ISSN: 2450-6869

eISSN: 2719-6763

No. 15, 2022

DEFENCE SCIENCE REVIEW

http://www.journalssystem.com/pno/

DOI: 10.37055/pno/158811

Actual and future digital threats and their impact on civil and military cybersecurity management

Original article

Received: 2022-12-28

Revised: 2022-12-28

Accepted: 2022-12-29

Final review: 2022-12-29

Peer review:

Double blind

Keywords:

hackers, cyber-attacks, digital threats, cyber vulnerabilities and damages, cybersecurity risk management

Oriana Helena Negulescu[1,A-D]
ORCID 0000-0001-7937-2066

Elena Doval[2,B-D]
ORCID 0000-0002-2809-8631

Ana Roxana Stefanescu[2,B-D]
ORCID 0000-0003-4762-3814

A – Research concept and design, B – Collection and/or assembly of data, C – Data analysis and interpretation, D – Writing the article, E – Critical revision of the article, F – Final approval of article

[1] Department of Management and Economic Informatics, Transilvania University of Brasov, Faculty of Economics and Business Administration, Romania

[2] Spiru Haret University Bucharest, Faculty of Legal Science and Economics, Romania

Abstract

Objectives: (1) What is the hacker community made up of and what are the main vulnerable industries? (2) What are the main types of digital threats and how are they characterized? (3) What are the vulnerabilities and damage caused by cyber-attacks? (4) What are the ways to detect digital threats? (5) What measures can be taken to prevent and avoid these attacks? (6) What does the cyber security management process consist of? (7) What cybersecurity evidence and trends can be selected?

Methods: Document analysis; data selection and assambly; synthesis; conceptualization; interpretation.

Results: The research results are: a presentation of the hacker community and the main vulnerable industries; a brief definition of the types of digital threats; presentation of various vulnerabilities and damages caused by cyber-attacks; a selection of the ways to detect digital threats; a selection of the main measures to prevent and avoid these attacks; cybersecurity management process and a selection of evidence and trends regarding cyber security. Also, two conceptualizations are proposed: the approach to cyber risk management and 10 basic actions to prevent and avoid cyber risks.

Conclusions: The current and future situation is not encouraging for the management of organizations in terms of the risks caused by cyber-attacks, which are increasing significantly. The solution to prevent and avoid these threats is for civil and military organizations to implement Cybersecurity risk management.

Corresponding author: Oriana Helena Negulescu – Department of Management and Economic Informatics, Transilvania University of Brasov, Faculty of Economics and Business Administration, Bulevardul Eroilor 29, Brașov 500036, Romania; email: oriana.negulescu@unitbv.ro;

Introduction

In our century, information is the main means for knowledge, power over competitors and the source for managerial decisions. The rapid advance of information technology has determined the creation of cybernetic space, composed of IoT, cloud, 4-5 G systems, metaverse, robots, etc. This space is extremely useful both in personal life and in business, and especially in public activities, including national defense. At the same time, means of attacking the security of information storage were also created, which causes serious threats. „Security threat may be defined as being the danger of the nations' loosing the peace, safty and freedom. The term includes the social, economical, political, democratical, informational and borders threats.

Considering the international security, the main identified eight threats are the followings: corruption; terrorism; chemical and biological weapons; nuclear and radiological weapons; infectious diseases; smuggling, counterfeiter and piracy; territorial expansion strategy, and the last, but not the least, the cyber weapons" (Negulescu, 2015). Regarding the digital threats, Taylor (2021) states "Cybersecurity risks pervade every organization and aren't always under IT's direct control. Business leaders are forging ahead with their digital business initiatives, and those leaders are making technology-related risk choices every day. Increased cyber risk is real — but so are the data security solutions". Any way, „the world security environment is characterized 'as extremly fluid and unpredictable" (Adrian, 2012).

During and after the end of the Covid19 pandemic, cyber attacks (phishing attacks, malware, ransomware attacks, espionage attacks and others) have increased alarmingly and become more and more complex, and hackers are making huge profits. Advanced persistent threats are being challenged in all areas of activity. "hacking groups specializing in deep and complex cyber attacks on large organizations are playing the same chess game between world powers. Groups in India, China, Russia, Iran – and one can only guess, the US – are hacking strategic targets more than ever, aligned with the political and economic goals of their "backer" countries" (Gutiérrez, 2021).

However, the pandemic led to an increase in risks, especially due to remote activities. "Cybercrime, which includes everything from theft or embezzlement to data hacking and destruction, is up 600% as a result of the COVID-19 pandemic. Nearly every industry has had to embrace new solutions and it forced companies to adapt, quickly" (Mclean, 2022).

