack can frequently be interrelated with attacks in one area leading to attacks in another, such as an attack on the IT infrastructure or a phishing scam that could lead to the installation of ransomware. The exfiltration of the electronic health data record is often the primary goal of attackers due to its value on the back market, while ransomware operators also often target healthcare providers. The GDPR and the HIPPA regulatory frameworks stipulate

security standards for securing patient data and leverage high fines for breaches due to non-compliance with their directives. Healthcare providers need to ensure that cybersecurity mitigations are followed to reduce the ability of malicious actors to cause harm within their organizations.

**References**


[1]. J. Mold, "Goal-Directed health care: Redefining health and health care in the era of value-based care," Cureus, vol. 9, no. 2, Feb. 2017, doi: 10.7759/cureus.1043.

[2]. S. Nifakos et al., "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review," Sensors, vol. 21, no. 15, p. 5119, Jul. 2021, doi: 10.3390/s21155119.

[3]. F. Luh and Y. Yen, "Cybersecurity in Science and Medicine: Threats and Challenges," Trends in Biotechnology, Mar. 2020, doi: 10.1016/j.tibtech.2020.02.010.

[4]. December 2021 Healthcare Data Breach Report, HIPAA Journal, Jan. 18, 2022. https://www.hipaajournal.com/december-2021-healthcare-data-breach-report/.

[5]. W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire, "Phishing in healthcare organisations: threats, mitigation and approaches," BMJ Health & Care Informatics, vol. 26, no. 1, p. e100031, Sep. 2019, doi: 10.1136/bmjhci-2019-100031.

[6]. Conaty-Buck, S. (2017). Cybersecurity and healthcare records. Am Nurse Today, 12(9).

[7]. N. O'brien, G. Martin, M. Durkin, and S. Ghafur, "SAFEGUARDING OUR HEALTHCARE SYSTEMS A GLOBAL FRAMEWORK FOR CYBERSECURITY."

[8]. EU's General Data Protection Regulation Set to Disrupt the Medical Industry," www.healthitoutcomes.com.

[9]. "Who does the data protection law apply to?," European Commission, 2021. https://ec.europa.eu/info/law/law-topic/data-protection/.

[10]. O. for C. Rights (OCR), "Summary of the HIPAA Privacy Rule," HHS.gov, May 07, 2008. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[11]. K. Jercich, "The biggest healthcare data breaches of 2021," Healthcare IT News, Nov. 2021. https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021

[12]. A. H. Seh et al., "Healthcare Data Breaches: Insights and Implications," Healthcare, vol. 8, no. 2, p. 133, May 2020, doi: 10.3390/healthcare8020133.

[13]. L. Fernández Maimó, A. Huertas Celdrán, Á. Perales Gómez, F. García Clemente, J. Weimer, and I. Lee, "Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments," Sensors, vol. 19, no. 5, p. 1114, Mar. 2019.

[14]. G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: how safe are we?," BMJ, vol. 358, p. j3179, Jul. 2017, doi: 10.1136/bmj.j3179.

[15]. OWASP, "OWASP Top 10:2021," owasp.org, 2021. https://owasp.org/Top10/.

[16]. M. Eichelberg, K. Kleber, and M. Kämmerer, "Cybersecurity in PACS and Medical Imaging: an Overview," Journal of Digital Imaging, vol. 33, no. 6, pp. 1527-1542, Oct. 2020, doi: 10.1007/s10278-020-00393-3.

[17]. J. Gillum, J. Kao and J. Larson, "Millions of Americans' medical images and data are available on the internet. Anyone can take a peek," ProRepublica report, 2019, Online: https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet.

[18]. EMA, "Medical devices - European Medicines Agency," European Medicines Agency, Nov. 26, 2018. https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices#borderline-products-section (accessed Apr. 06, 2022).

[19]. S. Venkatesha, K. R. Reddy, and B. R. Chandavarkar, "Social Engineering Attacks During the COVID-19 Pandemic," SN Computer Science, vol. 2, no. 2, Feb. 2021.

[20]. A. Marotta and S. E. Madnick, "Analyzing the Interplay Between Regulatory Compliance and Cybersecurity (Revised)," SSRN Electronic Journal, 2020, doi: 10.2139.

[21]. S. T. Argaw et al., "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks," BMC Medical Informatics and Decision Making, vol. 20, no. 1, Jul. 2020, doi: 10.1186/s12911-020-01161-7.

[22]. D. Tyler and T. Viana, "Trust No One? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture," Applied Sciences, vol. 11, no. 16, p. 7499, Aug. 2021, doi: 10.3390/app11167499.

# Integrating and Shaping Military Cyber Defence in Operational and Intelligence Planning

**Joseph JONES**
Founder, OS2INT, Skive, Denmark
joseph.jones@os2int.com

**Abstract**

*The cyber threat landscape has undoubtedly evolved at an exponential rate. As such, NATO and EU forces have transformed their capabilities to meet present-day operational challenges in cyberspace. However, this paper will not only identify relative successes by NATO and EU forces with regards to their respective development of cyber defence capabilities, it will also indicate limitations with regards to the projection of power within cyberspace and the lack of national and international coordination concerning offensive cyber operations and the collection of intelligence from cyberspace.*

**Index terms:** cyber capacity building, cyber defence, cyber intelligence, military cyber operation

## 1. Introduction

This chapter will discuss how the present-day cyber threat landscape has significantly evolved to an extent where cyberspace is now considered a fourth operational arena for military forces. By analysing how competing militaries have transformed their capabilities and exercised unrestrained information maneuver in cyberspace, this article will point out inadequacies within NATO and the EU's unified approach towards hostile cyber threats, namely because of a lack of coordination and interoperability with regards to Offensive Cyber Operations and intelligence-gathering. In conclusion, this article will point out that competing military forces continue to re-shape and refine their mode of operations within cyberspace, NATO and EU military forces will remain restricted in their capability to disrupt hostile cyber threats and deny such threats with the ability to maneuver within cyberspace. Furthermore, the article will recommend greater interoperability between NATO and EU members across all operational spectrums including Offensive Cyber Operations and intelligence-gathering.

## 2. The Future-Force Concept of Operations in Cyberspace

Not only do state-aligned cyber threats continue to evolve, yet increase in terms of their overall lethality, hostile militaries are widely known to have taken effective steps to integrate military offensive and defensive capabilities across the entire spectrum of military and intelligence capabilities, from tactical-level military formations to strategic-level military intelligence agencies. In light of the rapidly evolving threat, western militaries have a clear requirement to adapt to this rapidly evolving threat by transforming their own military structures and implementing required cyber capabilities.

The UK Ministry of Defence [1] defines cyber operations as the "planning and synchronizations of activities in, and through, cyberspace to enable freedom of maneuver and to achieve military objectives". When clearly defining the categories - or roles - of cyber operations, the following is deemed to be a more concise range of terminology:

- **Offensive Cyber Operations:** Activities that are designed to project power and to enable militaries to achieve their tactical, operational, and strategic objectives in cyberspace.
- **Defensive Cyber Operations:** Activities that include the conduct of active and passive measures aimed at preserving the military's use of cyberspace and enable information maneuver.
- **Cyber Intelligence, Surveillance and Reconnaissance:** A broad array of intelligence, surveillance, and reconnaissance (ISR) activities conducted across the entire spectrum of cyberspace including friendly, neutral and enemy domains in order to strengthen understanding and complement existing ISR activities.

For its part, the North Atlantic Treaty Organization (NATO) and the European Defence Agency (EDA) have developed and implemented their own cyber defense architecture frameworks to address the highly militarized cyber threat landscape whilst offering member states a common approach that promotes inter-operability. That said, the onus remains on individual members to shape their capabilities and build effective capacity within military formations in accordance with the strategic aims of NATO and the EDA. In their respective Architecture Frameworks NATO [2] and EDA [3] only addresses cyber defense operations, ultimately achieving some level of interoperability between NATO and / or EDA member countries with regards to Defensive Cyber Operations and to a lesser extent, Cyber Intelligence, Surveillance and Reconnaissance. However, there remains an overall lack of interoperability and a common approach with regards to Offensive Cyber Operations across NATO and EU member states.

The integration of military cyber capabilities should only take place within the scope of a wider transformation that addresses current and emerging threats. The best-case study from which to explain how NATO and EU member countries should build operation cyber capacity would be to look closely at the UK's 'Future Force Concept'. Describing this concept, the UK Ministry of Defence [4] indicates that the concept is best described as an over-arching programme that encompasses a series of transformation projects ranging from the implementation of advanced soldier systems (clothing, personal weapons and protective solutions) to the reorganizing of military units in accordance with the UK's National Security Capability Review 2017 [5] and its successive Integrated Review of Security, Defence, Development and Foreign Policy 2021 [6]. The latter of which concluded the need for the UK to develop a new National Cyber Force and Counter-Terrorism Operations Centre which covers the full extent of internal and external security threats. As such, the Future Force Concept sees that the future British military will become a threat-integrated, but comparably small fighting force. Additionally, the Future Force Concept also recognizes that technology will remain a significant factor in any future conflict and a significant factor that drives change in the military.

Whilst it is recognized that any threat review or analysis undertaken by NATO and / or EU member countries is likely to be conducted in isolation - as a direct result of classification restrictions and the use of intelligence sources whose details need to be adequately protected - open-source information should be considered.

## 3. The Role of Cyber Capacity Building

Cyber capacity building encompasses the development and implementation of cyber capabilities through the integration of technology, provision of training and mentoring, and the wider implementation of national-level reform. It should also be strongly based on the outcomes of an integrated threat review / analysis and be driven by Defence and industry partners cross-government within two clearly defined parameters: Force Development and Force Generation.

Force Development within the scope of cyber operations of a cyber military force should be a joint force effort that encompasses the full spectrum of military functional areas including Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance - otherwise referred to as 'C4ISR'. When developing and enacting Force Development, it should follow the following key processes:

- **Force Design:** The desired scope and structure of the cyber force should address the key outcomes of the Threat Review and keep within the parameters outlined within the military's wider operational commitments. Specifically, it should take into account the availability of personnel, funding and systems.
- **Structural Development:** Like the wider military, the cyber force should have a clear structural leadership that is clearly designed and implemented according to the C4ISR functional areas concept.
- **Talent Acquisition:** The bulk effort within the Force Development phase, talent acquisition should be a joint effort from across the military to identify and acquire the necessary talent for cyber operators from the enlisted ranks. It can be argued that the role of cyber operators should be filled from personnel from J2 (Intelligence) and J6 (Communications) functional areas; this is based primarily on the fact that cyber operations require a higher level of technical expertise and certainly requires an intelligence-driven approach. Going further, the identification and acquisition of talent should also be driven by a corporate-level initiative that aims to recruit part-time specialists - or cyber reservists - within the cyber and EMA industry that will also make way for high-level training and mentoring to naturally evolve. Again, it can be argued that the process of talent acquisition for cyber operations specialists should be conducted across J2 and J6 functions to ensure that technical expertise and intelligence capabilities are fully satisfied in this regard.

Force Generation is best described as the physical processes employed by the military to implement capabilities within its cyber force. By default, it is a circular process that constantly evolves, and is designed to take place in concert with Force Development. The generation of the cyber force should be driven by the overall needs of the armed forces as opposed to the needs of individual services. Concurrently, it should also be reinforced by a corporate-level programme from which specialist-level training and capabilities are implemented. Force Generation can be further described by the following processes which should occur in the following order, though overlaps may take place:

- **Education**: A comprehensive education curriculum should be devised and implemented across any new or existing cyber force. It should be focused on indicating how Cyber and EMA activities intend to integrate into the wider military and in what operational spectrums it intends to support, and how. This education should be continuously devised and implemented across the force as opposed to being delivered irregularly.

- **Force Management**: With the structure of the cyber force constructed and required talent acquired, a management structure should be devised and implemented consisting of generalists and specialists with clear roles and responsibilities.
- **Systems Integration**: In accordance with the Threat Review and wider Defence Review, the necessary systems required for any new or existing cyber force should be acquired and integrated as per the military's budget allocation and procurement rules. Systems include general and specialized hardware, hardware and software, and access to third-party intelligence.
- **Specialized Training**: The design, development and implementation of specialized training should take into account individual roles within the cyber force in addition to the range of systems that cyber operators will be expected to use. For the most part, such training will naturally be provided by systems providers; remaining training themes including intelligence collection techniques, penetration testing and malware analysis (to name but a few) should be designed and delivered by competent third-party service providers. Specialist training should also be balanced against the cyber force's current needs and the needs identified during the Force Development stage.
- **Red and Blue Team Exercises**: Activities in the form of exercises should be designed and delivered over regular periods in order to maintain the overall readiness of the cyber force and to ensure that capability gaps are effectively identified and addressed. Additionally, the wider military should adapt existing military exercises to include cyber-related serials for example, cyber and electro-magnetic attacks targeting Battlegroup, Brigade and Divisional-level formations. Lastly, the cyber force should also play an integral part in multi-national NATO and EU Battlegroup (EUBG) exercises.

## 4. Strategic-Level Capability Development

In its 2018 Framework for Future Alliance Operations report, NATO detailed the future scope of joint operations, indicating that operations in cyberspace would not only see a significant increase but would grow to become more inter-twined with joint ground, air and sea operations [5]. Meanwhile, the UK's Future Force Concept envisages that the British Armed Forces will become increasingly involved in joint NATO-EU operations as opposed to engaging in unilateral conflicts [4]. As such, both of the aforementioned reports emphasize a greater effort towards developing inter-operable capabilities, cross-domain effects, systems and doctrine.

Each NATO and EU member country will inevitably structure their strategic-level cyber capability differently than others - most likely due to their own interpretation of threats and military requirements. Until the mid-2000s, most of the larger NATO member countries including the United States, United Kingdom, France and Germany structured their strategic-level cyber capability along the lines of their own communications intelligence agencies, sometimes augmented by military intelligence specialists. In the United Kingdom, strategic level cyber was almost exclusively led by the Government Communications Headquarters (GCHQ), working alongside strategic partners namely their 'Five Eyes' partners in the United States, Canada, Australia and New Zealand. However, following the National Security Strategy and Strategic Defence and Security Review 2010, the United Kingdom saw strategic-level cyber operations delegated to a centralized joint military and intelligence capability responsible for overseeing national-level cyber operations and the delegation

of capabilities to operational and tactical formations - primarily within Force Troops Command, also known as the 6th (United Kingdom) Division [7].

## 5. Conclusion

An increase in Russian and Chinese information maneuver within cyberspace has inevitably focused the attention of NATO and EU members to increase their capacity to counter this evolving threat. Whilst noticeable efforts to increase the cyber defense posture of Western countries and enhance interoperability between them is evident, a considerable lack of interoperability with regards to offensive cyber operations and cyber intelligence-gathering has been observed. Additionally, there remains a lack of a unified approach by NATO and EU member states with regards to the design and implementation of inter-operable cyber capacity building programmes. In stark contrast, both Russia and China have taken into consideration the evolving nature of the modern battlefield by shaping their military approach to operations in cyber space. Individually, several NATO and EU member states have unilaterally begun re-shaping their military capabilities, though such transformation programmes - such as the United Kingdom's 'Future Force Concept' - does not address the need for processes and systems to be interoperable with NATO and EU allies.

Moving forward, the raising of capacity and the development of cyber capabilities within strategic-level formations should undoubtedly be driven by the need to increase interoperability and joint operations between NATO and EU member countries. As such, the development of doctrine, implementation of red and blue team exercises in addition to exchange programmes should actively be encouraged. Whilst interoperability with regards to Cyber Defence Operations is somewhat reinforced within the NATO Architectural Framework [3] and the EDA's Cyber Defence Refence Architecture [2]; the lack of interoperability with regards to Offensive Cyber Operations and Cyber Intelligence, Surveillance and Reconnaissance reinforces the requirement for greater-level cooperation between countries and their respective militaries. Indeed, it is likely that NATO and the EDA view Offensive Cyber Operations and Cyber Intelligence, Surveillance and Reconnaissance to be the sole responsibility of its individual members, though it can be argued that the current cyber threat environment reinforces the need for greater interoperability in this regard.

## References

[1]. 2018. Future Force Concept (Joint Concept Note 1/17). [ebook] Ministry of Defence. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643061/concepts_uk_future_force_concept_jcn_1_17.pdf [Accessed 3 April 2022].

[2]. "Cyber resilience, a prerequisite for autonomous systems - and vice versa," Default. [Online]. Available: https://eda.europa.eu/webzine/issue16/cover-story/cyber-resilience-a-prerequisite-for-autonomous-systems-and-vice-versa/. [Accessed: 04-Apr-2022].

[3]. North Atlantic Treaty Organization, "NATO Architecture Framework (Version 4)," North Atlantic Treaty Organization, 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/1/pdf/NAFv4_2020.09.pdf (accessed Apr. 04, 2022).

[4]. "Development, Concepts and Doctrine Centre Future Force Concept." [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643061/concepts_uk_future_force_concept_jcn_1_17.pdf.

[5]. North Atlantic Treaty Organization, "Framework for Future Alliance Operations, 2018 Report" North Atlantic Treaty Organization, 2018. https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf.

[6]. "Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy." [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf.

[7]. "National Security Capability Review." [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.

# Children and the Internet: Vulnerability or Opportunity?

**Nicoleta APOLOZAN**
The Institute for Crime Research and Prevention, General Inspectorate of Romanian Police, Bucharest, Romania
nicoleta.apolozan@politiaromana.ro

**Abstract**

*As a member of the implementation team of the Cyberex RO Project - Improving, cooperating and preventing in the fight against cybercrime, I conducted a survey among students aged 10 to 18 on the topic of online security. This paper discusses the results of this survey regarding children's habits on using the Internet, the safety measures they know and use, their level of information and their need to learn about Internet safety issues.*

**Index terms:** digital skills, level of information, information needs, online behaviour, online safety

## 1. Introduction

For children, the Internet is an important resource for learning, personal development or socializing and entertainment, but it is also an environment where risks are present to the same extent, if not to a greater extent, than in real life. As previous studies have shown, "online activities are not in themselves beneficial or harmful to children" and "opportunities and risks go hand in hand" [1].

Both the rapid development of Internet-connected devices and the easy and quick access to the Internet, and the growing interest of children in using them, wanting to reap all the benefits of a "connected" life [2], contribute to the presence of the growing number of minors on the Internet, while also exposing them to the risks involved by the online environment, from infecting their devices with malicious software and stealing information from them, to more serious acts such as blackmail and online child pornography [3].

As some previous studies show, the transnational dimension of cybercrime, in addition to the ineffectiveness of regulatory enforcement mechanisms in this area [4], makes it difficult to investigate and prosecute those responsible. Thus, the importance of informing and educating children in order to behave responsibly on the Internet is once again emphasized [5], [6].

In this paper I discuss the results of a survey conducted among young students between the ages of 10 and 18 on the topic of Internet safety. This survey was part of a larger study, *Risks and Vulnerabilities of Students in the Online Environment*, conducted by the Institute for Crime Research and Prevention in 2021, as part of the RO Cyberex Project - Improvement, Cooperation and Prevention in the Fight against Cybercrime, funded by the European Union from the Internal Security Fund - Component for Police Cooperation.