Also, the Russian invasion in Ukraine has amplified the cyber-attacks (Lewis, 2022; Csis, 2022). "Russia sought to disrupt services and install destructive malware on Ukrainian networks included phishing, denial of service, and taking advantage of software vulnerabilities. The primary targets were Ukrainian government websites, energy and telecom service providers, financial institutions, and media outlets, but the cyberattacks encompassed most critical sectors. This was a wide-ranging attack using the full suite of Russian cyber capabilities to disrupt Ukraine" (Csis).

In this context, it is more than necessary that in any type of organization the management gives a special place in the current and long-term strategy to the monitoring of cyber attacks, which have become real threats to information security. Therefore, the aim of the work is to clearly highlight the main aspects that concern cybersecurity management in civil and military activity.

The pursued objectives are:

- Presentation of the hacker community and the main vulnerable industries;
- Defining the types of digital threats;
- Presentation of various vulnerabilities and damages caused by cyber-attacks;
- Selection of ways to detect digital threats;
- Selection of the main measures to prevent and avoid these attacks;
- Cybersecurity management process;
- Selection of evidence and trends regarding cyber security.

1. Methods

The methodology used in writing this study is based on documentation, using public information from websites and ideas launched by different authors or specialized companies; analysis of the collected material; information synthesis; generalization, conceptualization and own interpretation.

2. Results and discussion

In the conditions of the continuous increase in the vulnerability of the use of devices based on the Internet, it is necessary for every organization to include Cybersecurity risk management in its organizational structure. For this purpose, the work addresses the necessary basic elements and thus responds to the predetermined objectives (fig.1).

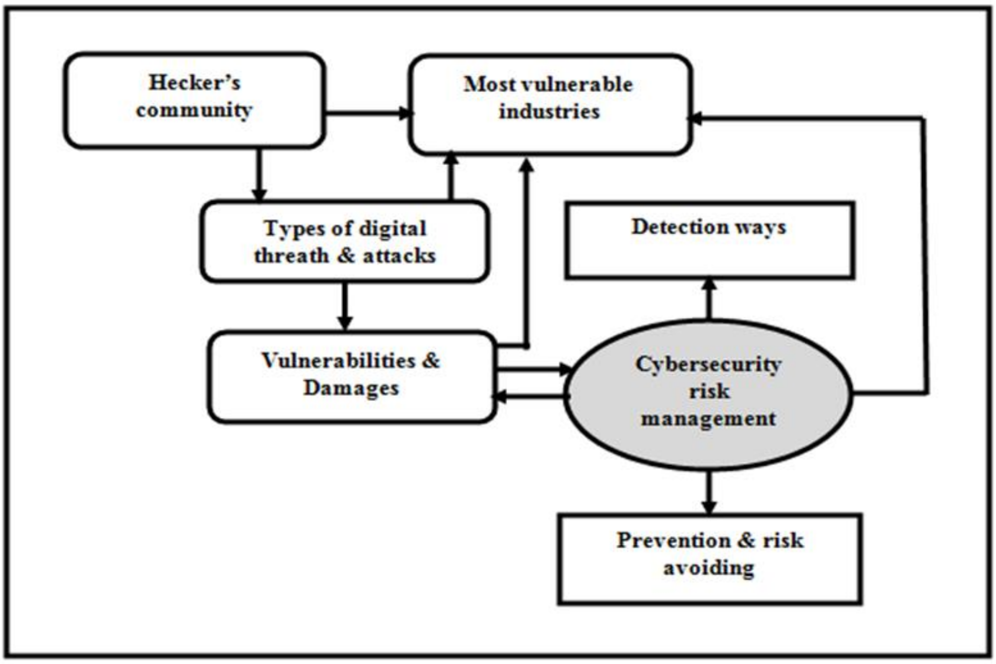
Hecker's community
Most vulnerable industries
Types of digital threath & attacks
Detection ways
Vulnerabilities & Damages
Cybersecurity risk management
Prevention & risk avoiding

Fig. 1 Approaches to cybersecurity risk management

Source: the authors' concept

2.1 Hacker's community and the most vulnerable industries

The hacker community is made up of individuals, criminal organizations, states, unfair business competitors, vengeful employees, industrial spies, terrorists. They come from different countries, including Russia, China, North Korea and others (preyproject.com).

Depending on the hacked object, hacking is divided into 5 categories: Network hacking; Hacking of websites; Computer hacking; Password hacking and e-mail hacking (javatpoint.com).

1. Network Hacking: Network hacking means gathering information about a network with the intention of harming the network system and hindering its operations using various tools.
2. Website Hacking: Website hacking means taking unauthorized access to a web server, database and changing information.
3. Computer Hacking: Computer hacking means unauthorized access to computer and stealing computer information, computer ID and password by applying hacking methods.
4. Password Hacking: Password hacking is the process of recovering secret passwords from data that has already been stored in the computer system.

5. Email Hacking: Email hacking means unauthorized access to an email account and its use without the owner's permission.

Hackers can enter the cybernetic system of the organization through 4 ways: through the network, through the web page, through access and through post-exploitation.

Tietsort (2022) identified 15 types of cybercriminals, which could be grouped according to their dangerousness into 3 categories: useful, enemies and dangerous criminals (fig. 2, table 1).

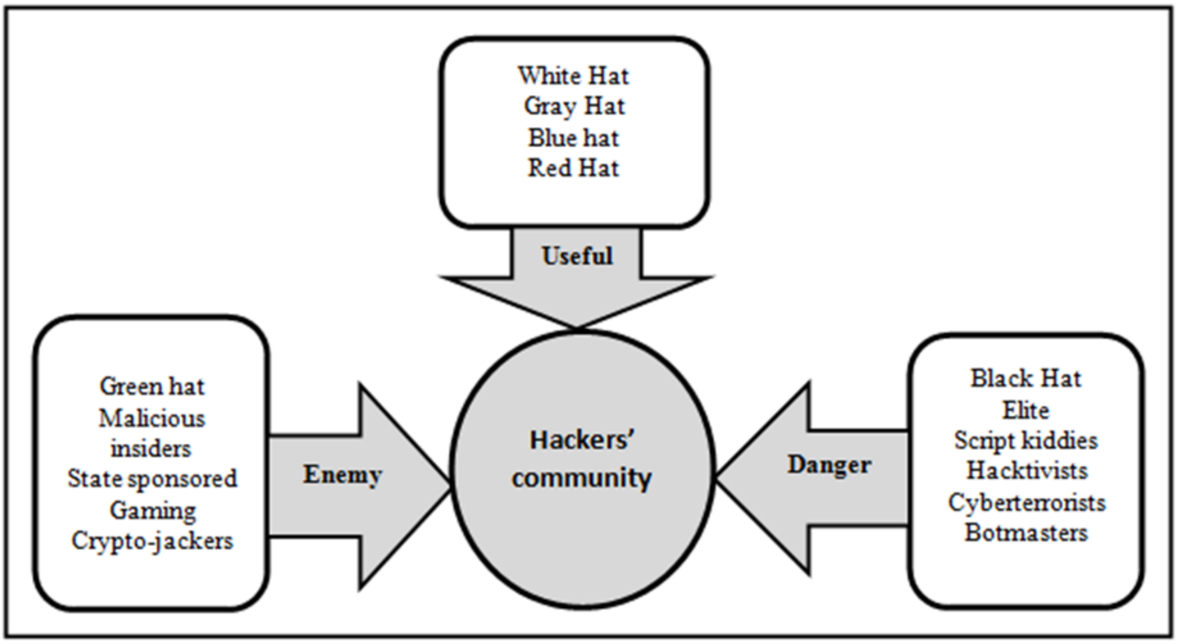

Fig. 2 Groups of hackers

Source: the authors' concept

Table 1 Characteristics of hackers

No	Hackers' types	Characteristics
Useful		
1	White Hat hackers	They, also called "ethical hackers" or "the good guys", test the security weaknesses and vulnerabilities of IT systems. They are rewarded by government agencies and companies for the vulnerabilities found in the system.
2	Grey Hat hackers	They intentionally penetrate the system to find vulnerabilities and inform the system administrators about the weak points to be improved. They are mostly good, but technically still illegal.
3	Blue Hat hackers	They work for IT security firms to evaluate software applications and detect weak points in order to take corrective measures. They are pre-launch penetration testers.