Within this project, I was part of the implementation team, as a research expert, carrying out both the research methodology and the analysis, interpretation of data and drafting of the research

report. I took care of the results of the survey exclusively, and those of the interviews conducted with specialists in collaboration with the other expert from the Institute.

The study aimed, first of all, to identify the main risks and vulnerabilities faced by young students aged 10 to 18 in Romania in the online environment (mainly child pornography and cyberattacks), in order to substantiate, on a scientific basis, the activities of preventing online crime against children.

A component of the study consisted of conducting a survey on a sample of 1445 young students, nationally representative for the population of students aged 10-18 years (a random, multistage, stratified sample). The sampling error was ± 3%, at a 95% confidence level, and the data were collected between 16.11 - 03.12.2020. For more details on the research methodology, it can be consulted in the research report, fully available online [7].

The objectives of the survey included the description of children's usage habits and their behaviour on the Internet, the assessment of the level of knowledge and use of safety measures in Internet use, and identifying risk factors and vulnerabilities to cyberattacks and child pornography. We also considered identifying the need to inform this segment of the population about online safety measures.

## 2. The results of the survey

### 2.1. Children's habits when using the Internet

The results of the study show that more than a third of students started using the Internet at a very young age, when they were less than 7 years old (14% less than 5 years old, to which is added about 25% between the ages of 6 and 7).

It is also observed that the self-taught method is the defining learning path for most of the respondents, so that 40% of the students state that they have learned on their own how to use the Internet, without any help, to which is added those who claim to have learned on their own, but were also guided by other people (27%). As a result, 67% of students say that they have found out how to use the Internet mainly on their own.

The vast majority of students surveyed (96%) used the Internet every day, but depending on the age group, we noticed that the percentage was slightly lower for students under 14 (93%) compared to those aged higher (over 98%). While there were no significant differences between girls and boys in terms of Internet usage, urban students connected more often than rural students (97% compared to 93%).

In general, minors access the Internet from multiple devices, depending on their availability. Thus, most (approximately 76%) have access to the Internet from their own mobile device (smartphone or tablet), but they also connect from home, from their own computer or laptop (48%), from a computer or laptop used by family (25%), on TV (23%), on a game console (11%), on the phone or tablet of an adult family member (e.g. parents, grandparents - 7%), on a tablet received from school (4%), on the phone or tablet of another minor family member (e.g. brother, cousin - 4%) or from school, on a school device (computer, laptop, tablet - 3.5%). Depending on their age, the results show that students over the age of 14 have access to the Internet from their mobile device in a higher percentage than those who are younger (82% over the age of 14, compared to 69% at a younger age).

Given the suspension of physical education in schools and the conduct of online teaching activities due to the COVID 19 pandemic, the most frequently mentioned Internet activity was online schooling (82% of respondents). However, the favourite online activities of minors were, in order, the use of social networks (64%), writing, reading, checking emails (61%), instant messaging (59%),

watching movies or online series (59%) and voice or video calls using applications that use the Internet (57%).

Online games are also one of the favourite activities of students in the online environment, with 54% of students saying that they spend time with online games with other people, and 47% say that they play such games alone.

Boys are much more interested than girls in online games that they can play with other people (67% vs. 42%), as well as in online games that they can play alone (58% vs. 39%). In contrast, girls are more interested than boys in using social media (69% vs. 59%) and watching movies or series online (66% vs. 51%).

In general, students under the age of 14 have a much greater interest in posting on their own vlog (e.g. on YouTube, TikTok) compared to other age groups (31% compared to 14% of those aged 14-15 and 18% over 15 years). In contrast, both 14-15 year olds and 16-18 year olds show a greater interest in purchasing goods or services online (e.g. books, concert tickets, train tickets, sports equipment, clothing, etc.) - 49% and 46%, respectively, use of social networks (76% and 78%, respectively), instant messaging (72% and 67%, respectively), entertainment (e.g. watching videos or audio-videos on YouTube, including watching vloggers) - 61% and 56%, respectively, as well as downloading movies, series or music (41% and 33%, respectively).

The biggest differences between urban and rural students are in the use of the Internet for online shopping (40% urban, 18% rural), watching movies and online series (65% and 43% respectively), voice or video calls (63% and 43% respectively), instant messaging (64% and 45% respectively) and entertainment (e.g. watching videos or listening to audio files on YouTube, including vloggers) - 57% and 38%, respectively.

### 2.2. Young students' safety on the Internet

Most of the students between the ages of 10 and 18 say that they feel safe when surfing the Internet (73%). Boys are much more confident than girls about Internet safety, with 81% of boys saying they feel safe on the Internet (to a large or very large extent), while 67% of girls say the same.

As the age of students increases, so does the percentage of those who say they feel safe on the Internet: 71% of those under the age of 14, 74% of 14-15 year olds, and 78% of 16-year-olds and over.

The focus of students on Internet security measures is mainly on blocking people who are bothering them and changing the privacy settings of their profile on social networks.

Thus, most of the students (93%) state that they know how to block a person who is bothering them on the Internet (on social networks, e-mail or online messaging application). Instead, their percentage decreases in connection with settings that require more knowledge, such as changing profile privacy settings on social networks (79%), blocking pop-ups with notifications (66%) or site security checks (63%). Less than half of students between the ages of 10 and 18 (48%) say they know how to enable or change filters (change how their computer or Internet browser selects which sites or content to view).

Boys are more likely than girls to check that the sites they use are safe (71% of boys versus 56% of girls), to activate and change filters (54% of boys compared to 43% of girls) and block pop-ups with ads or other annoying notifications (69% of boys compared to 63% of girls).

On the other hand, girls are more interested in changing the profile privacy settings on social networks (83% of girls compared to 75% of boys).

There are no significant differences between boys and girls in the skills of blocking people who bother them on the Internet (instant messaging, social networking or email), deleting the history of the sites they have visited or searching and finding information on how to use the Internet safely.

In terms of age, the number of younger students (under 14) with a higher level of knowledge of Internet safety is lower than the number of older students. The most significant differences are in the case of skills such as blocking pop-ups with ads or other notifications, deleting the history of the sites they have visited and changing the privacy settings of the profile on social networks. In contrast, the degree of knowledge of these measures by students aged 14-15 is comparable to that of older students (16-17 years).

Minors in rural areas differ from those in urban areas by the fact that there are fewer children who know how to use security measures on the Internet, the biggest differences being found in changing the privacy settings of the profile on social networks (69% rural compared to 83% urban) and blocking pop-ups with various advertisements or notifications (55% rural compared to 71% urban).

### 2.3. Students' knowledge on Internet safety and online risks

89.4% of respondents considered that they are sufficiently well informed about the risks on the Internet, approximately the same degree of confidence being felt by both students studying in urban and rural areas.

Considering the age of the students who took part in the opinion poll, there is a decrease in confidence in their own risk-avoidance skills on the Internet as they get older. Thus, 44.6% of respondents under the age of 14 consider themselves well informed, while only 24.4% of those over the age of 15 state that they have sufficient information.

Most of the students said that they knew that they could report the unpleasant events they encounter on the Internet to the police or directly on the site. 53.2% of them said they knew a phone number they could call if needed. Only about a third of students were aware that they could report disturbing behaviours on the Internet via email, websites, or online forms.

The age group that has most stated that they know how to report crimes or other behaviours that bother them on the Internet is that of students under 14 years of age. Of those who said they were informed about how to report, about 75% were studying in urban schools.

Regarding the information needed to be safe on the Internet, most of the respondents appreciated the need to assimilate details about social networks, mentioning elements such as the security of accounts related to various services, exploitation of personal data and identity theft.

Another significant share of the answers referred to the need to acquire IT-specific notions: protection against viruses, methods used by hackers, as well as in-depth elements such as creating dedicated protection software, using VPN, protection against flooding threats. At the same time, they emphasized the importance of knowing the elements that differentiate the safe content from the potentially harmful one.

Last but not least, they highlighted the importance of information on the types of offenses related to the online environment, their consequences, as well as the competent institutions they can turn to in case they become victims of such offenses.

The answers given by the students show an increased interest in the use of social networks to the detriment of other types of information, applications or sites. In fact, a large number of respondents stated that they had enough information to be safe, using the resources available online to update their knowledge in the field.

## 3. Conclusions

The results of the survey show a very large share of daily Internet users among young students, their own mobile devices being the most accessed equipment, and the self-taught method being the defining learning path for most respondents. At the same time, the entertainment (social networks, vlogs, movies or series) occupies the agenda of young users of Internet.

As they grow older, youths engage in the purchase of goods and services on the Internet, but there is also a growing sense of security for the online environment, while becoming aware that they are not sufficiently informed about how to protect their devices and themselves in the virtual world.

Social networks play a key role in students' discourse, as these are mentioned by respondents in topics such as the main ways of using the Internet, concern for account security (e.g. regular password replacement) and potential risks, such as breaking their accounts, indecent conversations or various illegitimate requests from strangers.

The information that the students aged between 10 and 18 years want to receive from the authorities, as well as from other organisations with concerns in the field, aims, as we have previously shown, first of all, how to secure their accounts on social networks, but they also show interest in learning how to exploit personal data securely, highlighting both the concern of becoming a victim of identity theft and the desire to find out how to protect themselves from it.

They have also expressed the need of learning about the elements that differentiate safe content from potentially harmful content, as well as the desire to learn more about specific types of offenses related to the online environment and their consequences.

Last but not least, the students were interested in receiving information about the institutions they can turn to if they become victims of these crimes and what is the concrete way in which they can be helped to overcome the situation of victimization.

## References

[1]. Velicu, B. Balea & M. Barbovschi, 2019, Internet access, uses, risks and opportunities for children in Romania. EU Kids Online 2018 results, EU Kids Online and DigiLiv-REI, https://www.academia.edu/38372598/Acces_utiliza_ri_riscuri_s_i_oportunita_t_i_ale_internetului_pentru_copiii_din_Roma_nia_Rezultatele_EU_Kids_Online_2018.

[2]. S. Molter, G. Martinez, M. Garmendia, J. Croll, A. Järventaus, 2021, Children's rights in the digital space, Observatory for sociopolitical developments in Europe, https://www.researchgate.net/publication/352821929_Children's_rights_in_the_digital_space.

[3]. Europol, 2021, Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg, https://www.europol.europa.eu/publications-events/main-reports/Internet-organised-crime-threat-assessment-iocta-2021.

[4]. M. Pisaric, 2012, EU legal framework of fight against child pornography on the Internet, https://www.researchgate.net/publication/269660273_EU_legal_framework_of_fight_against_child_pornography_on_the_Internet.

[5]. Phippen, 2017, ”What Do We Mean by “Child Online Safety”?”, in Children’s Online Behaviour and Safety, Palgrave Macmillan, London, https://doi.org/10.1057/978-1-137-57095-6_1, pp. 1-13.

[6]. J. Savirimuthu, 2012, The Child, Media Literacy and Online Safety Policy Implications, https://www.researchgate.net/publication/304655900_The_Child_Media_Literacy_and_Online_Safety_Policy_Implications.

[7]. General Inspectorate of Romanian Police, Risks and vulnerabilities of young students in the online environment, The Institute for Crime Research and Prevention, Bucharest, https://www.politiaromana.ro/files/pages_files/raport_cercetare_Proiect_Cyberex.pdf.

# Cybersecurity of WordPress Platforms. An Analysis Using Attack-Defense Trees Method

**Gabriel PETRICĂ, PhD**
Faculty of Electronics, Telecommunications and Information Technology,
University POLITEHNICA of Bucharest, Romania
gabriel.petrica@upb.ro

**Abstract**

*The aim of this paper is to analyze the techniques for securing a Content Management System, highlighting the vulnerabilities of the WordPress platform. The study includes qualitative and quantitative analyzes on the resilience of CMS platforms to cyber-attacks, simulated by the AD Trees methodology. The data provided by CVE is used to build possible attack scenarios that could compromise the cybersecurity of the web application. At the end of the paper, in order to minimize the impact of these attacks, solutions are proposed as sets of countermeasures within the Attack-Defense Trees.*

**Index terms:** Attack-Defense Tree, CMS, cyber-attacks, software vulnerabilities, WordPress

## 1. Introduction

In today's information society, a Content Management System (CMS) is a modern and easy-to-use tool that accelerates an organization's ability to create, disseminate, and update various types of content. Current web technologies enable organizations to deliver consistently updated, real-time content and meet clients' dynamic demands. CMS is the solution for automated control of information collection, management, and distribution [1].

Among the features of a Content Management System, we can mention:

- easy to install and adapt to various types of websites;
- the graphical interface is simple and facilitates content management (text, images, multimedia objects);
- is suitable for different types of content;
- benefit from regular updates.

The functionalities of a CMS consist mainly of 3 aspects: *data collection*, *components management* and *content publishing*. *The collection* is the process of creating or acquiring data, automatically converting the format, the aggregation process, reusing information, and content segmenting into metadata. *Components management* can refer to several aspects regarding [2]:

- the system (components security, automatic indexing, management dashboard, scalability, flexibility and simplicity);
- document management (keeping document versions, several types of formats, automatic updating and deleting, compatibility with other applications);
- publishing (using a template for a consistent layout, automatic content conversion, advanced customization system, multilingual interface).

In the content lifecycle management process (fig. 1) the following steps are considered [3]:

- content organization and planning;

- defining the workflow;
- content creation;
- data storage and availability in case of emergency;
- professional content editing;
- checking the content before its publication;
- deleting / archiving the content or updating it to bring it back to the attention of the audience.

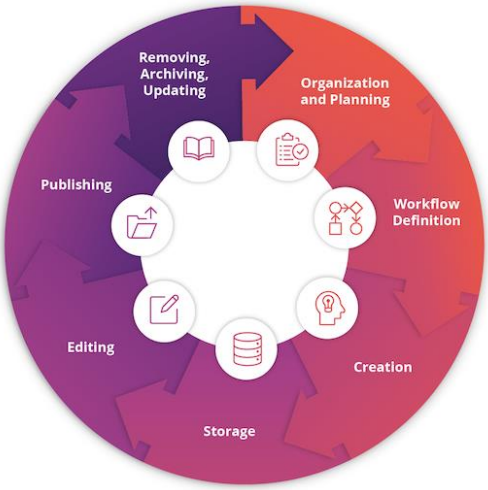



**Fig. 1.** Content lifecycle management steps [3]

## 2. WordPress vulnerabilities

Content management systems are becoming more and more popular and, thanks to the features offered, the number of websites using CMS is growing exponentially. That's why websites developed with a content management system are becoming attractive targets for cybercriminals.

The security of the infrastructure that connects to the Internet environment is essential for organizations when considering the security of their network. Even if the infrastructure that connects to the outside world does not store sensitive information, there is a significant risk to the reputation of organizations in the event of cyber-attacks. Security vulnerabilities in content management systems installed on organizations' web servers are often exploited by cyber attackers. Once such a system has been compromised, the web server can be used as a tool to facilitate intrusion attempts or to launch other cyber-attacks [4].

An attacker can use automated tools to find security vulnerabilities in web servers or CMS platforms. Usually, these intrusions are the result of a low level of security of the victim's computer or server rather than deliberate attacks. If a software vulnerability is found or a CMS has been compromised, the attacker can:

- gain access to the authenticated and privileged areas of a web application;
- upload malware to the web server to facilitate access through Remote Administration Tool (RAT);
- inject malicious content into legitimate web pages.

The different ways of identifying and noting software vulnerabilities and the lack of interoperability between databases and tools related to the same vulnerabilities led to the launch of the Common Vulnerabilities and Exposures (CVE) project in 1999. Designed and coordinated by Mitre Corporation, CVE is a tool for monitoring and standardizing the most common vulnerabilities, which ensures trust between the parties when is used to discuss or share information about a unique vulnerability of an application, operating system, service or firmware [5]. Each known vulnerability

is uniquely identified in the National Vulnerability Database (NVD) and is also available in the CVE list, with detailed descriptions for each vulnerability, as well as a Common Vulnerability Scoring System (CVSS) that quantifies (on a scale from 0 to 10 - maximum severity) the impact of that vulnerability [6].

For a WordPress platform, the distribution of software vulnerabilities in 2021, based on data collected by CVE Details [7], is described numerically in the next table and graphically represented in fig. 2.

**Table 1.** WordPress software vulnerabilities reported in 2021 [7]

| # | CVE ID | Vulnerability Type(s) | Score | Affects Confidentiality? | Affects Integrity? | Affects Availability? |
|---|---|---|---|---|---|---|
| 1 | CVE-2021-44223 | Exec Code | 7.5 | Partial | Partial | Partial |
| 2 | CVE-2021-39203 | Bypass | 6.0 | Partial | Partial | Partial |
| 3 | CVE-2021-39202 | XSS | 3.5 | None | Partial | None |
| 4 | CVE-2021-39201 | XSS, Bypass | 3.5 | None | Partial | None |
| 5 | CVE-2021-39200 | +Info | 4.3 | Partial | None | None |
| 6 | CVE-2021-29450 | +Info | 4.0 | Partial | None | None |
| 7 | CVE-2021-29447 | undefined | 4.0 | Partial | None | None |
| 8 | CVE-2020-36326 | undefined | 7.5 | Partial | Partial | Partial |

We note that these software vulnerabilities generally have a medium impact on the security of the WordPress platform (with a score between 3.5 and 7.5 points). However, there are three exceptions, which partially affect the components of the C-I-A (Confidentiality, Integrity, and Availability) triad:

- CVE-2021-44223, “Execute Code” type vulnerability: “WordPress before 5.8 lacks support for the Update URI plugin header. This makes it easier for remote attackers to execute arbitrary code via a supply-chain attack against WordPress installations that use any plugin for which the slug satisfies the naming constraints of the WordPress.org Plugin Directory but is not yet present in that directory.” [8];
- CVE-2020-36326: “PHPMailer 6.1.8 through 6.4.0 allows object injection through Phar Deserialization via addAttachment with a UNC pathname” [9];
- CVE-2021-39203, “Bypass” type vulnerability: “Authenticated users who don't have permission to view private post types/data can bypass restrictions in the block editor under certain conditions” [10].

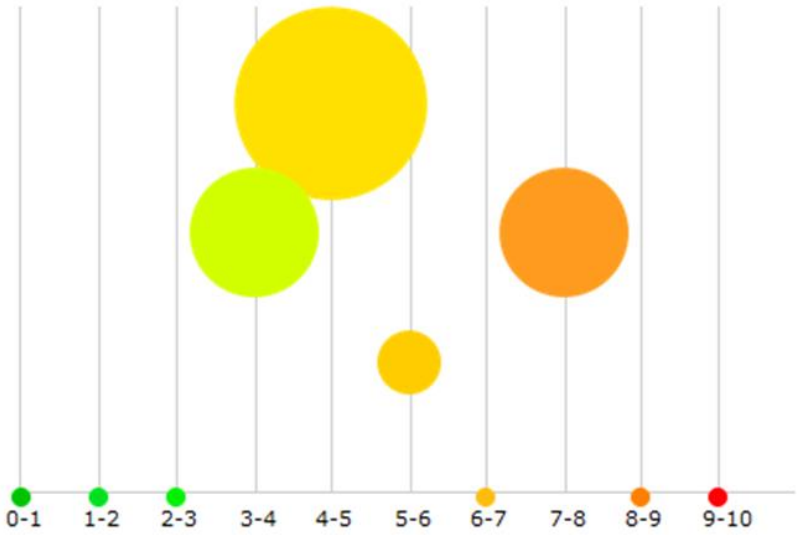



**Fig. 2.** WordPress software vulnerabilities distribution in 2021, by CVSS score (according to CVE Details [7])

## 3. Exploiting WordPress vulnerabilities. Attack-Defense Trees

Attack-Defense Trees (AD Trees) is a graphical methodology used by both system designers and personnel specialized in ensuring information security in various fields (information technology, military or aerospace industry, banking or business, etc.) to model and analyze system security threats. This method, introduced by Bruce Schneier, provides a graphical analysis of the ways in which a target (computer, network, organization) can be attacked (a goal can be reached by a potential threat) and indicates the measures taken by the defender to prevent achieving that goal by the attacker [11].