4	Red Hat hackers	They are aggressive and function as law enforcement by following black hats and destroying their systems with aggressive and illegal tools.
Enemy		
5	Green Hat hackers	They are self-starters, eager to learn. Take appropriate certification courses and online tutorials to develop your skills to become a black hat
6	Malicious insider	They are malicious people inside the organization who attack their own companies to "prove" that they are right about security vulnerabilities or who take revenge for various reasons or denounce certain illegal practices of the company.
7	State or nation-sponsored hackers	They work for government agencies. They gain access to other nations' systems to monitor cyber threats or steal confidential information
8	Gaming hackers	They do unsportsmanlike hacking. They are the professional players who accumulate credits online and steal credits from other players through DDoS attacks.
9	Crypto-jackers	They do crypto-mining in the shadows; exploits cryptocurrency by infecting devices with malware that extracts scripts and sends them to hackers, They don't steal data and do no harm.
Dangerous criminals		
10	Black Hat hackers	They, called the obvious "bad guys", are dangerous, highly skilled, and motivated by personal and financial gain. They hack with malicious intent, and they leverage their knowledge of programming languages, network architecture, and networking protocols.
11	Elite hackers	They are innovators and influencers. They create the latest malware and advanced types of cyber-attacks to penetrate stronger security systems.
12	Script kiddies	They want attention and make a lot of noise. They don't learn but buy existing malware kits and predefined scripts created by real hackers on the Dark Web. In general, they commit DoS or DDoS attacks.
13	Hacktivists	They consider their activity a form of protest against those who do not share their political, ideological, social, religious, etc. ideas; they usually go against intelligent organizations and governments.
14	Cyberterrorists	They threaten or damage a country's networks and infrastructures; create panic, disrupt operations for large sums of money, usually in cryptocurrency.
15	Botmasters	Also called bot herders or bot army leaders, they create armies of bots loaded with malware and then launch high-volume attacks.

		They typically target routers, cameras, and other Internet of Things (IoT) devices with weak security systems. They threaten or damage a country's networks and infrastructures; create panic, disrupt operations for large sums of money, usually in cryptocurrency.

Source: (Tietsort, 2022)

JavaTpoint mentions the most famous hackers, including Gary McKinnon, who was accused of the "biggest military computer hack of all time" in 2002. He has successfully hacked the network of Navy, Army, Air Force, NASA system of the United States Government javapoint.com).

Any type of hacking is illegal and unethical. "The moral rules and the acceptance of the international agreements may protect the civilian people, but the criminal organizations' hackers have no morals (Negulescu, 2015).

Even cybersecurity spending is increasing but breaches are still happening (Carey & Jin, 2019).

Every organization is at risk of a data breach, systems hack, malware or ransomware attack, or of cybercriminals illicitly accessing their network's processing power (Manship, 2022). The authors found that the most targeted industries attacked by hackers are: Business (such as: e-commerce/retail and small business), Healthcare and Medical, Banking and Credit/Financial, Government and Military, Education and Energy and Utilities. The list can be completed with manufacture, construction, aviation and marine.

The commerce technology and business are facing the attackers that continuously search for new vulnerabilities in humans, organizations, and technology (Liu et al., 2022).

Aviation concerns airlines, airports, air traffic management entities, as well as other key service operators in the aviation subsector, the services of which are interrelated and often interdependent (Radomska, 2021).

The maritime sector, which until now was considered safe due to the lack of Internet connectivity and the isolated nature of ships in the sea, is showing a 900% increase in cybersecurity breaches on operational technology as it enters the digital era (Akpan et al., 2022).

2.2. Types of digital threats

A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general (Trellix). There are known 17 different types of cyber attacks (Aura), but the most common malwares could be: virus, trojan hors, worms, ransomware, data breaches, spyware, denial of service (DoS) attacks.

The main characteristics of these digital threats are presented in table 2.

Table 2 Characteristics of the main digital threats

Types of digital threat	What is	Ways to act	Means to spread	References
virus	a type of malware	- it attaches itself to other programs, self-replicates and spreads from one computer to another; - has 4 phases: rest, propagation, triggering, execution	on devices and networks: emails, downloads, messaging services, old software, malvertising	Avast
trojan hors	a type of malware other than a virus	it fakes a patch, is an illegal free copy of software, is strange email with an invoice or receipt	free software and music, ads in the browser and on seemingly legitimate apps	Malwarebytes a.; Levin, 2022.

worms	a subset of Trojan horse malware	- it exploits parts of an operating system that are automatic and invisible to the user;
		-it can spread or self-replicate from one computer to another without human activation, after breaching a system
			It spreads in a network through Internet connection or LAN (Local Area Network) through: Phishing, Spear-Phishing, Networks, Security Holes, File Sharing, Social Networks, Instant Messaging, External Devices	Malwarebytes b;
				Techtarget;
				Bedell et al., 2022;
				Vigderman & Turner, 2022.

ransomware	a type of malware that employs encryption	-it deny a user or organization access to files on their computer.
		-it uses asymmetric encryption.
		-it paralyze an entire organization.
		-iIt steal data.
			It is distributed using email spam campaigns or through targeted attacks across a network, target database and file servers; Malspam, Malvertising, Spear phishing, Social engineering	Checkpoint.com;
				Trellix.com;
				Kaspersky;
				Cisa;
				Malwarebytes c.;
				Fruhlinger, 2020.

data breaches	Is stolen or taken information	information is stolen or taken from a system without the knowledge or authorization of the system's owner	It uses as methods: hacking or malware attacks; insider leak; payment card fraud;	Trendmicro;
				Komnenic, 2022;
				Cloudmask;

			loss or theft; unintended disclosure	Termly.

spyware	is a type of malicious software	it monitors internet activity, tracks login credentials and spies on sensitive information	it is downloaded without the user's authorization on computer or mobile devices using internet connection	Veracode;
				Fortinet;
				Gillis et al.

DoS (denial of service) attacks	is a cybercrime economic model	it shut down a machine or network, making it inaccessible to its intended users	It uses as methods flooding services or crashing services that triggers a crash to servers	Paloaltonetworks;
				Corero Marketing;
				Dahiya & Gupta, 2020.

Source: the authors' concept

2.3. Vulnerabilities & Damages

Vulnerabilities

Cyber attacks do not generally lead to the death of people, but they cause a series of damage to databases, sometimes even the total loss of them, theft of information and important material damages. The main vulnerabilities of the common types of threats are briefly presented below.

Viruses infect computers inconspicuously and are often designed to destroy personal files or gain control of devices. Viruses could be split into two categories: "those that begin to infect and replicate as soon as they land on your computer, and those that lie dormant, waiting for you to unwittingly execute the code" (Avast).

Trojans can act as "a bit of standalone malware, or as a tool for other activities, such as delivering future payloads, communicating with the hacker at a later time, or opening up the system to attacks" (Malwarebytes a).

Worms have the main function of staying active. “They double up to spread to uninfected computers. They often do this by exploiting parts of an operating system that are automated and invisible to the user” (Malwarebytes b.). "After a computer worm loads and begins running on a newly infected system, it will typically follow its prime directive: to remain active on an infected system for as long as possible and spread to as many other vulnerable systems as possible" (Techtarget).

Ransomware is used by hackers to gain financial advantages. They design a private key that they sell to victims so they can access their database again. "The attacker makes the private key available to the victim only after the ransom is paid. Without access to the private key, it is nearly impossible to decrypt the files that are being held for ransom" (Trellix).

This type of cybercrime is usually of two types: Locker ransomware, which blocks basic computer functions and Crypto ransomware, which encrypts important data, such as documents, pictures and videos, but not to interfere with basic computer functions (Kaspersky). "The user is presented with a message explaining that their files are now inaccessible and will only be decrypted if the victim sends an untraceable Bitcoin payment to the attacker" (Fruhlinger, 2020).

Data breaches cause financial and reputational losses because stolen data "may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security" (Trendmicro).

Spyware is an application that starts as soon as the device is turned on and continues to run in the background, stealing memory and slowing down the processor. It can also redirect web searches and control the results provided, modify your computer's dynamic link libraries, track web browsing history, passwords and other private information, and secretly change firewall settings. "Some forms of spyware can even identify when the device is trying to remove it from the Windows registry and will intercept all attempts to do so" (Techtarget). Spyware typically follows a three-step process from being installed on a device to sending or selling the information it has stolen: infiltrate, monitor and capture, and send or sell (Fortinet).

DoS (denial of service) attacks or DDoS (distributed denial-of-service on servers) often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. "Although DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle" (Paloaltonetworks). Attacks can be: the use misconfigured network devices by sending forged packets; a connection request is sent to a server but never completes but continues until all open ports are saturated with requests and none are available for legitimate users to connect; an input is sent that takes advantage of the errors in the target that subsequently freezes or destabilizes the severer; the target is attacked from many locations at once.

Most of thus vulnerabilities are due to human mistakes (social engineering), configuration, poor cyber hygiene, cloud, mobile device, third party, IoT, poor data management, inadequate post-attack procedure (Embroker).

Damages

The main damages caused by **computer viruses** are: (Avast; Csis):

- Slow or stuttering performance;
- Corrupted or deleted files;
- Incessant pop-ups or adware;
- Program failure and operating system crashes;
- A constantly spinning hard drive;
- Malfunctioning apps, files, and other programs;
- Crashing or freezing apps;
- Unexplained changes to your device or account settings (avast.com; csis.org).

In addition to causing these negative performance issues, computer viruses can also steal personal data such as usernames, passwords and credit card details. Some viruses can send spam to all the user's contacts who can download the virus and thus spread (Avast).

Many of the symptoms of a **computer worm** are like that of a computer virus, such as: computer slows down, freezes, crashes or throws up error messages; files are missing or corrupted or that the hard drive's space is rapidly depleting inexplicably (malwarebytes.com). The worms also provoke: drop other malware like spyware or ransomware; it consumes bandwidth; delete files; overload networks; steal data; open a backdoor or deplete hard drive space (Patents).