An AD Tree can have two types (categories) of nodes: attack nodes (represented by circles) and defense nodes represented by rectangles, while the *root node* of the tree describes the main target (objective) of one of the players (attacker or defender, depending on the role analyzed). The *root* node represents a state of success (from the point of view of the attacker), while the nodes of the tree express different ways to achieve the main goal [12]. An Attack Tree is a subclass of AD Trees in which only the actions of the attacker are considered.

In this hierarchical structure, each node can have one or more children of the same type, which detail the purpose of the node into several sub-objectives. Thus, each path represents a unique type of attack (a possible scenario). The relations between nodes can be conjunctive or disjunctive, being defined as follows:

- the objective of a conjunctive node is reached when all its objectives directly connected from the lower level are reached (AND logical function) - AND (N_1, N_2) - fig. 3.a;

- the objective of a disjunctive node is reached when at least one of its objectives directly connected from the lower level are reached (OR logical function) - fig. 3.b.


**Fig. 3.** The *root* and *N_1*, *N_2* nodes in an AD Tree: (a) AND function; (b) OR function

In this paper we used the ADTool application [13] because it allows the construction of the attack / defense scenarios in a descriptive way, based on a language consisting of six operators that can have as arguments labels or other operators:

- op() - *or-proponent* (OR operator for the attacker), op(x, y) = x ∩ y;
- oo() - *or-opponent* (OR operator for the defender);
- ap() - *and-proponent* (AND operator for the attacker), ap(x, y) = x ∪ y;
- ao() - *and-opponent* (AND operator for the defender);
- cp() - *countermeasure-proponent* (operator for the attacker), cp(x, y) = x ∩ y';
- co() - *countermeasure-opponent* (operator for the defender).

We conducted a case study based on the security analysis of a web application built on a WordPress platform. After installing the necessary tools and the actual implementation of the Web application, we built the Attack Tree based on the ADT methodology with the main objective "WordPress security breach" by exploiting software vulnerabilities of the WordPress platform identified in 2021. Delaying response or blocking operation of application, unauthorized data extraction, monitoring activity or inserting malicious code are other objectives of a potential attacker.

Possible attacks will exploit the eight software vulnerabilities reported in 2021 for WordPress platform [14], indicated in tab. 2 and represented graphically in fig. 4.

**Table 2.** WordPress vulnerabilities reported in 2021 [14]

| WordPress | TOTAL | Execute Code | Bypass | XSS | Gain Information | Other types |
|---|---|---|---|---|---|---|
| | 8 | 1 | 1 | 2 | 2 | 2 |

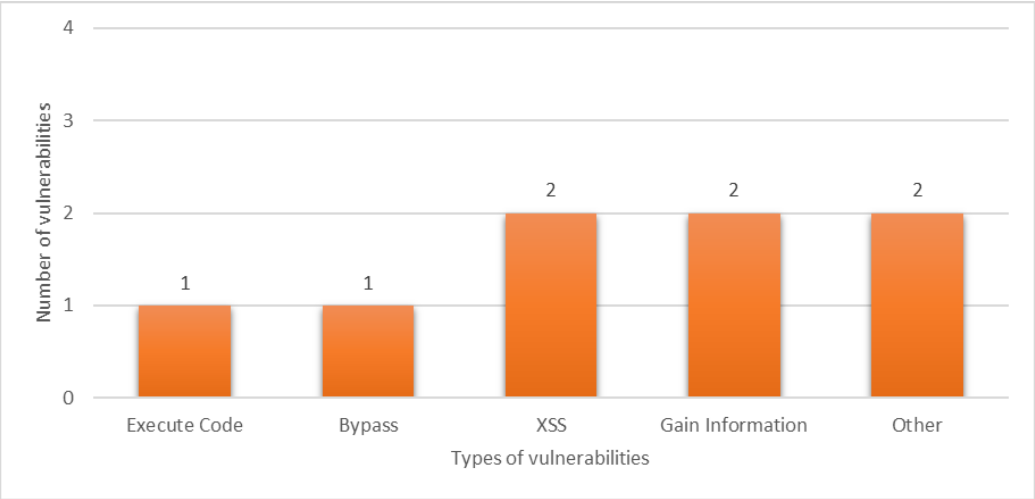



**Fig. 4.** Vulnerabilities in WordPress platform (according to CVE [14])

The code of the Attack Tree (represented in fig. 5) is indicated below: the achievement of the proposed objective ("*WordPress security breach by exploiting software vulnerabilities*") will be possible by exploiting any of the eight vulnerabilities identified (CVE-2021-44223 *or* CVE-2021-39203 *or*… *or* CVE-2020-36326).

```
op(CVE-2021-44223, CVE-2021-39203, CVE-2021-39202, CVE-2021-39201, CVE-2021-39200, CVE-2021-29450, CVE-2021-29447, CVE-2020-36326)
```

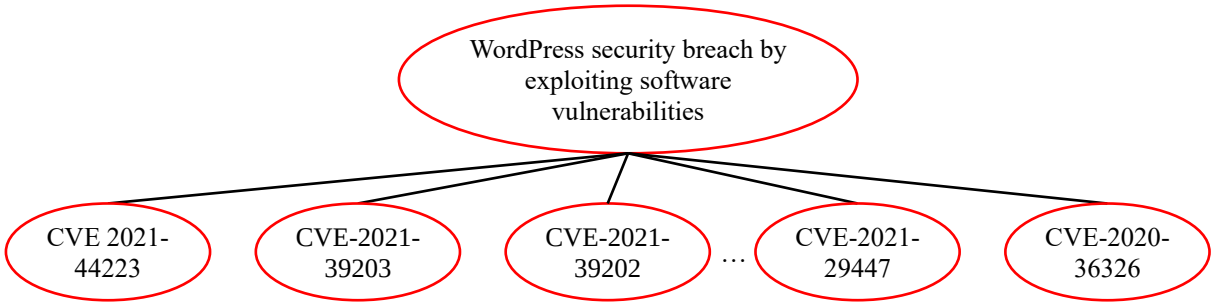



**Fig. 5.** Attack Tree - the objective "*WordPress security breach by exploiting software vulnerabilities*"

The countermeasures adopted by the defender refer to the following categories of corrective actions (see tab. 3 and fig. 6 representing the AD Tree with the implemented countermeasures):

- fixing CVE vulnerabilities;
- secure management of passwords;
- validate the data entered for authentication and limit the number of login attempts;
- other measures (the countermeasures N_4).

**Table 3.** Countermeasures / corrective actions

| Countermeasures | Corrective actions |
|---|---|
| N_1 | Update WordPress components: platform (core) / plugins / themes<br>Delete unused plugins / themes |

| Countermeasures | Corrective actions |
|---|---|
| | Installation from secure sources<br>Rules in .htaccess (configuration file used by Apache web server) |
| N_2 | Requesting a minimum length password<br>Weak passwords warnings<br>Mechanism for generating random passwords<br>Controls for complex passwords<br>Not allowing passwords with a typical content<br>Password strength indicator<br>Encrypt stored passwords<br>Sending passwords only through secure protocols<br>Provide a reset procedure if the password has been forgotten<br>Require a periodic password change |
| N_3 | Limit login attempts for a user / IP address<br>Using CAPTCHA technology<br>Implementing 2-factor authentication<br>Full input validation<br>Using Web Application Firewall<br>Creating an unpredictable account name and granting administrator rights, followed by deleting the default administrator account (“admin”)<br>Disconnect idle accounts<br>Show minimal information if login failed (e.g. “Incorrect login”) |
| N_4 | Limiting responses to queries<br>Disable XML-RPC protocol<br>Changing the default tables prefix, at WordPress setup or later (manually or by using a plugin)<br>Request re-authentication before changing sensitive settings |

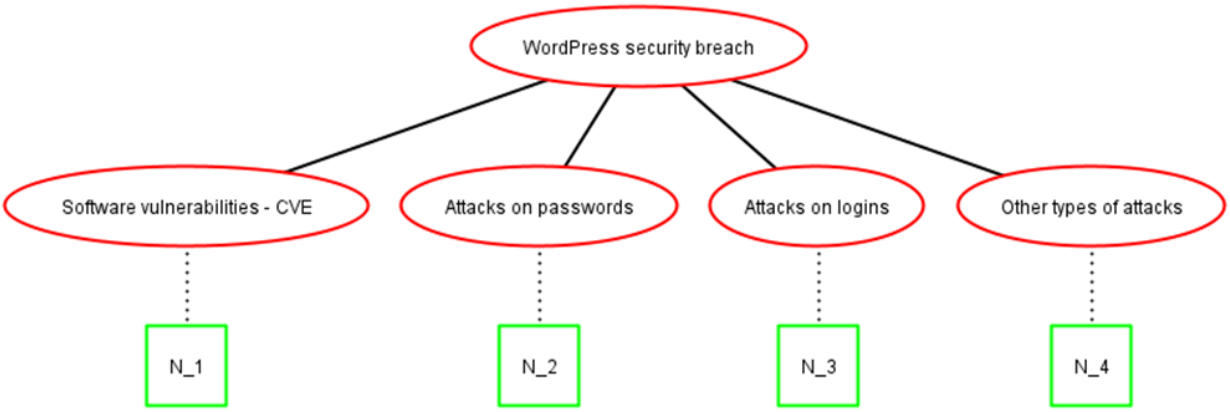



**Fig. 6.** AD Tree with the implemented countermeasures

The code of this AD Tree will be based on the operators op() and cp() and will have the following expression:

```
op(
 cp(Software vulnerabilities - CVE, N_1),
 cp(Attacks on passwords, N_2),
 cp(Attacks on logins, N_3),
 cp(Other types of attacks, N_4)
)
```

The AD Tree with the implemented countermeasures will have the configurations presented in fig. 7: the logical values *true* / *false* were inserted for the labels corresponding to the attack types, respectively to the countermeasures. The true / false quantitative analysis for the “Software vulnerabilities - CVE” label and N_1 countermeasures allow the following conclusions:

- if the label "Software vulnerabilities - CVE" is *true* and N_1 set of countermeasures is *false* (not implemented), the security is compromised (the top objective "WordPress security breach" is *true*) - see fig. 7.a;
- if the label "Software vulnerabilities - CVE" is *true* and N_1 set of countermeasures is *true*, the attacker does not achieve his goal ("WordPress security breach" is *false*) - see fig. 7.b.

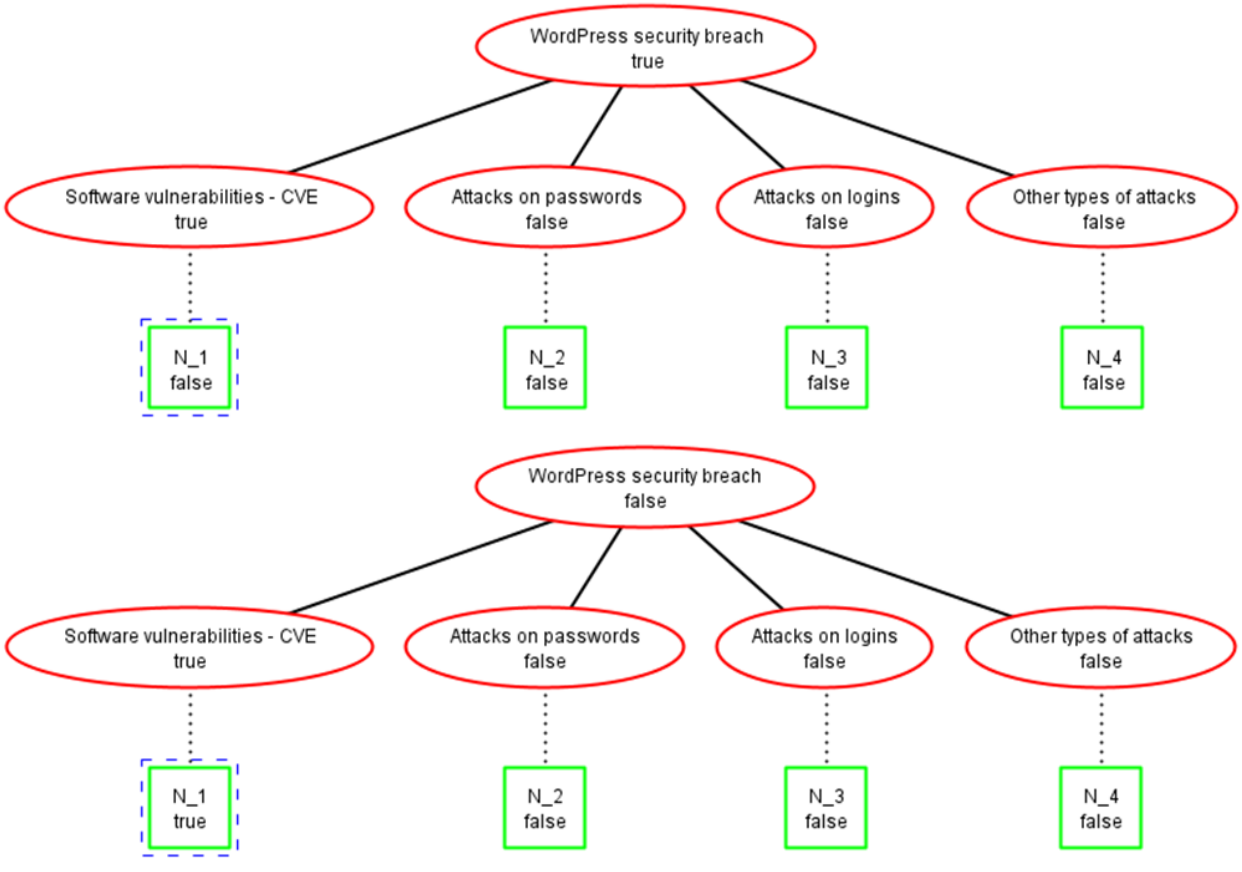



**Fig. 7.** AD Tree with countermeasures:
(a) N_1 set of countermeasures is disabled (false); (b) N_1 set of countermeasures is activated (true)

## 4. Conclusions. Further developments

Apart from the four types of software vulnerabilities presented in tab. 1, over time there have been other types of WordPress vulnerabilities that have allowed various types of cyber-attacks on web applications: SQL injection, Denial of Service, Directory Traversal, Cross Site Request Forgery (CSRF) or Gain Privilege (see CVE database). Among the solutions for protection against these types of attacks we can consider [15]:

- use of input validation and isolation techniques against injection attacks;
- implementation of authorization and authentication mechanisms to prevent security breaches;
- creating backup copies of data;
- use of secure connections.

Security controls that assess vulnerabilities during the installation of a CMS can include:

- use of specific tools to scan for security vulnerabilities, such as WPScan for WordPress;
- performing vulnerability assessments of the custom code or plugins used to enhance some functionalities of CMS.

Further developments of this study consist in extending the analysis to other software components of a complex web application. Vulnerabilities can be identified in the operating system, web server, PHP version, databases, or other software components. Other situations that may lead to application malfunctions include physical attacks (steal or destroy of equipment and access to the server room).

This paper is a starting point in studying the security of a web application built on a WordPress platform. Defending against cybersecurity threats is an ongoing process that must involve awareness of the latest techniques and tools, correlated with the hardware and software environment in which the application operates, but also with user training, the most vulnerable component in ensuring security in an organization.

**References**

[1]. Adobe, Glossary term ”Content management”, https://business.adobe.com/sg/glossary/content-management.html.
[2]. C. Benevolo, Evaluation of Content Management Systems (CMS): a Supply Analysis, 2017.
[3]. Contentstack, Content Lifecycle Management for the Modern Enterprise, https://www.contentstack.com/blog/all-about-headless/content-lifecycle-management/.
[4]. Securing Content Management Systems, 2020, [Online] https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Securing%20Content%20Management%20Systems%20%28June%202020%29.pdf.
[5]. CVE - Common Vulnerabilities and Exposures, https://cve.mitre.org/.
[6]. NIST Common Vulnerability Scoring System Calculator Version 3, https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.
[7]. CVE Details - CVSS Scores for WordPress, https://www.cvedetails.com/cvss-score-charts.php?product_id=4096.
[8]. Vulnerability Details: CVE-2021-44223, https://www.cvedetails.com/cve/CVE-2021-44223/.
[9]. Vulnerability Details: CVE-2020-36326, https://www.cvedetails.com/cve/CVE-2020-36326/.
[10]. Vulnerability Details: CVE-2021-39203, https://www.cvedetails.com/cve/CVE-2021-39203/.
[11]. B. Schneier, Attack Trees, Dobb's Journal, 1999, https://www.schneier.com/academic/archives/1999/12/attack_trees.html.
[12]. G. Petrică, S.D. Axinte, I.C. Bacivarov, Dependabilitatea sistemelor informatice, Matrix Rom, București, 2019, ISBN 978-606-25-0529-5.
[13]. B. Kordy, P. Kordy, S. Mauw, P. Schweitzer, ADTool: Security Analysis with Attack-Defense Trees, Proceedings of the 10th International Conference on Quantitative Evaluation of Systems, 2013, DOI: 10.1007/978-3-642-40196-1_15.
[14]. CVE Details, WordPress: Security Vulnerabilities Published In 2021, https://www.cvedetails.com/vulnerability-list/vendor_id-2337/product_id-4096/year-2021/WordPress-WordPress.html.
[15]. G. Petrică a.o., Cybersecurity Guide, 2021, ISBN 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN, https://www.cyberlearning.ro/cybersecurity-guide/.

# Cyber-Laundering

**Dr. Nathalie RÉBÉ**
Financial Crimes and AML Consultant, Luxembourg
reben@caramail.fr

**Abstract**

*The aim of this chapter is to help the reader gain understanding of the various money laundering practices using technology and discover the way they may be utilized by criminals to finance their illegal endeavors. The author will discuss international compliance and regulatory mechanisms, as well as international countermeasures to deter cyber-laundering.*

**Index terms:** Cyber-laundering, Financial Crimes, Internet Regulations, Virtual Asset / Currencies

## 1. Introduction

Our interconnected world offers new and innovative ways to transfer and disguise funds that represent new money laundering concerns. The internet includes extensions of established payment systems, as well as new payment methods, which operate differently from traditional monetary transactions. As criminals have always been agile in adopting new methods and technologies to circumvent laws, they now take advantage of technological innovation and globalization to further expand their illicit businesses. By conquering and controlling the "cyber space", they can anonymously exploit new opportunities to evade the system and make high value transactions without paper trails or legal accountability. With the use of such methods, they can manage to stay one step ahead of law enforcement.