A **trojan horse** installed on the computer can spy, steal personal information, and/or create backdoors that allow other hackers to do the same (Levine, 2022).

The most damaging **ransomware** actions would combine precision-guided munitions and cyber-attacks to disable or destroy critical targets. They are also used to disrupt finance, energy, transportation, and government services to overwhelm defenders' decision-making and create social unrest (Csis).

The consequences of **data breach** can include destruction or corruption of databases, the leaking of confidential information, the theft of intellectual property and regulatory requirements to notify and possibly compensate those affected (Cloudmask). These attacks cost the companies huge amount of money that “include lost data, business disruption, revenue losses from system downtime, notification costs, or even damage to a brand’s reputation. In the visual below, we outline the impacts a business may face from the first year up to the third year” (McLean, 2022).

Spyware is designed to go undetected, there are several tell-tale signs that could be indicators of a device being infiltrated. These include: 1) Negative hardware performance, such as: A device running slower than usual and Devices suffering frequent crashes and freezes and 2) A drop in application or browser performance, such as: pop-up ads repeatedly appearing in browsers; unusual error messages; unexpected browser changes; new icons appearing in the taskbar; browser searches redirecting to new search engines. Note that these symptoms are also indicative of the presence of other malware, not just spyware, so it is important to dig deeper into issues and scan devices to discover the root of the problem (Fortinet).

DoS (denial of service) can cost an organization millions of dollars in terms of remediation costs, lost revenue, lost productivity, loss of market share, and damage to brand reputation (Corero Marketing, 2021).

Barriers that overcome cyber security challenges: lack of security cybersecurity budget, inadequate cybersecurity professionals, weak collaboration among states "Only 28% of states reported that they had collaborated extensively with local governments as part of a security program during the past year, with 65 % reporting limited collaboration" (Ward & Subramanian, 2021). Poor resilience in the environment of international institutions of strategic status to establish space situational awareness of key importance for future global defence and deterrence (Borek et al., 2022).

2.4. Detection ways

In cyber risk management, some threats can be detected, and others very difficult or not at all. If a free malware removal tool is used, it will monitor the device in real time to detect, block, and remove viruses and other malware (Avast).

To detect **worms** a computer worm detection system can be used, which determines whether the anomalous behavior is caused by the computer worm and can determine an identifier for detecting the computer worm based on the anomalous behavior. The computer worm detection system can also generate a recovery script for disabling the computer worm or repairing damage caused by the computer worm (Vigderman & Turner, 2022; Patents).

Trojans run software in the background that cannot be seen and uses precious computing power. They can install programs that cause pop-ups to appear on your screen, sometimes asking for login or banking information, or they can harvest information (Levin, 2022).

Ransomware cannot be detected. The only solution is to always have spare copies (Brewer, 2016; Cisa).

Breach detection tools (also known as intrusion detection tools) are used to detect data breaches, which can help identify network threats. They are software or hardware products capable of recognizing active threats and alerting relevant security personnel that they need to take action. These types of tools can monitor the network and send an alert if they suspect:

suspicious user behavior, network vulnerability or threats in applications and programs (Nibusinessinfo).

When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring (Sikorski & Honig, 2012).

Spyware removal is made possible by solutions that can identify and remove malicious files, such as robust cybersecurity software that provides complete spyware removal, deep cleans spyware-affected devices, and repairs any files or systems that may be infected (Fortinet).

As for **DoS attacks or DDoS**, they are very difficult to detect, due to the random distribution of the attack systems (often worldwide), as the target is attacked from many locations at once, as well as due to the unique characteristics of the threats (Paloaltonetworks; Onelogin).

2.5. Prevention & risk avoiding

Before facing the damages and losses caused by cyber attacks, the management of organizations must design a strategy and implement a plan to prevent and avoid the risks of infection of any digitized devices (Cyberproof). The most common 10 actions that should be included in the strategic plan are presented in figure 3.

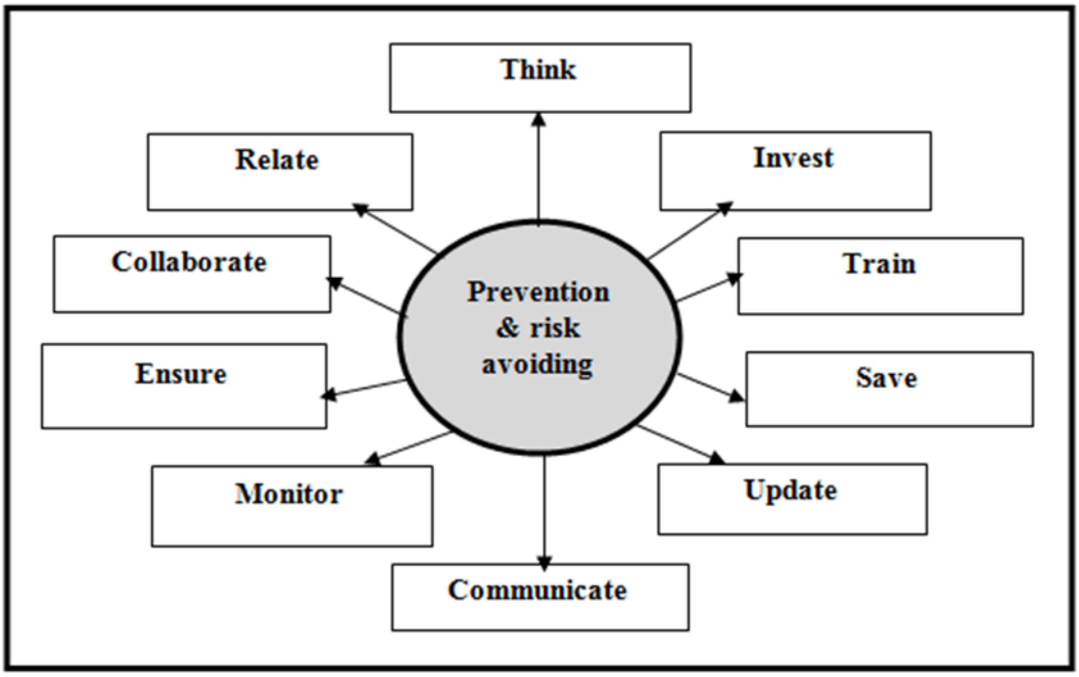

Fig. 3 The 10th actions to prevent and avoid cyber risks

Source: the authors' concept

A manager must use the following actions in his preventive and risk avoidance strategy of cyber threats: think, invest, train, save, update, communicate, monitor, ensure, collaborate and apply diplomacy in relationships:

- Think like a hacker and be continuously warned about the dangers and prepared to act immediately, called "Zero trust access" (Fortinate).
- Invest in attack risk detection software, as well as in a security protocol that encrypts the in-transit data exchanged between the web browser and the client-server for networking, cloud and network operations.
- Periodically provide the staff with the necessary training.
- Continuously save data and professional information on verified external devices.
- Update the necessary software.
- Communicate any anomaly that occurs in the system.
- Continuously monitors the security of system entries.
- Take out an insurance policy for risk transfer.
- Collaborate with stakeholders and conclude alliances that include "the security levels of individual members and their defence capabilities" (Szyłkowska, 2022).
- Apply diplomacy in relations, especially "between international institutions with strategic status" (Borek et al., 2022).

In order to maintain and improve compliance with data protection legislation and good practice, organizations can implement the ISO/IEC 27001 standard, which is used worldwide as a yardstick to indicate effective information security management. It is the only generally recognized certification standard for information and cyber security (Bsigroup).

2.6. Cybersecurity risk management

Cybersecurity risk management is an ongoing process of identifying, analyzing, evaluating, and addressing your organization’s cybersecurity threats. It needs holistic perspective necessary to address risk in a comprehensive and consistent manner (Hyperproof).

As in the case of any risk, cyber risk management is not the task of a team but the responsibility of the entire staff of an organization. Cyber risk management is iterative and includes 6 basic processes:

- risk analysis - understand the specific threats to your business
- risk strategy - determine the processes and controls your business needs
- implementation of risk solutions - deploy the necessary cyber security measures
- risk training - educate staff about their role in managing cyber risks

- monitoring - review and test effectiveness of your security measures
- risk transfer - consider insuring against cyber risks and plan for contingency

Following these established IT risk management processes will help to build resilience and ability to prevent, detect and respond to cyber threats in a way that minimises business disruption and financial loss (Nibusinesinfo). Information security management encompasses many areas, from perimeter protection and encryption to application security and disaster recovery (techtarget).