To comprehend the functioning of online unlawful financial activities, we will discuss how services can be abused, and describe the numerous ways to launder money and assets online. We will also review cyber-laundering risk factors, suspicious activities, and regulatory loopholes, such as weak or inefficient regulations, privacy concerns, jurisdictional conflicts, or law enforcement issues. In the end, recommendations and conclusions will be provided, along with current and future problematics related to cyber-laundering matters.

## 2. How online financial services can be abused?

Money laundering is the concept of converting illegally obtained money, to make it look like it was legitimately obtained. Cyber-laundering, can then simply be defined as the practice of money laundering carried out online. The internet can be used to launder money through multiple methods and at all stages of the money laundering process, namely the placement, layering or integration phases. Criminals can easily disguise their transactions, convert them into cash, they later on deposit in banks. Virtual currencies and assets can also be created and exchanged via a decentralized network of computers, to avoid financial institutions or governments' oversight.

Since the internet is the perfect platform for commerce, financial criminal activities can easily occur online, as transactions fall outside existing regulatory definitions. Therefore, cyber-laundering, is often related to cybercrimes such as: the sale of control substances, the sale of illegal items such as

firearms, tax evasion, terrorism financing, computer crimes, human trafficking, child exploitation, scams, fraud, extortion, etc.

## 3. Ways to launder money and Assets online

There are three main cyber-laundering typologies [1]:

- Internet payment services (such as mobile payments, micro payments or digital precious metals);
- Store value cards and smart cards;
- Online banking.

Additionally, cyber-laundering methods comprise crypto dark pools, over the counter purchases, crypto mining, art, NFT, crypto ATM, and physical to digital goods translation. While these techniques are quite famous ways to launder money, online gambling, gaming, auctions, and virtual worlds and assets are also starting to be known from the general public.

## 4. Risk Factors

The evolution of technology has allowed criminals to transfer large sums of dirty money via the internet. There are quite a few money laundering risk factors associated with new technologies. They include anonymity, the speed of the transactions, untraceable transactions, the cross-border nature of the internet, and third-party funding [2]. Since the internet crosses geographical border, online activities involve several jurisdictions, mutual legal assistance treaties issues, and the ability to transfer unlimited value.

Nowadays, it is nearly impossible to follow an account access and utilization, as it is possible to conduct transactions online from public terminals, and with high-level encryption. The anonymity online services provide also permits to avoid personal "face to face" contact, and to fulfill the "know your customer" compliance principle.

## 5. Suspicious Transactions

Cyber-launderers generally benefit from compliance detection and reporting inefficacy. As technology providers are unable to properly identify and authenticate parties, there is an obvious lack or inadequacy of audit trails, record keeping, and suspicious transaction reporting regarding online financial activities.

There are known "*red flags*" which can help recognize potential illicit online financial behaviors. These specific indicators can be classified into categories, such as: the size and frequency of transactions; transactions' patterns (irregular, unusual, or uncommon); the sender or beneficiary suggest criminal activity; the source of funds or wealth, relationship to criminal activities; or geographical risks [3].

## 6. Regulations

There are many organizations dedicated to preventing and stopping money laundering and cyber-laundering activities such as the United Nations, the European Union, the European Commission, the Financial Action Task Force, the International Monetary Fund, the Financial Crime Enforcement Network, the European Banking Authority, the Basel Institute, and the Egmont Group which established the Financial Intelligence Units. In such effort, several countries and international institutions have introduced robust legislations, recommendations, and policies.

Although Australia, the European Union, and the United Kingdom have created regulations concerning virtual currency, most countries do not have their own cyber-laundering legislation. In the European Union, the most famous tools to combat cyber-laundering are the Fifth [4] and Sixth [5] Anti-Money Laundering Directives implemented by its Member States. There are many legal instruments related to cyber-laundering, however they often rely on money laundering and counter-terrorism financing offences.

Other international policies concern cyber-laundering activities, including: the 2006 Anti-Money Laundering and Counter-Terrorism Financing Act [6]; the Bank Secrecy Act [7]; the 2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act [8]; the International Convention for the Suppression of the Financing of Terrorism [9]; the 2020 Lawful Access to Encrypted Data (LEAD) Act [10]; and the 2001 USA PATRIOT Act [11].

The OECD Financial Action Task Force's work carry a great importance in the fight financial crimes. Their main recommendations related to cyber-laundering are the following:

- 2013 Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments, and Internet-Based Payment Services [12];
- 2014: FATF report: Virtual currencies. Key definitions and potential AML/CFT risks [13];
- 2015: Guidance for a Risk-Based Approach to Virtual Currencies [14];
- 2019: Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers [15]; and
- 2021: Revised 2019 Guidance on Virtual Assets and Virtual Asset Service Providers [16].

## 7. Privacy concerns

Data protection remains a key problematic in the anti-money laundering detection process. Various cyber-laundering methods are hard to keep track of, since each transaction cannot be recorded, as it would undoubtfully cost providers too much time, money, and data storage. While the level of recordkeeping of transactions and of ownership is important for the law enforcement process, detailed recordkeeping will most of the time decrease customer acceptance, because of privacy concerns.

The Financial Action Task Force 2019 "travel rule", requires "to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting Virtual Assets transfers" [17]. However, a few recent regulations raise questions about recordkeeping's privacy concerns. Data protection laws considerably differ in various jurisdictions. For example, the European Union General Data Protection Regulation [18] has significant requirements to protect the privacy of EU persons. It requires compliance with safeguards for the protection of personal data from "technology enabled EU financial marketplace". There is also potential for conflict with other laws such as the CLOUD Act [19].

## 8. Jurisdiction

In some jurisdictions, the degree of regulation varies depending on the type of online financial service provided. Whereas in other jurisdictions, the same services are simply not regulated. There can be regulated and unregulated entities. Providers are not necessarily required to obtain a license or register for the provision of certain financial online services in some countries. As a result, there are no legal money-laundering reporting requirements for such providers in these jurisdictions. Therefore, criminals often privilege the most advantageous forum. Such regulatory gap creates

loopholes which lead to unlawful behaviors, while making it difficult to investigate and prosecute cyber-laundering.

## 9. Law enforcement

Several cyber-laundering law enforcement issues have emerged. First, as the current enforcement mechanism relies on defined financial and geographic borders, determining competent jurisdictional authority in the case of financial cybercrime can be a difficult task. Second, existing supervisory regulatory regimes constantly require revision for each known or new typology, since technology is in perpetual evolution. Third, the speed and volume of online transactions make it difficult to identify and find felons. Fourth, it is complicated to ensure accurate and adequate records of the transactions and persons involved. Last, stored value cards are clearly more difficult to detect and track than physical currency.

## 10. Recommendations

In this chapter, we have seen numerous regulatory issues regarding online financial crimes. Recalling that several factors work in the favor of criminals, such as the anonymity provided by the internet, the asymmetry in regulations, and the lack of adequate legal obligations for online financial service providers. To further complicate matters, many online funds services are covered by privacy regulations such as which make it complex for governments to uncover details of transactions if users do not allow access.

In an attempt to fill these legal loopholes, various recommendations will now be issued:

First, governments should prohibit the cryptocurrency exchanges they regulate from clearing and settling transactions with unregulated exchanges.

Second, regulators should prohibit exchanges from buying and selling cryptocurrencies that are explicitly designed to evade controls.

Third, anti-money laundering verification and reporting requirements should be enhanced concerning prepaid cards, crypto ATMs, marketplaces, and crypto mining operations.

Fourth, there is a clear need to extend the classification of virtual asset service providers to other online activities, in order to extend the scope of actual legislations.

Last but not least, governments need to elaborate privacy and data sharing laws that are in adequacy with the detection and reporting of online financial crimes.

## 11. Conclusions and Problematics

Since the internet is designed to work internationally, it provides criminals the means to operate worldwide, using multiple currencies. The diminishing of international financial borders creates an additional challenge for law enforcement, as it makes it difficult to determine jurisdictional authority. Traditional law enforcement techniques and methods have therefore become less effective or even obsolete.

Moreover, there are presently too few statutes and regulations focusing on cyberlaundering matters, and they also rely on defined financial and geographic borders. Governments must then take into account the latest technological developments, along with cultural and cross-jurisdictional regulatory issues, while building new money laundering policies. Law enforcement, regulatory agencies, and the private sector clearly have a part to play in the policy-making process. They must get together to discuss issues of mutual concern, and develop effective and reasonable measures to prevent and detect online financial crimes without impeding the commercial and consumer advantages of new technologies.

Enhance cooperation and coordination efforts among nations are necessary to ensure that policies and standards to fight cyber-laundering activities are consistent with the actual threats encountered. To effectively investigate financial cybercrimes, and trace questionable electronic fund flows, regulators and law enforcement authorities require new tools and techniques. There is also a great need to find the appropriate balance between an individual's right to financial privacy and the legitimate need of law enforcement and regulatory authorities to prevent and detect crime.

**References**

[1]. Financial Action Task Force - FATF, (2012-2020). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, [online]. Available: www.fatf-gafi.org/recommendations.htm.

[2]. Financial Action Task Force - FATF, (2012-2020). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, [online]. Available: www.fatf-gafi.org/recommendations.htm.

[3]. Financial Action Task Force - FATF, (2020). Money laundering and terrorist financing. Red flag indicators associated with virtual assets [online]. Available: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.

[4]. 5AMLD, (May 30, 2018). Directive (EU) 2018/843 of the European Parliament and of the Council, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, Official Journal of the European Union, 156, 43-74 [online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843.

[5]. 6AMLD, (October 23, 2018). Directive (EU) 2018/1673 of the European Parliament and of the Council on combating money laundering by criminal law, Official Journal of the European Union, 22-30 [online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=EN.

[6]. Australian Government, (2006). Anti-Money Laundering and Counter-Terrorism Financing Act, Canberra, [online]. Available: https://www.legislation.gov.au/Details/C2020C00362.

[7]. United States Government, (1982). Bank Secrecy Act, [online]. Available: https://www.govinfo.gov/content/pkg/USCODE-2012-title31/pdf/USCODE-2012-title31-subtitleIV-chap53-subchapII-sec5311.pdf.

[8]. United States Congress, (2018). H.R.4943.- CLOUD Act, [online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/4943.

[9]. United Nations, (1999). International Convention for the Supression of the Financing of Terrorism, [online]. Available: https://www.un.org/law/cod/finterr.htm.

[10]. US Congress (2020). S.4051 - Lawful Access to Encrypted Data Act, [online]. Available: https://www.congress.gov/bill/116th-congress/senate-bill/4051?r=1&s=1.

[11]. United States Government, (2001). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, [online]. Available: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf.

[12]. Financial Action Task Force - FATF, (2013). Guidance For a Risk-Based Approach: Prepaid Cards, Mobile Payments, and Internet-Based Payment Services, the Financial Action Task Force (FATF), Paris, France, 1-47, [online]. Available: https://www.fatf-

gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf, accessed on April 7, 2021.

[13]. Financial Action Task Force - Financial Action Task Force - FATF, (2014). FATF report: Virtual currencies. Key definitions and potential AML/CFT risks [online]. Available: https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html.

[14]. Financial Action Task Force - FATF, (2015). Guidance For a Risk-Based Approach: Virtual Currencies, the Financial Action Task Force (FATF), Paris, France, 1-48, [online]. Available: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

[15]. Financial Action Task Force - FATF, (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, the Financial Action Task Force (FATF), Paris, France, 1-59, [online]. Available: www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html.

[16]. Financial Action Task Force - FATF, (2021). March, Draft updated Guidance for a risk-based approach to virtual assets and VASPS, FATF/PDG (2020)19/REV1, Sixth draft - Public Consultation. FATF, Paris, France.

[17]. Financial Action Task Force - FATF, (22 February 2019). Public Statement - Mitigating Risks from Virtual Assets, FATF, [online]. Available: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html.

[18]. European Union, (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679).

[19]. US Congress, (2018). H.R.4943.- CLOUD Act, [online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/4943.

# Cyber-Attacks Identification and Measures for Prevention

**Shubham CHOPRA[1], Hitesh MARWAHA[2], Anurag SHARMA[3]**
Faculty of Computational Science, GNA University, Phagwara, Punjab, India
[1] shubham.chopra@gnauniversity.edu.in
[2] hitesh_marwaha@gnauniversity.edu.in
[3] anurag.sharma@gnauniversity.edu.in

**Abstract**

*In the present digitization era, almost everything is available online, at just one click away from us, which offer a lot of opportunities, like saving a lot of time, but also many challenges, due to the existence of many cyber-attacks, more complex and difficult to be detected. The cyber-attacks effects can be data theft, modification, or alteration. In recent time, cybersecurity is very important also in the academic field, because schools and universities systems are connected online. To protect our data from various attacks, cybersecurity plays the most important key role. Cybersecurity helps in ensuring the safety of data, personally identifiable information, and intellectual property. Cybersecurity is not only for individuals, a specific group or organization, but it is for all the people and for the government to keep data integrity, confidentiality, and availability. This paper presents the cybersecurity concept, analyzing different cyber-attacks and the specific preventions measures.*

**Index terms:** cyber-attacks, cyber-threats, cybersecurity, prevention measures

## 1. Introduction

The whole world is leading towards IoT (Internet of Things). Everything becomes digital from maintaining a student academic records to paying online to life saving equipment and everything which is on the Internet is not secured from the cyber criminals. They use different tricks to get access in our systems to steal personal and financial details of users without getting into the knowledge of the victim.

Cybersecurity comes into play because we need to protect the systems, networks, devices, and data from the cyber-attacks. Everyone which is connected to the internet needs cyber security because all records of information is stored digitally and the cyber-attacks aim to exploit common vulnerabilities, in order to compromise the computer systems. The cyber criminals have ample motivation - there's a lucrative market for the sale and exploitation of the data.

Cybersecurity refers to the protection of data from the external resources present in the network or internet. In other words, cybersecurity is the practice to defend the critical systems, servers, networks, data from malicious attacks carried out by some unauthorized persons such as cybercriminals, hackers, spammers.

The cybersecurity concerns with the 3 basic concepts:

- **Confidentiality** - It refers to when data or information is read or copied by someone who is not authorized to do so that leads to "loss of Confidentiality". Example: military secrets.

- **Integrity** - It refers to when data or information has been changed or being modified by someone who is not authorized to do so that leads to “loss of Integrity”. Example: a user entering incorrect data into the database.
- **Availability** - It refers to when data or information is not been available to the authorized person to access it or the data or information is destroyed by unauthorized person so that the authorized person can not access it that leads to “loss of Availability”.

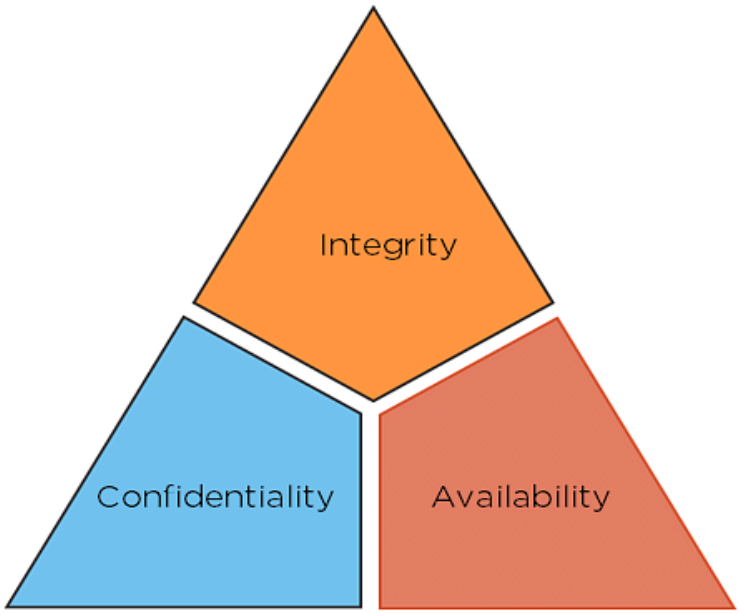



**Fig. 1.** C-I-A triad [1]

Increase in the cyber-attacks and data breaches no one is remain untouched with this problem as of now it's the era of digitalization everything is known available online and especially due to pandemic also, we have to shift physical to digital or virtual. Individuals, governments, for-profit companies, not-for-profit organizations, and educational institutions are all at risk of cyberattacks and data breaches and In the near future, the number of attacks will grow as digital technologies evolve so as to protects all categories of data from theft and damage which includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems. It is no longer a question that "when a cyber-attack will occur" and with the advancement in the techniques of cyber-attacks antivirus software or firewalls are not much the efficient to protect us from these attacks. This is why cyber security is much needed and is of such great importance.

## 2. Cybersecurity threats and their prevention

Malware refers to a variety of forms of malicious software’s or malicious code that include viruses, trojans, spyware, adware, botnet, ransomware or can be in any executable form or in an active web content such as animated GIF’s, embedded object. So that they are used to disrupt or damage or hijack the resources or assets or system of a authenticated user. In other terms these are inserted into a system which used to compromise the so-called C-I-A triad. Malware can be distributed by various ways such as [2]:

- Email attachment.
- Fake internet ads.
- Infected application software’s or websites.

### 2.1. Phishing

Phishing refers to cyber-attack that uses disguised email as a weapon. It pretends to be the entity, person or company you often used to deal with it generally. The goal of this is to forcefully believe the recipient into believing that the information or message is needed or wanted by the recipient and by clicking it leads to download malware which helps the attacker to get an access into the infected person systems information.

Phishing is a form of fraudulent activity with the motive to steal personal and financial details of a user, which is usually done through email which seems to be from a legitimate or reputable source. The attacker tries to be the part of that organization or provides you a cloned website of a Company or organization from which the user wants to communicate or for getting services or something else. Usually, it is difficult for the user to distinguish between the genuine one and the cloned one which is going to be used by the attacker to trap the target user. There are some steps used for phishing attacks which is used by the attacker to obtain information from the target user [3]:

- Planning.
- Compose Fraudulent email.
- Attack the target.
- Gather Credentials.
- The End Game.

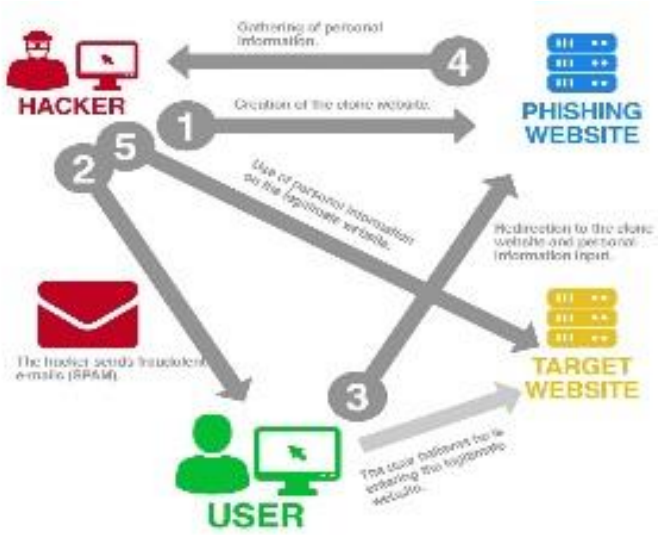



**Fig. 2.** Phishing attack mechanism [4]

**Planning** - The attacker starts with the Planning game here "game" refers to make a spoof of a legitimate or reputable website from where the attacker gathered the user's or target's credentials or information. It becomes difficult for the target to distinguish between the spoof and legitimate and genuine website and here the target gets trapped first.

**Compose fraudulent email** - As shown above in the figure 2, the attacker (Phisher) then composes a fraudulent email with the help of spoof website used for phishing. The Email is composed in such a way that it seems legitimate to the target.

**Attack the target** - The next step is to attack the user, as we mentioned earlier that it becomes difficult for the target to distinguish between the spoof and legitimate and genuine website the target tends to open the email which contains the link of the phisher phishing website.

**Gather credentials** - After being redirected to the phishers phishing website. The target user enters the login credentials on that website which automatically provides the same credentials to the

phisher (attacker) also. Unknowingly the target user takes the bait and just gone through the data theft.

**Accessing information** - In this last step the phisher (attacker) using the data obtained from the phishing website logins to the official target website and now can access all the information of the victim or targeted user. The attacker can also sell the login credentials or the obtained information of the target user or victim on the Dark web.

**Anti-Phishing Techniques**

Anti-phishing is a service or technique that helps to prevent unauthorized access to secure information of a specific individual, Organization or Business. In other words, it is the efforts of blocking the Phishing attacks. Various Anti phishing applications are available to check whether the website is safe or legit on behalf of user. It can be integrated into the Web browser also. In general, anti-phishing techniques can be classified into following four categories [5].

- Content Filtering- In this methodology content/email are filtered as it enters in the victim's mailbox using machine learning methods, such as Bayesian additive Regression Trees or Support Vector Machines.
- Blacklisting- Blacklist is collection of known phishing Web sites/addresses published by trusted entities like Google's and Microsoft's blacklist. It requires both a client & a server component. The client component is implemented as either an email or browser plug-in that interacts with a server component, which in this case is a public Web site that provides a list of known phishing sites.
- Symptom-Based Prevention- Symptom-based prevention analyses the content of each Web page the user visits and generates phishing alerts according to the type and number of symptoms detected.
- Domain Binding- It is a client's browser-based techniques where sensitive information is bind to a particular domain. It warns the user when he visits a domain to which user credential is not bind.

## 2.2. SQL Injection

A SQL injection is a cyber-attack which usually deals in stealing or damaging the data present in the database by using malicious Structured Query Language (SQL) statement which can used to retrieve the content of entire database or can also be used to add, modify or delete records in the database.

The attacker finds that whether the webpage or web application uses SQL databases such as MySQL, Oracle, SQL server and after that exploit the vulnerabilities by injecting malicious SQL statements. After that the attacker searchers for the vulnerable user inputs within a web application or webpage of which the attacker uses such inputs and can also create input content which is known as malicious payload which plays a significant role in the overall attack performed which is then the content or so-called malicious payload executed in the database. There are several types of SQL injection attacks such as [6]:

- In-band SQLi.
- Blind SQLi.
- Out-of-band SQLi.

```
# Define POST variables
uname = request.POST['username']
passwd = request.POST['password']

# SQL query vulnerable to SQLi
sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" + passwd + "'"

# Execute the SQL statement
database.execute(sql)
```

**Fig. 3**. SQL Injection statement [6]

**Prevention of SQL Injection attack**

The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The developer must sanitize all input, not only web form inputs such as login forms. Turning off the visibility of database errors on your production sites can also be a good idea.

If you discover an SQL Injection vulnerability you can use a web application firewall to sanitize your input temporarily. There are certain Primary defenses options available that should be followed to prevent SQL Injection [7]:

- Option 1: Use of Prepared Statements (with Parameterized Queries).
- Option 2: Use of Properly Constructed Stored Procedures.
- Option 3: Allow-list Input Validation.
- Option 4: Escaping All User Supplied Input.

### 2.3. Man in the middle (MITM)

Man in the middle cyber threat refers to intercept the communication of the two authenticated user or while the user communicating or requesting resource or information from server so that to steal data or information also the attacker may filter the data. As the attacker is present unknowingly in the middle of the communication.

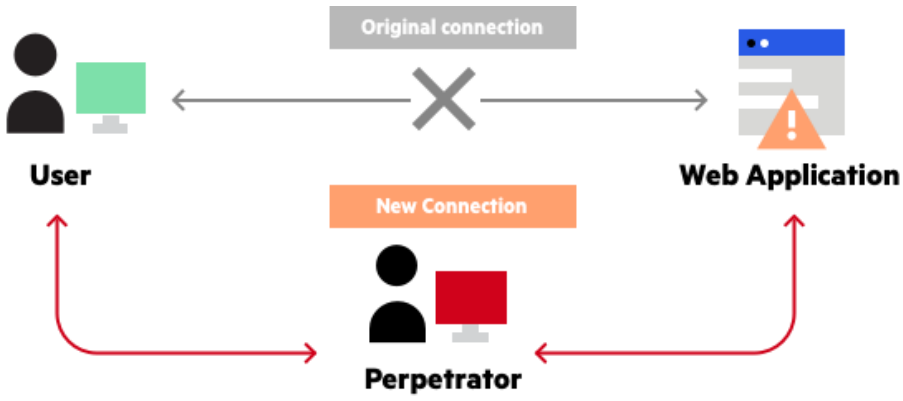



**Fig. 4.** Man-in-the-middle attack mechanism [8]

A successful MITM attack involves two specific phases: Interception and Decryption [9].

**Interception phase**

This phase deals with that how the attacker inserts themselves as the "man-in-the-middle". As the attacker intercepts the users original or legitimate network traffic with the fake network traffic before it reaches to its intended destination. It is frequently done by creating a fake open Wi-Fi network or when a user connects to an open public Wi-Fi.

Once the attacker inserts themselves successfully then may choose a technique from a variety to get further with the attack:

- IP spoofing involves an attacker altering the IP packets by disguising himself.
- ARP spoofing involves use of forged ARP message to link attackers MAC address with the target's legitimate IP address.
- DNS spoofing also known as DNS cache poisoning involves an attacker altering or infiltrating a DNS server so that the target web traffic gets redirected to the attacker's fake website.

**Decryption phase**

After the Interception the decryption phase comes in to play as a MITM attack doesn't stop here, as in this phase the attacker which has the target's encrypted data after gaining the access now need to be decrypted so that the attacker is able to read it and use it. For decrypting the data any method can be adopted by the attacker:

- HTTPS Spoofing is a method which makes the target to believe that the certain website is safe and authenticated when it's not by sending the fake certificate to their browser.
- SSL Hijacking involves the attacker passing a forged authentication keys to both the user and application during TCP handshake and pretending to be a secure connection which is not and the entire session is in control of the so called "man-in-the-middle (attacker).
- SSL Stripping involves the attacker downgrading a user secure HTTPS connection to unsecure HTTP version of the website while the secure connection to the secure website is maintained by the attacker.

**Prevention of MITM**

Some measures aimed to prevent MITM attacks are [10]:

- Avoid Wi-Fi networks that aren't password protected and never use a public Wi-Fi network when dealing with some sensitive personal information.
- Use a Virtual Private Network (VPN).
- Log out of sensitive websites such as banking websites.
- Use multifactor authentication.
- Use a firewall to for a secure connection.
- Use antivirus software to protect your devices.

## 3. Cyber Security Tips and Best practices

Ensuring cybersecurity and remain protected from cyberattacks is challenging, however. It's difficult to keep up when cybercriminals are persistently looking for new ways to expose security risks. Still, there are a number of ways to ensure cybersecurity are as follows [11]:

**Keep software up-to-date**

Software companies typically provide software updates for 3 reasons: to add new features, fix known bugs, and upgrade security. Always update to the latest version of your software to protect yourself from new or existing security vulnerabilities.

**Avoid opening suspicious emails**

If an email looks suspicious, don't open it because it might be a phishing scam.

Someone might be impersonating another individual or company to gain access to your personal information. Sometimes the emails may also include attachments or links that can infect your devices.

**Keep hardware up-to-date**

Outdated computer hardware may not support the most recent software security upgrades. Additionally, old hardware makes it slower to respond to cyber-attacks if they happen. Make sure to use computer hardware that's more up-to-date.

**Use a secure file sharing solution**

The files you share are only as secure as the tools you use to share them with. Adopt a secure file sharing solution to encrypt your files while they're in transit and at rest to prevent unauthorized access and keep your files safe.

**Use anti-virus and anti-malware**

As long as you're connected to the web, it's impossible to have complete and total protection from malware. However, you can significantly reduce your vulnerability by ensuring you have an anti-virus and at least one anti-malware installed on your computers.

**Use VPN for a secure connection**

For a more secure and privatized network, use a virtual private network (VPN). It'll encrypt your connection and protect your private information, even from your internet service provider.

**Creating strong passwords and change it frequently**

Put more effort into creating your passwords. You can use a tool like howsecureismypassword.net to find out how secure your passwords are.

**Enable 2-Factor Authentication**

Many platforms now allow you to enable 2-factor authentication to keep your accounts more secure. It's another layer of protection that helps verify that it's actually you who is accessing your account and not someone who's unauthorized. Enable this security feature when you can.

**Remove adware**

Adware collects information about you to serve you more targeted ads. It's best to rid your computer of all forms of adware to maintain your privacy. Use adware cleaner tools to clean adware and unwanted programs from your computer.

**Double check for HTTPS on websites**

When you're on a website that isn't using HTTPS, there's no guarantee that the transfer of information between you and the site's server is secure. Double-check that a site's using HTTPS before you give away personal or private information.

**Avoid using public networks or Wi-Fi**

When you connect to a public network, you're sharing the network with everyone who is also connected. Any information you send or retrieve on the network is vulnerable. Stay away from public networks or use a VPN when you're connected to one.

**Maintain Back up of important data**

Important data can be lost as a result of a security breach. To make sure you're prepared to restore data once it's lost, you should ensure your important information is backed up frequently on the cloud or a local storage device.

**Train employees**

The key to making cybersecurity work is to make sure your employees well trained, in sync, and consistently exercising security practices. Sometimes, one mistake from an improperly trained employee can cause an entire security system to crumble.

**Hire a "White Hat" hacker**

Not all hackers are bad. Some hackers expose security risks for the sake of helping others improve their cybersecurity by keeping them aware of security flaws and patching them. These hackers are known as "white hat" hackers. It might benefit you to hire one to help you find risks you never knew you had.

## 4. Conclusion

As of now everything is somehow connected to the internet cyberattacks are increasing at an alarming rate which is a serious matter of discussion and specific prevention steps should be taken from individual as well as from the government side also by implementing or making new laws for ensuring the safety of public as well as government sensitive information. One of the most important reasons for the occurrence of these attacks are lack of adequate knowledge about the cyber security. No one wants to accept that they are the victim of these attacks or breaches not even government or any other industry as it will present a bad image in front of public which raises a question in their mind that even they are not protected so how they will protect us, protect our sensitive information.

This study shows the steps for identifying a cyber-attack, techniques used by cyber criminals to get access in systems and how we can prevent or protect our computer systems. The motive of this paper is to provide an idea and create awareness, for whom security of their network or information is the key aspect.

## References

[1]. https://www.simplilearn.com/ice9/free_resources_article_thumb/cia_triad.png.
[2]. https://blog.netwrix.com/2020/06/12/malware-prevention/.
[3]. Shankar, A., Shetty, R., & Nath, B. (2019). A review on phishing attacks. International Journal of Applied Engineering Research, 14(9), 2171-2175.
[4]. https://www.swascan.com/swascan-phishing-simulation-attack/.
[5]. Gaurav, Madhuresh Mishra, Anurag Jain, "Anti-Phishing Techniques: A Review", International Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 2, Issue 2, Mar-Apr 2012, pp. 350- 355.
[6]. https://www.acunetix.com/websitesecurity/sql-injection/.
[7]. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html.
[8]. https://www.imperva.com/learn/wp-content/uploads/sites/13/2017/09/man-in-the-middle-mitm-attack.png.
[9]. https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/.
[10]. https://www.pandasecurity.com/en/mediacenter/security/man-in-the-middle-attack/.
[11]. https://www.titanfile.com/blog/cyber-security-tips-best-practices/.

# Analysis of Online Marketplace Scams

**Mihai COTITU**
General Inspectorate of the Romanian Police, Crime Research and Prevention Institute,
Research Department, Bucharest, Romania
mihai.cotitu@politiaromana.ro

**Abstract**

*One of the many effects of the Covid-19 pandemic was reflected in the accelerated migration of many face-to-face activities towards the online environment, with online trading experiencing a significant growth during this period. At the same time, the risks specific to the digital environment have gone through a prosperous period. Thus, a telling example is given by the period August - December 2020, during which, at the level of the relevant authorities (D.I.I.C.O.T. and the Romanian Police) were registered approximately one thousand cases, based on cybercrime with similar modus operandi. These cases involved the collection of personal data through online resources, phishing, targeting in particular those who posted advertisements for the sale of objects through the OLX platform.*

**Index terms:** classiscam, cybersecurity, marketplace, scam, WhatsApp

## 1. Introduction

The current paper aims to describe a recent type of online scam that has occurred through online marketplaces, the methods used by the perpetrators and the ways victims were deluded, the final goal being to support and to prevent future offences. This research is based on the analysis of online marketplaces posts/ announcements and interviews with police officers.

In comparison with previous scams carried out through the Internet, in which case perpetrators targeted people seeking for goods/acquisitions, therefore potential clients, a new practice among the scammers was identified recently: victims were selected from the sellers, people seeking to sell a product through an online marketplace.

In close connection with this reverse action (the perpetrator being the supposed customer/ buyer) the modus operandi is characterized by the eagerness to purchase and the lack of attention paid to the details of the good for sale. No details on the object of the transaction are required and no attempt is made to negotiate its value. Even if such requests (the reason for the sale, the request for a lower price) were made, they are rather of complacency and are limited to a single exchange of a limited number of inquiries.

## 2. How it works

It should be noted that the negotiation between the two parties, in order to complete the transaction, occurs mainly or exclusively outside the dedicated chat platform of OLX[1], on communication channels such as WhatsApp or using a classic phone call. Another peculiarity of these

[1] OLX is an online platform (marketplace) dedicated to buying and selling goods and services.

cases is the rather accurate depiction of the marketplace, which might seem authentic to a regular internet user or to a person who does not pay particular attention to safety details. Thus, after the discussion, the victim was offered a link, apparently similar to those generated by the portal that we already mentioned, in which he or she filled in the data written on the card in order to, hypothetically, receive the money for the good that was being sold. It should be noted that these steps are abnormal for a sale, and are also an indicator of a low-level of knowledge regarding online transactions. In a brief period of time, usually immediately after the data was disclosed, the bank account connected to the card was emptied, either in multiple steps or in a single transaction. Moreover, these transactions do not attract the attention of the banks. Confronted with the requests to not validate the transactions on behalf of the victims, the banks would often refuse to block them, claiming there is no ground for the request unless a criminal investigation is open. The banks consider the victims willingly provided their data, and that is why the request does not represent a reason for blocking transactions. A new indication of the technological capacity of the perpetrators is given by the possibility of the latter to carry out the operation even if there is security solutions such as the 3D-secure code, without it being disclosed by the victim, but only issued for the purpose of the transaction. Please note that, in some cases, as a preliminary step to better aiming their criminal activities, the victims were being asked in advance for information regarding the balance available into the account.

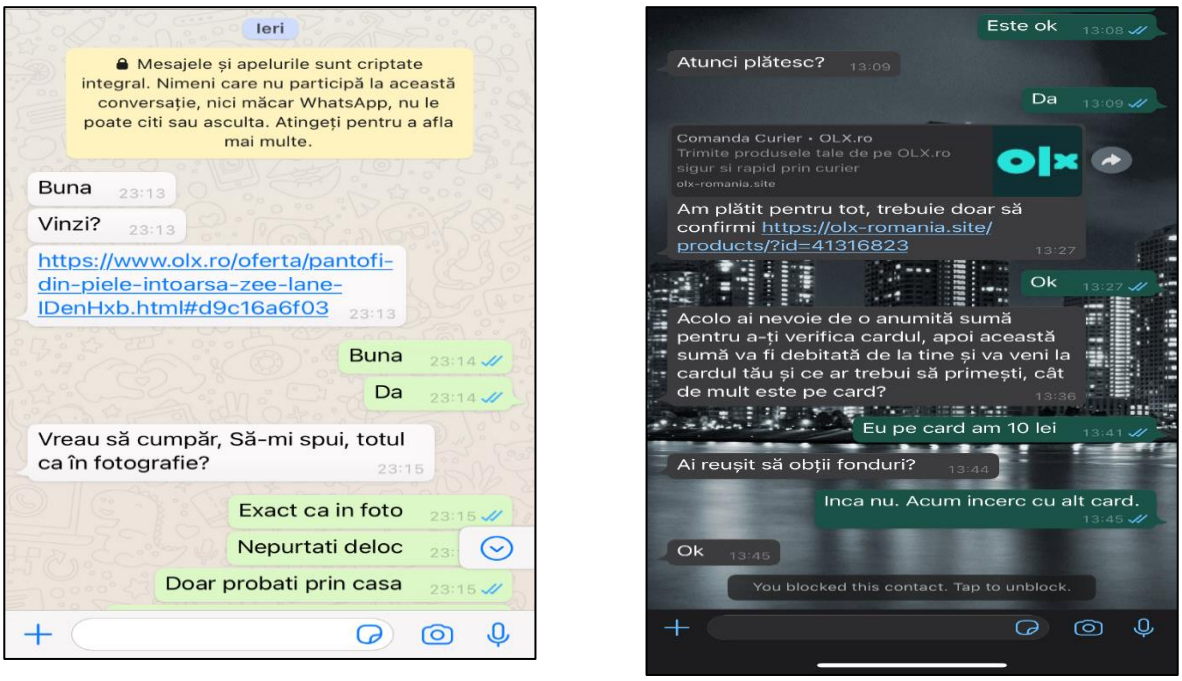



**Fig. 1**

As police workers also pointed out, the use of the previously mentioned channels (WhatsApp, classic call) makes the investigative steps more difficult. Moreover, criminals have the IT technique that allows the systematic alternation of telephone numbers through software that generate quickly random new numbers, beyond the simple method of purchasing and then disposal of pre-paid cards. Under these terms, the details regarding the author vary from file to file, the interception or location measures (geographical tracking) being either difficult to justify or imprecise, inconclusive.

The elements that may indicate the presence of organized crime cells are highlighted by situations in which the perpetrators have used classic telephone calls to contact the victims, on the opposite side of the call being a person who either tried to give the impression of the same nationality as the victim or had some training/practice to achieve this goal. Such a scenario may indicate the

willingness of criminals to gain some prior knowledge, or their ability to engage other people and hire collaborators. Therefore, the pecuniary benefits of this method, which allows payment to third parties, are also deducted. The use of the phone call was highlighted during the interviews with police officers, coming into contradiction with the previous elements that we had until then, that this type of offence is usually committed by foreign criminals. Previously, it was known that they preferred to communicate exclusively via WhatsApp, the language used not having the usual conversational fluency, indicating the possible use of an automated translation tool.


**Fig. 2**

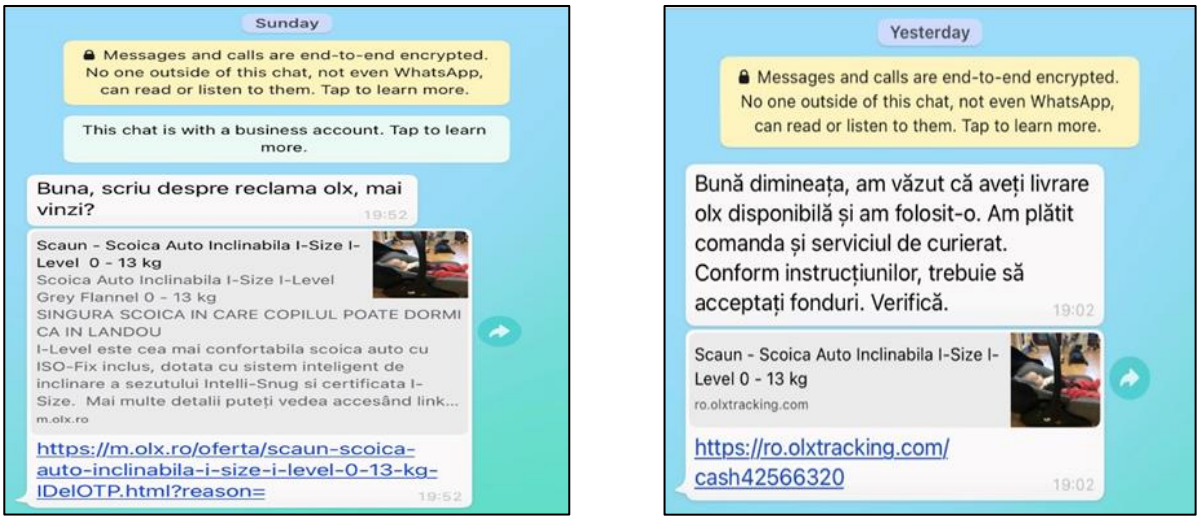



**Fig. 3**

Starting from this point, we cannot pass over the main weak spot of this equation: the victim and the need to inform her regularly about a minimum set of rules regarding online transactions, as well as about other undersupplied safety measures that users should adopt in order to have a positive online experience, highlighted by the investigative structures involved in resolving these cases (collaboration with the police, providing personal data). In educating the general public and in close connection with the perception of the state authority, we reiterate that, in some cases, the victims initially address CERT-RO, and the banks, but regarding the notifications submitted to police officers authorized to investigate these types of offences, they are reluctant to provide the data necessary for investigative activities and refuse to give out personal information, therefore they do not meet the requirements of Ordinance 27/2002 (on the regulation of petition settlement activities) or of the Order 33/2020 (on petition settlement activities, audience and counselling of citizens in the Ministry for Internal Affairs) and their notifications can be considered null, even though the initial form contains only some simple fields that are mandatory for the investigation to start.

In addition to the data presented above, as some users have reported their experiences in the online environment, new elements can be mentioned, such as:

- Scanning a QR code for the transaction, an action that does not involve forwarding the money to the seller, but giving up the value targeted by him;

- Payment already made by the alleged purchaser followed by the generation of a link in which the seller receives a confirmation that the requested amount of money has been transferred, but he is conditioned by the payment of a shipping fee;


**Fig. 4**

- The mentioning of another trading currency in the false link (e.g. rubles);

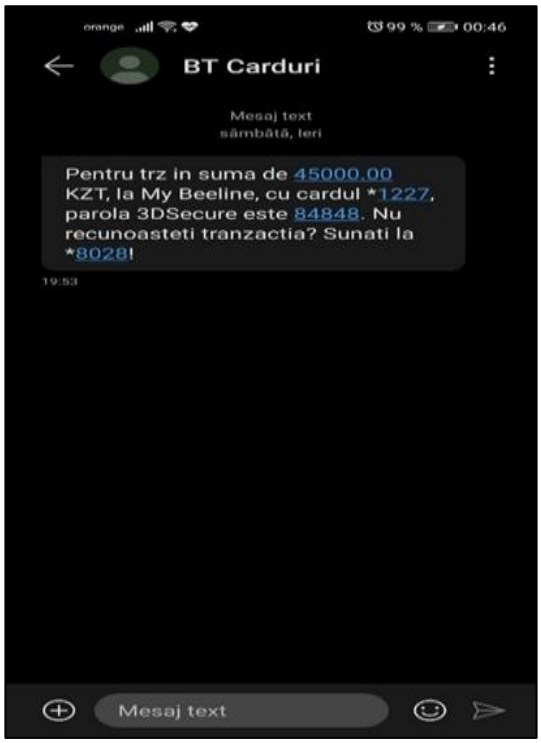



**Fig. 5**

- Being redirected to an alleged link belonging to a courier company;

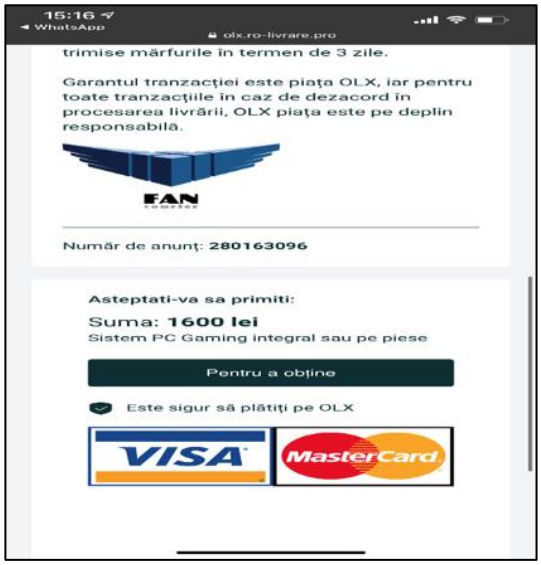
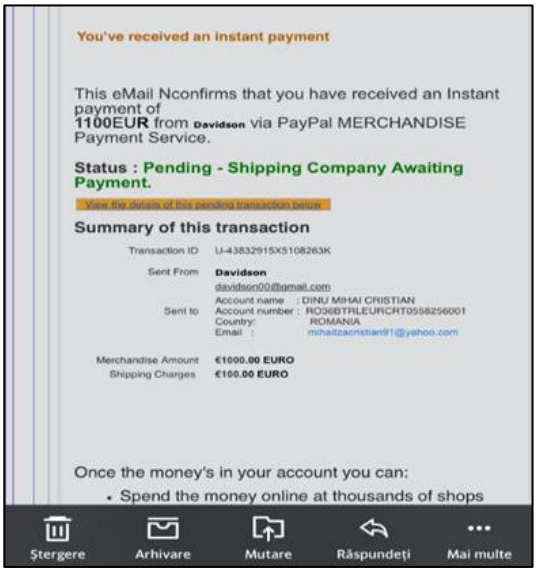



**Fig. 6**

- In order to create the impression of authenticity, in some cases, e-mails are sent imitating the brand elements of online payment companies.



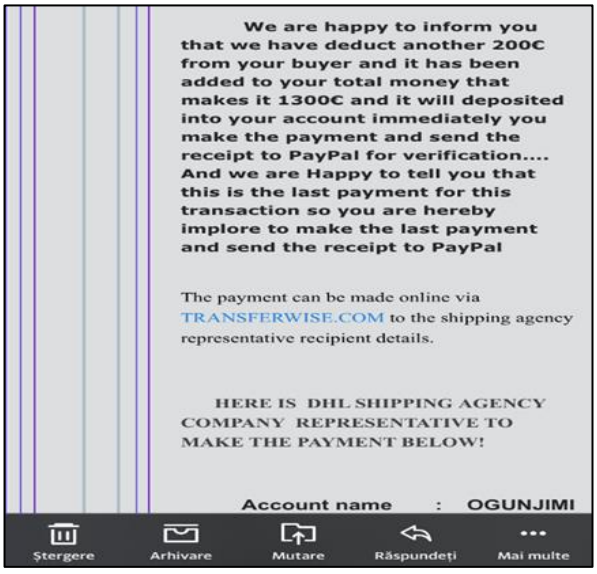




**Fig. 7**

Thus, in a predictive sense, these situations may be relevant for the possible variation of the scammer's way of action in the next period. CERT Poland issued warnings about ad platforms, through which text messages were issued to sellers prompting them to accept money. In fact, once approved, the money was being transferred to the offender's account, the operation being subsequent to the disclosure of card data. Returning to the national level, there is a reaction from the public to this scam, by posting on the targeted websites messages in which they would reveal their experiences with this type of scams and the people involved.

Focusing on the external context, even though the group that owns the OLX platform operates in several countries, national investigators did not receive information on similar cases from their

external counterparts. At the same time, they anticipate a perpetuation of phishing attempts, by using different platforms.

Comparing a series of online articles on similar topics, we find that similar practices have been encountered in other European countries (such as France, Poland, Bulgaria) as well as in much faraway countries (e.g. India). In the case of Poland, we can even speak of an overlap of the intensity of the facts, given the fact that the local branch of CERT issued a similar warning for the same platform, in October. This warning message also referred to a new method, in the way of issuing to the seller an alleged message approving the transaction, which in fact represented an agreement to withdraw that amount.

During the desk research, other reports indicated that there were more than 40 groups, especially from Russia, specialized in crimes involving the theft of personal data, especially banking data. Moreover, these reports issued a warning about the increase of these types of crimes, in parallel with the emergence of a new way of scamming, through false advertisements, a scam-as-a-service scheme. The presence of the attacks has been reported in a much larger number of countries, on a wider range of trading platforms.

Looking at the technical aspects of such crimes, the reports indicates that most offenders are based in Russia. After moving the conversation to another communication service (Telegram, WhatsApp) they use bots (programmed systems that can take over certain predefined tasks) to lead the victim to a link that mimics the format of certain websites, online marketplaces or delivery services, link necessary to take over bank credentials.

The method called Classiscam, involves an automated scam with the purpose of stealing money and bank credentials. They mainly use the portals or providers that are very popular on an international scale, such as: Leboncoin, Allegro, OLX, FAN Courier, Sbazar etc.

Specialists have identified about 40 groups of Russian origin using this technique, of which 20 operate in Bulgaria, the Czech Republic, France, Poland, Romania, the United States and in other states of the former Soviet Union, while another 20 groups focus strictly on Russia. According to estimates, their income was $ 6.5 million in the previous year, with an average per victim of $120, about $61,000 a month for each group, or a total of about $522,000 a month. In Russia, this type of scam was initially identified in the summer of 2019, but the peak was recorded in the spring of 2020, with the online migration of many activities. If 280 fake links were removed in the summer of 2020, the number grown to around 3,000 in December.

However, it is indicated that these attacks in Eastern and Western Europe are still in their infancy. In a predictive way, we can say that in the future, criminals will not rely heavily on "fake buyers" scenarios. Using the same portals, they will publish attractive ads (bait), displaying various electronics, and in order to create the illusion of authenticity, they will use phone numbers adapted to the local specifics of each country.

From an organizational point of view, the groups have a pyramidal hierarchy, headed by "administrators", followed by members who are dealing with recruitment, creating false links and managing some of the banking problems.

## 3. Keeping up with it

Over time, either through systematic progress or under the need to identify solutions in crisis situations, digitalization is becoming an integral part of several areas of our day-to-day activities.

Beyond acquiring these new ways of interacting with the online world, it is imperative to know the set of rules that will guide these new behaviours. In relation to/Regarding the online transactions

and the services provided by different online platforms, a collective approach is required both from the institutions involved in the investigation of these types of offences and from the private institutions whose clients or users may be affected.

Preventive measures are all the more necessary as, even if at the level of General Police Inspectorate of Romania there is a unit that manages this form of crime, at the territorial level the resources - from IT to the human one - are drastically limited.

These limitations place a favourable position, both in terms of accessibility and efficiency, of an information-awareness campaign carried out with the efforts of several actors, both from the private and public/state field.

**References**

[1]. I. Arghire, "Telegram-Based Automated Scam Service Helps Fraudsters Make Millions", securityweek.com, https://www.securityweek.com/telegram-based-automated-scam-service-helps-fraudsters-make-millions (Accessed on 20.02.2022).

[2]. "Classiscam expands to Europe: Russian-speaking scammers lure Europeans to pages mimicking classifieds," https://www.group-ib.com/media/classiscam-in-europe/ (Accessed on 18.02.2022).

[3]. J. Espinoza. "Digital payments deepen the threat of online fraud in Covid era". https://www.ft.com/content/d56bdbbb-f7f3-4b44-98c3-e1a372ed2280 (Accessed on 20.02.2022).

[4]. "Gang arrested for fraud on Olx: Everything you need to know about this 'big scam' while using Olx, Quikr". https://www.gadgetsnow.com/slideshows/gang-arrested-for-fraud-on-olx-everything-you-need-to-know-about-this-big-scam-while-using-olx-quikr/the-moment-you-post-your-ad-on-olx-or-quikr-you-will-get-a-call-from-a-prospective-buyer-in-many-cases-almost-immediately/photolist/75783800.cms (Accessed on 20.02.2022).

[5]. J. Jay. "Russian-speaking scammers tricking European shoppers using scam sites". teiss.co.uk. https://www.teiss.co.uk/news/russian-speaking-scammers-tricking-european-shoppers-using-scam-sites-8716 (Accessed on 20.02.2022).

[6]. H. Dugh. "Planning to sell stuff on OLX, Quikr? You might be cheated by fraudsters - Don't make these mistakes" https://www.zeebiz.com/personal-finance/news-planning-to-sell-stuff-on-olx-quikr-you-might-be-cheated-by-fraudsters-dont-make-these-mistakes-109014 (Accessed on 18.02.2022).

[7]. "Rising OLX fraud major concern for Gurugram Police" https://www.andhram.com/national/rising-olx-fraud-major-concern-for-gurugram-police/ (Accessed on 21.02.2022).

[8]. R. Jain. "Scammers are now using WhatsApp to steal money - here's how you can protect yourself". https://www.businessinsider.in/tech/apps/news/scammers-whatsapp-stealing-money-how-to-protect/articleshow/72976604.cms (Accessed on 20.02.2022).

[9]. "Telegram-Based Classiscam Operation Targeting Users of European Marketplaces". https://cyware.com/news/telegram-based-classiscam-operation-targeting-users-of-european-marketplaces-dd8d2183 (Accessed on 21.02.2022).

[10]. "The Mammoth Goes Abroad: Online Fraud Groups Move into the EU, US, and CIS". https://sk.ru/news/the-mammoth-goes-abroad/ (Accessed 18.02.2022).

[11]. T. Ankit. ”Don't fall prey to online scams on Paytm, WhatsApp and other popular apps”. https://www.wionews.com/Technology/Dont-Fall-Prey-To-Online-Scams-On-Paytm-Whatsapp-And-Other-Popular-Apps-337451 (Accesed on 19.02.2022).

[12]. ”Țeapă pe OLX! Cum a fost păcălită o ploieșteancă de un cumpărător din altă țară”. https://www.ziarulincomod.ro/teapa-pe-olx-cum-fost-pacalita-o-ploiesteanca-de-un-cumparator-din-alta-tara-foto/ (Accessed on 21.02.2022).

# Zero Trust Security

**Ioan-Alexandru DUMITRU**
Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest, Romania
dumitrualex2004@yahoo.com

**Abstract**

*Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, whether they are inside or outside the perimeter of the network. No specific technology is associated with the Zero Trust architecture; It is a holistic approach to network security that incorporates several different principles and technologies. The traditional security of the IT network is based on the „castle-and-moat" concept. In that model, it's hard to gain access from outside the network, but everyone on the network is trusted by default. The problem with this approach is that once an attacker gains access to the network, he has free rein over everything inside.*

**Index terms:** access management, cybersecurity, Zero Trust architecture

## 1. Introduction

Zero Trust is a network security model based on a strict identity verification process. The framework stipulates that only authenticated and authorized users and devices can access applications and data. At the same time, it protects those applications and users from advanced Internet threats.

This model was first introduced by an analyst at Forrester Research and, while not a completely new theory, has become increasingly important for modern digital transformation and its impact on the security architecture of business networks. As the modern workforce becomes more and more mobile, accessing applications from multiple devices outside the business perimeter, businesses have adopted a "check, then trust" model, which means that if someone has the correct user credentials, they are allowed on any site, application or device they request. This has led to an increased risk of exposure, dissolving what was once the company's trusted control zone and leaving many organizations exposed to data breaches, malware and ransomware attacks. Protection is now required where applications and data are located, as well as users and devices.

Users, devices, applications and data move outside the enterprise perimeter and control area. New business processes driven by digital transformation increase risk exposure. "Trust, but verify" is no longer an option, as the advanced threats are moving around the perimeter of the company [1].

Traditional perimeters are complex, increase risk and are no longer compatible with current business models. To be competitive, companies need a reliable network architecture capable of protecting enterprise data wherever users and devices are located, while ensuring that applications run quickly and seamlessly.

## 2. Zero Trust security - history and importance

The term "Zero Trust" was coined by an analyst at Forrester Research Inc. in 2010, when the concept model was first presented. A few years later, Google announced that they had implemented

Zero Trust security in their network, which led to a growing interest in adoption in the technology community. In 2019, Gartner, a global research and consulting firm, listed Zero Trust security access as a core component of Secure Access Service Edge (SASE) solutions.

More than the lack of resources, cyber security seems to be suffering from a lack of an effective approach, especially as the climate of work changes. The emergence of remote work as the norm for many companies comes with new cyber security challenges. Remote work results in less control over the organization's resources, which increases the risk of data breach. Therefore, it is more important than ever to approach cybersecurity from a risk-based perspective.

The idea of Zero Trust has gradually grown over the years, especially with the rise of SaaS and remote work. It has also become more feasible as the technologies and tools built into its framework become commonplace. Zero Trust is rooted in the belief that nothing should be trusted, whether it is online or offline. Instead, always check.

Zero Trust architecture is not a quick fix, nor is it a tool. Rather, as an aviation certification guide, it is a general framework for network security. Because trust is essential for remote teams, it is worth investigating whether eliminating this cybersecurity factor can contribute to greater protection.

## 3. Main principles and technologies behind Zero Trust security

The philosophy behind a Zero Trust network assumes that there are attackers both inside and outside the network, so no user or machine should be trusted automatically.

Another principle of Zero Trust security is access with the least privilege. This means giving users only access to what they need, such as an army general who provides soldiers with information based on their need to know. This minimizes each user's exposure to sensitive parts of the network.

Zero Trust networks also use micro segmentation. Micro segmentation is the practice of dividing security perimeters into small areas to maintain separate access for separate parts of the network. For example, a network of files that live in a single data center using micro segmentation may contain dozens of separate and secure areas. A person or program with access to one of those areas will not be able to access any of the other areas without separate authorization.

Multi-factor authentication (MFA) is also a core value of Zero Trust security. MFA simply means the need for more evidence to authenticate a user; just entering a password is not enough to gain access. A common application of MFA is 2-factor authorization (2FA) used on popular online platforms such as Facebook and Google. In addition to entering a password, users who activate 2FA for these services must also enter a code sent to another device, such as a mobile phone, thus providing two proofs that they are the ones they are claiming to be.

In addition to user access controls, zero trust also requires strict device access controls. Zero Trust systems need to monitor how many different devices are trying to access their network and ensure that each device is authorized. This further minimizes the attack surface of the network [1].

## 4. Identity and access management

According to the Verizon 2021 Data Violation Investigation Report, the use of stolen credentials of over-privileged users remains one of the biggest risks and targeting user credentials is the most favored technique of cyber-criminals. It is clear that access management on the device is outdated and insecure. A Zero Trust model provides access based on identity verification, rather than simply confirming the device. This is the idea behind multifactor authentication [2].

But Zero Trust does not stop there; It also includes continuous verification, a useful feature if a legitimate user session becomes hijacked. Zero Trust authentication is adaptive, contextual, and risk based. The most popular Zero Trust model for security authentication is the software-defined

perimeter (SDP). An SDP operates and grants access based on the need to know described above. It is already appreciated as a kind of next generation virtual private network (VPN).

Cyber security is the practice of protecting computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. It is also known as information technology security or electronic information security. The term is applied in a variety of contexts, from business to mobile computers and can be divided into several common categories.

Network security is the practice of securing a network of intruder computers, whether they are targeted attackers or opportunistic malware.

Application security focuses on keeping software and devices free of threats. A compromised application may provide access to data designed to protect you. Successful security begins at the design stage, long before a program or device is implemented.

Information security protects the integrity and confidentiality of data, both in storage and in transit.

Operational security (OPSEC) includes processes and decisions for handling and protecting data assets and is a security and risk management process and strategy, and it encourages IT and security managers to look at their operations and systems form an outside perspective. The permissions users have when accessing a network, the procedures that determine how and where and which data can be stored or shared are taken into account [3].

Disaster recovery and business continuity define how an organization responds to a cybersecurity incident or any other event that results in the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan that the organization fits into while trying to operate without certain resources.

End-user education addresses the most unpredictable cyber security factor: people. Anyone can accidentally introduce a virus into an otherwise secure system without complying with good security practices. Learning how to delete suspicious e-mail attachments, not connect unidentified USB drives, and various other important lessons is vital to the security of any organization.

## 5. The scale of the cyber threat

The global cyber threat continues to evolve at a rapid pace, with an increasing number of data breaches each year. A Risk Based Security report showed that a shocking number of more than 22 billion records were exposed as a result of 4,145 security breaches made public. Although the number is down about 5% from the previous year, the amount of compromised confidential data is the second highest since 2005.

Medical services, retailers and public entities have reported the most violations, and malicious criminals are responsible for most incidents. Some of these sectors are more attractive to cybercriminals because they collect financial and medical data, but all companies that use networks can be targeted for customer data, corporate espionage, or customer attacks [4].

As the scale of the cyber threat continues to grow, governments around the world have responded to the growing cyber threat with guidance to help organizations implement effective cyber security practices.

In the United States, the National Institute of Standards and Technology (NIST) has created a cyber security framework. To combat the proliferation of malicious code and help detect it early, the framework recommends continuous real-time monitoring of all electronic resources.

The importance of monitoring the system is reflected in the "10 Steps to Cybersecurity", provided by the UK Government's National Cyber Security Center. In Australia, the Australian Cyber Security Center (CCAA) regularly publishes guidance on how organizations can counter the latest cyber security threats.

Computer security has become an important part of computer science as it deals with identifying and searching for solutions to remove the main risks involved in accessing the virtual environment through various devices, such as computers, telephones, and mobile devices. The criteria for ensuring information security are availability and accessibility, integrity, identification and authentication, confidentiality, permanence and electronic archiving.

Availability ensures the strengthening of the security of the network or networks of computer systems and the provision of backups. It represents the possibility of using this information system at any time and is a first criterion for measuring the quality and security of the system. Availability is measured by the "number of nines". "Five nines uptime", which is the most common, means that, over a year, a system has been operational or in standby 99.999% of the time, or all but 5 minutes and 16 seconds within the full 365 days. In correlation with availability, there is also the criterion of accessibility, an important factor for data discovery, characterized by: the level of organization of data by classification according to importance or sophistication and the quality of cyber infrastructure that the organization has.

The integrity of the information represents "confirmation that the data transmitted, received or stored by an individual or collective user, are complete and have not undergone any changes", according to the European Union Agency for Cybersecurity. This criterion is so important in information security that it must be approached from 3 directions: technical, legal or organizational. The technical part states that any modification of a simple bit can affect the integrity of the system, the legal criterion focuses on maintaining the meaning of the information in the documents, and from an organizational point of view, the meaning, content and information available to users become relevant.

Identification and authentication are criteria that directly target the user who is to access and obtain information data. The identification of a user is represented by the establishment of his identity, following which the authentication is performed through a series of methods, among which:

- user name - login and password system;
- OTP system (One time Password) - the user receives a password with a limited duration (usually a few minutes) on a special device (token), which can only be used once for authentication;
- digital certificate - usually stored on a medium (USB); can be activated by PIN code;
- biometrics (fingerprint, iris of the eye, etc.).

Confidentiality is represented by the fact that only authorized persons or entities, under certain predetermined conditions, can have access to information characterized by this feature. Confidential information that is disclosed through various means (hacking or even simply human error) can affect the organization.

The permanence of the information system means its preservation over time, through specialized coding in order to provide access to information and to facilitate their quality management. This permanence is achieved through archiving, ensuring 3 important requirements:

- represents a proof of the activities of the organization during its existence, defending its interests.
- creates an information database that includes different situations, analyzes and studies accumulated from the organization's experience, in order to be used in future planning.
- ensures the preservation of intangible information throughout the existence of the organization [5].

## 6. Data loss prevention

Zero Trust applies the principle of minimum data access privilege. The model is a security concept that requires authentication to perform a particular task for users, before being granted access

to only the necessary data and resources. In order to prevent data leakage, matching risk with trust given to a particular user or device is essential.

Zero Trust requires three fundamental steps, applied at the level of applications and services within the network:

- Verify the user (authentication, step 1);
- Verify the device (authentication, step 2);
- Verify access privileges (authorization).

These three layers of verification are accomplished through a series of compliance checks based on the characteristics of each. These compliance checks can include information ranging from device encryption to user patterns of behavior and can continue to expand as more information about users and devices is collected [6].

The correct user permissions and network segmentation have the same end goals but approach them in different ways. In the event of a breach or direct attack, both help to limit the impact area, with zero trust on a more granular scale. A zero-trust policy helps to develop a robust process for detecting and responding to incidents by reducing the time it takes to detect, probe, and address a data breach.

## 7. Visibility control and endpoint access

One of the most important cyber security challenges for remote companies is maintaining a comprehensive visibility in a network of various endpoints, while "visibility is the key to defending any valuable asset." [7]

With a secure web gateway (SWG) we can close this gap by applying zero trust policies to secure endpoints using a database to filter incoming and outgoing traffic for individual devices.

A key factor in enforcement of zero trust policies is that visibility must be intelligent and real-time. That is, the user and application identity attributes for different endpoints must be continuously monitored for suspicious or malicious activity. In addition, it is also important to strengthen the functions of the various modern security resources for simplified access control. Here comes a margin of Secure Access Service Edge (SASE). An SASE integrates SD-WAN with cloud security services such as SWG, Cloud Access Security Broker (CASB), and next-generation firewall (NGFW). The result is a more productive security delivery that enable organizations to protect their critical data.

## 8. Compliance with cyber security policy

The consequence of implementing the policies explained above is to achieve a greater compliance of cybersecurity strategies. With the transformation of the digital cloud between industries, the creation and enforcement of cybersecurity policies is inevitable. In aviation cyber security, for example, there are companies like AFuzion that are leading the industry in the direction of new regulations for flight safety.

A SWG is more than just a URL filtering tool; It is also used to log all security events to enforce a company's cybersecurity policy regarding Internet access. A SWG works by accessing the permission and credentials regarding the URLs and describe a table for granting or denying access. This means that an employee web access is blocked from unwanted content using the organization's network resources. In this way, SWG works like a CASB, with the major difference being that the latter covers a wider range, enforcing security policies and cloud protection beyond the traditional limits of a firewall. CASB or SWG and NGFW integrated, both help the organization deal with the obscure IT challenges.

For effective Zero Trust implementation, monitoring of all network assets is necessary as the days of relying on perimeter-based controls to stay compliant and secure are long gone.

## 9. Conclusions

On the one hand, business - especially remote companies - is booming with confidence. On the other hand, this idea of "zero trust" seems to threaten the foundation of business operations.

Zero Trust removes all implicit trust and continuously validates every stage of a digital interaction. But Zero Trust does not equate with mistrust. Forrester, who pioneered the term in 2010, insists that it is not a question of tracking everything like a hawk, but of acknowledging that not all data is created equal. Some data or applications need more security and governance than others, and while certain assets need to be watched and controlled closely, others can be left with minimal controls.

The Zero Trust security compensates for the reality that threats could be anywhere, and that the Intranet of your organization is likely no safer than the Internet. Despite the name, Zero Trust means more about trust than just trust.

## References

[1] D.S. Reveron, Cyberspace and National Security - threats, opportunities and power in a virtual world, Georgetown University Press, Washington DC, 2018.

[2] R.A. Grimes, Hacking Multifactor Authentication, Wiley, September 2020.

[3] K. Geers, Strategic Cyber Security, NATO Cooperative Cyber Defense Center of Excellence, 2011.

[4] IBM Security, Cost of a Data Breach Report 2021, https://www.ibm.com/downloads/cas/OJDVQGRY.

[5] E. Smit, J. Van Der Hoeven, D. Giaretta, Avoiding a Digital Dark Age for data: why publishers should care about digital preservation, Learned Publishing, Volume 24, Issue 1, Jan 2021.

[6] K. DelBene, M. Medin, R. Murray, The Road to Zero Trust (Security) [White paper], https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF.

[7] Forescout, Total visibility: The Master Key to Zero Trust Security [White paper], https://www.forescout.com/resources/total-visibility-the-master-key-to-zero-trust/.

[8] J. Garbis, J.W. Chapman, Zero Trust Security - An Enterprise Guide, Apress, 2021.

[9] S. Rose, O. Borchert, S. Mitchell, S. Connelly, Zero Trust Architecture, NIST (SP) 800-207, 2020.

# Developing a Comprehensive Model for Digital Lifelong Learning Using Cyber Resilience Framework

**Costel CIUCHI, PhD**
Associated Professor at University POLITEHNICA of Bucharest
Information Technology and Digitalization Directorate, General Secretariat of the Government
costel.ciuchi@gov.ro

**Abstract**

*Ensuring a secure environment through the use of information systems are mandatory requirements of today's society, practically it become an intense and ongoing concern in relation to possible risks and threats. The development of organizations is conditioned by the use of information systems, which gain vital importance over time and become the "engine" of daily activity. Also, in addition to the fact that information systems meet administrative and operational needs, they have gradually gained a significant share at all levels of the organization, up to the strategic and decision-making level. The working flows model must include new approaches, starting from the technological levels to managerial levels including most important layer of an organization: human resources. User's education and cybersecurity management knowledge represent an important part of ensuring the real organization's data and influenced managerial decisions. Technological threats and vulnerabilities can compromise decisional process starting from the early stages. With all the latest security technology implemented, a system will become cyber resilient if will take in consideration the 3 dimensions - human resources, processes, and technology. To achieve this goals, new approaches in cyber security education is needed. The diversity of technologies and accelerated developments of information technology in all domains need to be supported by a complex educational environment who must meet the actual society requirements.*

**Index terms:** cyber resilience, cybersecurity, education, learning framework, resilience

## 1. Introduction

Nowadays, the big question it is not if your network will be attacked, but when it will be attacked? And the real question is how quickly can you respond to the threat and recover? The diversity of vulnerabilities and threats, doubled by the complexity of the attack vectors reinforce the need for cooperation in cyber education, awareness, and professional training.

To diversify the education and training process comes from the need to acquire abilities and skills in cybersecurity which is a consequence of a constantly dynamic global competition and the growing demand for a better-skilled workforce adapted to accelerated technological changes.

There are new domains and directions in cybersecurity that need to update the educational and training process, close to realities from generated by complex vulnerabilities and threats. Exploring new methods and methodologies is expected in the next period.

First step is to enhance a collaborations ecosystem between academia, the private sector, and public administration to develop cooperation platforms for exchange ideas and educational programs in field of cybersecurity.

## 2. Education, awareness and professional training process in the field of cybersecurity

Achieving goals in cybersecurity requires updating and developing new models and frameworks for enhance skills to all employees an organization, both horizontally and vertically concerning all areas of activity are needed.

The growing demand for a better-skilled workforce adapted to accelerated technological changes and to threats or vulnerabilities from cyberspace need to be supported by adaptive educational, awareness and professional training processes.

The current status of educational process in the field of cybersecurity remarks two approaches the field from different perspectives, such as NICE Cybersecurity Workforce Framework and European Cybersecurity Skills Framework.

### 2.1. Cyber-Resilience Framework

Staring from the process of the design, technical systems must have a set of characteristics like dependability (availability, reliability, maintainability, safety) and security. To became resilient, there were identified four essential specific features:

- **monitor** critical developments;
- **respond** to what is happening;
- **anticipate** threats and opportunities;
- **learn from** experience - from success, but especially from **failures**.

Cyber-resilience represents a framework that is designed to help organizations withstand attacks. It is an iterative process that provides the ways of recovery from an attack and allows a constant vigilance across the organization.

Once bypassed, traditional defenses become useless, but cyber-resilience integrates security into the core of the business itself, allowing for the resilience components to be present in all areas of the business. To build a cyber-resilience capability, organizations must focus on shortening the life-cycle stages between defense and detection and response and recovery.

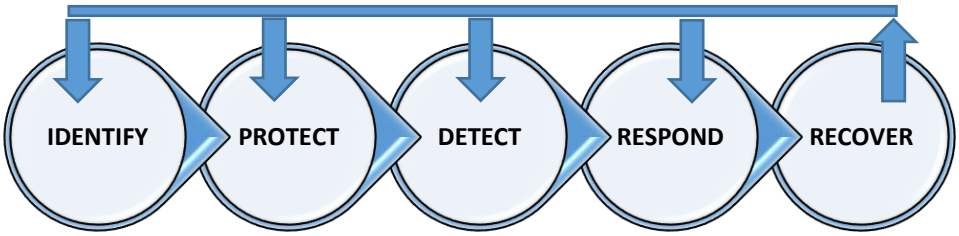



**Fig. 1.** Cyber-Resilience Framework [1]

To ensure resilience to an organizational ecosystem an important approach is to take in considerations all the dimension's, human resources, processes, and technology, with are involved in business model not only the technological part.

An important aspect related to cyber resilience culture in an organization, based on every component stage of resilience, is to develop and to build for the human resources and workforce an educational and continuous professional training strategy.

### 2.2. NICE Cybersecurity Workforce Framework

National Institute of Standards and Technology (NIST) developed a framework under The National Initiative for Cybersecurity Education (NICE) [2], Cybersecurity Workforce Framework

(NICE Framework) with the purpose to unify resources that establishes a unitary taxonomy and lexicon to describe processes from the cybersecurity domain. Also, connecting essential activities and associated tasks requires new skills and competences for the specialists, regardless of the particularity of the cybersecurity subdomain in which it operates. Modeling essential activities and associated tasks requires the development of the necessary steps to be taken in ensuring cybersecurity.

The NICE framework consists of interconnected components, the main grouping of common cybersecurity functions (categories - 7), distinct fields associated with activities (specialized area - 33) and detailed working groups which include the specific knowledge, expertise, abilities, and skills needed to perform tasks in a working role (working roles - 52).

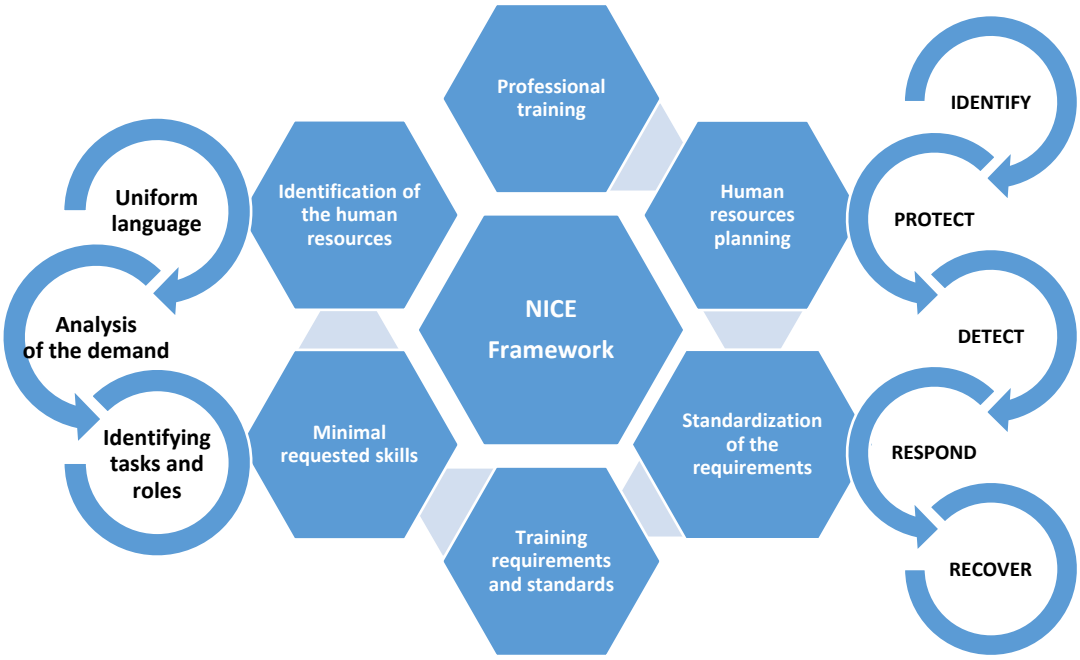



**Fig. 2.** Training and development model of skills [2]

In a continuous transformation domain, cybersecurity field needs experts with a complex and dynamic portfolio of expertise to face and execute essential cybersecurity actions for an organization.

**Table 1.** Mapping cyber resilience stages and NICE Framework categories

| *NICE Categories* | *Resilience Stages* |
|---|---|
| Analyze (AN) | **Identify** |
| Collect and Operate (CO) | |
| Investigate (IN) | **Protect** |
| Operate and Maintain (OM) | **Detect** |
| Oversee and Govern (OV) | **Respond** |
| Protect and Defend (PR) | |
| Securely Provision (SP) | **Recover** |

The main directions of common cybersecurity categories include the basic principles of resilience and represent a starting point for the developing a complete educational ecosystem.

### 2.3. EU Framework for Digital Education and Cybersecurity

European Union launch some initiatives to ensure a common understanding of the roles, skills, abilities, and knowledge used by and for employees, employers, and training providers in all EU member states to address the cybersecurity skills shortage.

The Digital Education Action Plan (2021-2027) [3] consist in a set of 13 action and is structured around two strategic priorities:

- promoting the development of a high-performance digital education ecosystem;
- improving skills and competencies for digital transformation.

The action plan is a result from challenges and opportunities of the COVID-19 pandemic, which has led to the unprecedented use of technology for education and training purposes.

The need to develop programs and mid-term plans, appear as a necessity especially in cybersecurity field, where Cybersecurity Act [4] granted ENISA new tasks to set up and maintain the European cybersecurity certification framework.

Also, strategy [5] is about reinforcing the presence on the technology, making up for the deficiencies of cybersecurity skills by enhancing cyber awareness, it aims to strengthen cyber diplomacy and cyber defence and to promotes standardization.

The development of a European Cybersecurity Skills Framework that would take into account the needs of the EU and each one of its Member States is considered an essential step towards Europe's digital future. Also, a common understanding of the roles, competencies, skills and knowledge used by and for individuals, employers and training providers across the EU Member States, in order to address the cybersecurity skills shortage is needed.

The European Cybersecurity Skills Framework is a result of joint work of ENISA and a relevant Ad Hoc Working Group on the European Cybersecurity Skills Framework [6]. The Group was formed in July 2020, following an ENISA public call for the creation of a multi-disciplinary group of experts that would promote harmonization in the ecosystem of cybersecurity education, training, and workforce development and develop a common European dialect for cybersecurity skills [6].

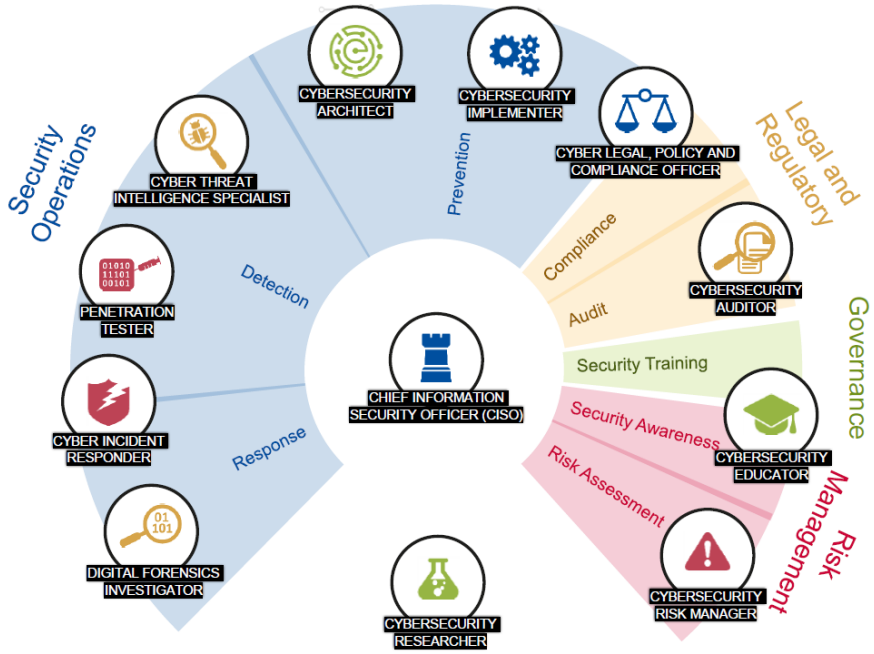



**Fig. 3.** CISO Mind Map - European Cybersecurity Skills Framework [7]

European Cybersecurity Skills Framework - is the European model that aims to facilitate the recognition of cybersecurity skills and become support for training programs in the field.

In this proposal, 12 relevant profiles in the field were selected to which unitary elements (dimensions) were associated, among which I mention: mission, deliverables, main tasks, main skills, key knowledge and e-Skills.

The main goal of this approach [7] is to create a robust, easy to use, expandable, neutral accessible, interoperable framework who will:

- Create a common understanding of the roles, competencies, skills and knowledge;
- Facilitate cybersecurity skills recognition;
- Support the design of cybersecurity related training programs.

## 3. Resilient model for learning process in cybersecurity

Improving education and research, represent key to achieving the overall objectives of cybersecurity policy and developing a trained workforce. Research and education approaches will only be effective if they include the multilateral and multidisciplinary nature of cybersecurity as a fundamental and ubiquitous element in culture, approaches, processes, systems, and technical infrastructures [8].

From the human resources perspectives, the approach of resilience requires the coordination of the main educational flows: learning / training / certification / assessment (EDU.LTC-A Cycle).


**Fig. 4.** EDU.LTC-A Cycle - Modelling the learning process

Relevant and quality skills and competencies are elements that need to be developed in accordance with the level of criticality associated with threats.

The need to update the educational mechanisms that can be adopted in order to develop complex models can be achieved considering the development of **key (technical) competencies** and **cross-cutting competencies** [9].

**Table 2.** Cross-cutting competencies [9]

| | **CROSS-CUTTING COMPETENCIES** |
|---|---|
| **ADEQUACIES (QUALIFICATIONS)** | EVALUATION, COMMUNICATION, ANALYSIS, INVESTIGATION |
| **ESSENTIAL SKILLS** | INTUITION, CREATIVITY, ADAPTABILITY, CONTINUOUS LEARNING |

The complexity of threats and cybercrime scams need to develop skills not only for professionals. Education for all users that use a system must be one of the priorities for critical infrastructure.

They must have competences and skills to identify and to report anomalies and all the intrusion attempts from their perspectives, in order to raise the level of security. In order to achieve this objective, a close cooperation is need between managers, developers, administrators and users.

Based on support of ENISA Ad-Hoc Working Group on Cybersecurity Threat Landscapes (CTL) [10], a report regarding Cybersecurity Threat Landscape for 2020-2021 (released in October 2021) were identified main threats, major trends observed with respect to threats, threat actors and attack techniques, and also were described relevant mitigation measures.

There are few important aspects that ENISA Cybersecurity Threat Landscape Report [11] reveals like:

- preferred target of attackers was public and government sector;
- most of the breaches in 2020 were caused by errors and system misconfigurations;
- highlights a spike in non-malicious incidents, human errors.

A different approach is needed to be settle for education process, professional training, awareness, and certification in cybersecurity. The proposed educational model has as main objectives the development of specific competencies and transversal skills considering the main attributes associated with resilience.

The development of educational processes in close connection with the cyber resilience framework will ensure the achievement of cyber resilience objectives and the achievement of a secure environment in accordance with the basic requirements associated with the field of cyber security.

Modeling educational flows based on the basic attributes associated with the cyber resilience framework (Identify, Protect, Detect, Respond, Recover) will ensure high security for technical systems, workflows and users. Also, the elements necessary to be improved will be highlighted, both from the point of view of human resource preparation and from the perspective of the competencies necessary to be developed:

- a common understanding of the roles, competencies, skills and knowledge used by and for individuals, employers and training providers;
- developing skills recognition framework and training programs in cybersecurity;
- building and sustain a professional cybersecurity workforce.

## 4. Conclusions

Cyber-attacks have been experiencing explosive diversification lately, some of which can be classified as global epidemics due to the high speed of spreading in the virtual environment. The threats to the information systems are characterized by an increased dynamics and a global character, making them difficult to identify and counteract.

Although there are numerous and better performing methods of protection, ensuring information security in the cyber environment can't be achieved only by technical measures, being mainly a human problem. Security incidents are frequently generated by an inadequate organization of security policies and less because of a security system failure. In this context, it is necessary to develop strategies on cybersecurity by defining policies in this respect and campaigns to prevent and combat cybercrime at national level [8].

Research and education in the field of cybersecurity must be priorities of public policies. Strengthening information security research, improving education and developing trained workforce are essential to achieving the overall cybersecurity policy objectives.

International cooperation plays a key role in this area, as cybersecurity challenges go beyond boundaries, extending to global interconnected systems. Collaboration with European and International entities is absolutely necessary, whether it is educational establishments, research centers, private companies or government institutions. Cooperation between institutions, organizations and the cybersecurity community can be useful in finding and fixing vulnerabilities. A proven cooperation mechanism in this regard is the coordinated disclosure of vulnerabilities [8].

Adoption of coherent public policies at Members State level on coordinated vulnerability disclosure and coordinated cross-sectoral action / trans-sectoral cooperation mechanisms will provide

the necessary ecosystem to ensure security in the community. The opening of communication channels, the creation of working groups and public consultation, the involvement of civil society and the public-private partnership are key directions that public policies should focus on.

This article aims to highlight avenues for an education model and an international collaboration to effectively combat threats and cybercrime. Using new approaches and methodologies to assist organizations and authorities to provide a platform for exchange of best practices, share resources for educational process in cybersecurity.

The need to respond to cybercrime and to raise awareness among relevant stakeholders and specially for the public on related matters, represent a key element that make from education domain a central pillar to any cybersecurity strategies [12].

Concluding, the adoption of comprehensive and up-to-date cybersecurity legislation to support the development of education capabilities should be a national priority. Ensuring a secure cyberspace is the responsibility of both the state and the competent authorities, the private sector and civil society. For the development of the cybersecurity culture, the most important levers are education and research, public-private partnerships and cooperation mechanisms at European level.

**References**

[1]. F. Dickson, P. Goodwin, Five Key Technologies for Enabling a Cyber-Resilience Framework, White Paper, International Data Corporation (IDC), Sponsored by: IBM, October 2020, Available: https://www.ibm.com/downloads/cas/YBDGKDXO.

[2]. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), NIST Special Publication 800-181, National Institute of Standards and Technology, July 28, 2020, Available: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

[3]. Digital Education Action Plan (2021-2027), European Commission, COM (2020) 624, Available: https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en.

[4]. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act, Official Journal L 151 15 (2019). Available: http://data.europa.eu/eli/reg/2019/881/oj.

[5]. European Commission (2020b) The EU's cybersecurity strategy for the digital decade. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN.

[6]. Ad-Hoc Working Group on the European Cybersecurity Skills Framework, Available: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls.

[7]. European Cybersecurity Skills Framework, Webinar, Available: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/webinar-presentations.zip.

[8]. I.C. MIHAI, C. CIUCHI, G. PETRICĂ, Current challenges in the field of cybersecurity - the impact and Romania's contribution to the field, The European Institute of Romania. - Bucharest, 2018, Available: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS_2017_Study_4_FINAL.pdf.

[9]. C. CIUCHI, Building a Resilient Ecosystem for Cybersecurity in Education, Cybersecurity - Challenges and Perspectives in Education, I.C. MIHAI, C. CIUCHI, G. PETRICĂ (editors), pp. 141-152, ISBN: 978-3-940237-26-2, DOI:10.19107/CYBERSEC-EDU. 2020.EN, Academica Greifswald, Rostock, Germany, 2020.

[10]. Ad-Hoc Working Group on Cyber Threat Landscapes, Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes.

[11]. ENISA Threat Landscape 2021, Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[12]. Considerations on Challenges and Future Directions in Cybersecurity, I.C. Mihai, C. Ciuchi, G. Petrică (coord.), eISBN 978-606-11-7005-0, ISBN 978-606-11-7004-3, Sitech, 2019, Available: https://www.arasec.ro/documente/CybersecurityRO2019.pdf.

# Establishing Effective Cyber Diplomacy and Deterrence Capabilities Between International Partners

**Cristian-Vlad OANCEA**
Provision IT Group, Bucharest, Romania
vlad.oancea@protonmail.ch

**Abstract**

*Changes has been always a constant in a modern and dynamic world, but the rapidity of change in the global security landscape accelerated after 9/11 and global war against terrorism. There is a new approach regarding political, ideological, economic and military race due to globalization which improved the landscape with good practices and developmental growth but is still a major driver of instability. While threat of conventional decrease, accordingly the spread of conflict, it complexity, accuracy, changeable and reach into many areas have emerged. Many new types of warfare have also emerging like cyber, network, digital, information, economic, media pursued cross domains both in peace or war. Especially nowadays but also during challenging times, deterrence has been an important part of foreign affairs of a nation, to conserve internal and external stability and preserve its integrity.*

**Index terms:** Cyber Diplomacy, Cybersecurity, Deterrence, IoT

## 1. Introduction

The etymology of "deterrence" starts with the Latin word "deterre" – to frighten from or away. The dictionary defines deterrence as "the action that persuades an opponent to give up something that is desired." [1]

Deterrence discourages an opponent from pursuing an unwanted action. It is a complex subject guided by a number of types, theories, forms, strategies and many other factors. All countries are managing and expanding their strategic area to secure freedom to conduct multi-domain actions by a wise combination of creating alliances and increasing their comprehensive national power which leads to an increased level of deterrence capability.

Deterrence requires a national strategy that integrates diplomatic, informational, military, and economic powers. India must develop strategies, plans, and operations that are tailored to the perceptions, values, and interests of specific adversaries. Deterrence strategies and actions must be developed for all phases of confrontation and conflict planning. Deterrence operations must, therefore, be planned and executed across all domains in concert with other elements of national and international power in order to achieve strategic objectives. A crucial aspect is that successful deterrence is knowledge-dependent and requires the ability to establish and secure communication access to adversaries in order to generate the desired decision outcomes. Human intelligence (HUMINT) naturally is essential in seeking to understand an opponent's values, culture, decisions, risk and capacity for situational awareness as well as obtaining other information required for effective deterrence. Situational awareness is the sine qua non for deterrence where political direction,

intelligence community, diplomacy, law enforcement, military, and even economic inputs must get synergised. Our military capabilities and potential must be visible and known to all as it's a pivotal ingredient of deterrence. Effective deterrence combines military and non- military means. In some cases, military capabilities may not be an effective tool to deter a particular adversary's action, making other instruments of power the primary deterrent. Additionally, the support of strategic partners should be integrated to increase deterrence credibility, but deterrence must be applicable as a unilateral approach. The deterrence will obviously be challenged by other affected Nations. Military actions will always remain the final pivotal option to achieve national objectives both proactive and reactive. One very important factor which is being increasingly accepted is the mind of the leader and people and their likely reaction to deterrence. I would like to re-emphasize here, that deterrence in security parlance covers a very wide spectrum of activities and domains and not just employment of armed forces.

## 2. Enhancing inter-operability between NATO and EU Member States

The major interest nowadays is to expand cooperation in fields that will support the realisation of objectives that NATO and EU Member States and organisations share. The EU Member States and NATO are capable of complementing each other well. Examples include the "PESCO" project [1] and the Multinational Medical Coordination Centre in Koblenz, Germany. A project for the storage of medical equipment tools was developed under the responsibility of the European Medical Command and the related agency is already in use.

This point highlight that the enhanced cooperation between NATO and the EU Member States is important for the nations that are not part of both organisations at the same time. The breakthrough regarding the participation of non-EU nations in PESCO that was negotiated under the German Council Presidency and will help further expand cooperation and thereby further improve the existing operational result.

Strengthening Europe's possibility to act, in this case, does not constitute a weakening of NATO nor does it question NATO, which is works well and serves its scope. An enhanced cooperation serves to improve both organisations ability to act. After all, this represents a shared goal: to improve an ability to act to guarantee future security for and in Europe.

## 3. Moving toward a unified interpretation of cyber operations within the Law of Armed Conflict

Security culture in the information age presents a lot of challenges. The cyber revolution gives get up to new threats and opportunities requiring immediate actions and policy responses. Understanding its nature and especially the consequences for security represents a slow learning process. Interpretation of cyber fact involves analysis of a new body of experience that actual existing assumptions may be unable to clarify. It requires a technical understanding of a changing technology, whose implications require time to learn and analyze because of its scientific complexity. The result has been a delay in the strategic reshaping to cyber actuality. The contemporary world faces up to an enormous cyber threat. The U.S. intelligence community rates this threat higher than global terrorism and warns of the potential for a catastrophic cyberattack. The range of feasible cyber conflicts is poorly understood by students or decision makers and it is quite unsure how conventional security mechanisms, such as deterrence and collective defense, apply to this fact. In addition, the principles of cyber offense and cyber defense still remain essential.

Also, the rules of engagement (ROEs) [2] for cyberspace operations have received increasing attention as opportunities for achieving military objectives in and through cyberspace have become more feasible. To the scope probable, it is necessary to apply the same principles that government the use of kinetic weapons to the use of cyber weapons, while recognizing the special attributes of the cyber space and cyber weapons. This has demonstrate to be a difficult challenge. A lot of the military's actual capabilities in the cyberspace field and the ROEs correlate to their purpose, still remain classified. Through inference, informed speculation and an growing audience understanding of the elementary technology, a growing shape of unclassified information is available regarding the principles and concepts that guide how decision makers formulate ROEs for operations in cyberspace.

In the kinetic world, proceeding quickly is often necessary to mitigate an immediate threat. Also, similar aspects have been applied to threats in cyberspace. Given the speed with which a cyber threat may cause damage, a reaction may be needed very quickly to mitigate or disrupt it. In fact, the duration on which action is needed may be so short as to prevent human involvement. However, an automated response may lead to unexpected and collateral outcome for which the consequences are not totally understood.

## 4. Bridging the gap between industry, academia and militaries

The rapid step of digital transformation is changing every aspect of our lives and is also creating needs for new skills and knowledge in the workplace.

Rapid technological evolution is changing the way businesses operate. Emerging and cutting edge technologies such as the Internet of Things (IoT), Cloud computing, Automation or Artificial Intelligence (AI) are enabling new model based, distributed, machine enabled business models and creating extraordinary opportunities to create new value. As job profiles, industry and military field evolve, shortages and mismatches can result, but universities may be able to help.

Private companies, government, the military industry and academia are all taking steps to close the cyber talent gap; however, their existing efforts and traditional approaches may not be sufficient to resolve the issue.

Applying a human-centric lens to the cyberspace ecosystem for cyber talent reveals critical action items that affect every level of the employee life cycle, from creating the overall talent pool and recruiting the right people to onboarding new hires, continuously developing new skills and expertise, retaining top talent, and even offboarding people in a manner that preserve an organization's talent brand.

Emerging technologies such as automation and artificial intelligence should be used to increase the traditional cybersecurity efforts. However, such technologies do not remove the need for human talent.

Governments at all levels play an important role in the cybersecurity talent ecosystem, not only in terms of needing such talent to defend systems and data, but also in terms of initiating policies and programs to support address the talent shortage.

The cyber talent gap definitely represents a global risk; but in coordination between governments, educational institutions, public and private sectors, military area, the cybersecurity talent area can rise and be seen as a leader by making confident moves and changing the face of this actual shortage.

Mastering the cyber talent shortage and addressing cyber risk effectively will require an innovative talent strategy, supported by a solid culture and a basic human and technology infrastructure.

Closing the cyber risk gap and enabling organizations to capture the full promise and importance of new technologies is a great opportunity of our time. Emerging technologies such as AI, Machine learning and Big Data can help expend an organization's traditional cybersecurity efforts; however, all those technologies will not skip the need for human talent, at least, not any time soon.

**References**

[1]. https://www.britannica.com/topic/deterrence-political-and-military-strategy.
[2]. https://eda.europa.eu/what-we-do/EU-defence-initiatives/permanent-structured-cooperation-(PESCO).
[3]. https://www.readcube.com/articles/10.1093%2Fcybsec%2Ftyx003.

# 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: https://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/