In order to protect systems against cyber attacks, managers of organizations usually refer to standards for certification and to so-called good practices, such as: Generally Accepted Information Security Principles (GAISP) developed in ISO standards series 27000 and OECD Guidelines for the Security of Information Systems of Government Commerce (OECD.org) (https://www.oecd.org/sti/ieconomy/2494779.pdf), which provides governments, business and individual users with guidance for protecting the security of information. Among the most used standards and good practice guides, we mention (table 3):

Table 3 Standards and good practice guidelines for cyber security management

No	Name	Content
1	ISO 27000 Series standards Examples:	It has 60 standards covering a broad spectrum of information security issues. The compliance with the standard is established through audit and certification processes, typically provided by third-party organizations approved by ISO and other accredited agencies.
	ISO 27000	It is an overview and vocabulary and it define information security management system (ISMS) program requirements.
	ISO 27001 and 27002	It establishes the requirements and procedures for creating an ISMS
	ISO 27018	It addresses cloud computing
	ISO 27031	It provides guidance on IT disaster recovery programs and related activities
	ISO 27037	It addresses the collection and protection of digital evidence
	ISO 27040	It addresses storage security
2	ISO/IEC Standard 15408 European Union	Standard containing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. ISO/IEC 15408-

		1/2/3:2005 - Information technology — Security techniques — Evaluation criteria for IT security
3	ISO/IEC 15408-1:2022	This document establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.
4	ITSEC	The Information Technology Security Evaluation Criteria (ITSEC is a structured set of criteria for evaluating computer security within products and systems
5	TCSEC	The Trusted Computer System Evaluation Criteria (TCSEC) book is a standard from the United States Department of Defense that discusses rating security controls for a computer system. It is also often referred to as the “orange book.”
6	NIST SP 800-53	It is the information security benchmark for U.S. government agencies and is widely used in the private sector; it helps the development of information security frameworks.
7	NIST SP 800-171	It has gained popularity due to requirements set by the U.S. Department of Defence regarding contractor compliance with security frameworks. Government manufacturers and subcontractors must have an IT security framework to bid on federal and state business opportunities.
8	NIST CSF	The NIST Framework for Improving Critical Infrastructure Cybersecurity, or NIST CSF, was developed to address U.S. critical infrastructure, including energy production, water supplies, food supplies, communications, healthcare delivery and transportation.
9	NIST SP 1800 Series	It is a set of guides that complement the NIST SP 800 Series of standards and frameworks. The SP 1800 Series of publications offers information on how to implement and apply standards-based cybersecurity technologies in real-world applications.
10	COBIT	It is a broad and comprehensive framework that has been developed to support understanding, designing and implementing the management and governance of enterprise IT. defines the components and design factors to build and sustain a best-fit governance system. The latest version is COBIT 2019 providing 40 processes.
11	CIS Controls	The Center for Internet Security (CIS) Critical Security Controls, Version 8 lists technical security and operational controls that can be applied to any environment. it is focused on reducing risk and increasing resilience for technical infrastructures.

12	HITRUST Common Security Framework	The HITRUST Common Security Framework includes risk analysis and risk management frameworks, along with operational requirements. The framework has 14 different control categories and can be applied to almost any organization.
13	GDPR	It is a framework of security requirements that global organizations must implement to protect the security and privacy of EU citizens' personal information. Its requirements controls for restricting unauthorized access to stored data and access control measures, such as least privilege, role-based access and multifactor authentication.
14	COSO	COSO is a joint initiative of five professional organizations. A guidance paper, "Managing Cyber Risk in a Digital Age," offers advice on how to prepare and respond to enterprise cyber threats. It aligns with the COSO Enterprise Risk Management Framework.

Sources: (Kirvan & Granneman (2021); Harisaiprasad, K. (2020); iso.org; enisa.europa.eu; itsec; technopedia.com).

3. Proofs and trends

Proofs

It is no doubt that the cyber crime represents the most dengerous threat for any organization's management. Cyberattacks are a serious threat to businesses in all industries. However, some industries are more vulnerable than others.

If the most vulnerable sectors take steps to improve their cyber security, they can reduce the risk of being targeted by hackers. The most used software is windows, so that the heckers prefere it to attack (Kraus et al. 2010; Monnappa, 2018; Editorial Desk, 2022).

Statistics made by different specialized companies provide evidence in support of these statements. Some of these are illustrated below.

- A survey conducted in the US, UK, Benelux, Scandinavia, Australia and New Zealand, reveals the sharp decrease in the effectiveness of organizations' IT security posture prior to COVID-19 and due to COVID-19 from 71% to 44% (Ponemon Report, 2020).
- Beamer (2022) found that some groups of hatchers are more active than others (table 4).

Table 4 Hackers' activty in 2021.

Hackers	**Outsiders**	**Organized criminal groups**	**Internal bad actors**	**Four or more attakers**	**Multiple partners**	**Partners**
Activity	70%	55%	30%	4%	1%	1%

Source: (Beamer, 2022)

- The origin of the most dangerous cyber-attacks is presented by DavidPur (2022) from the study carried out by the Cyber Threat Intelligence (CTI) team (fig. 4) identify the most common origins of cyber-attacks, basing our research on the verified indicators seen during attacks.

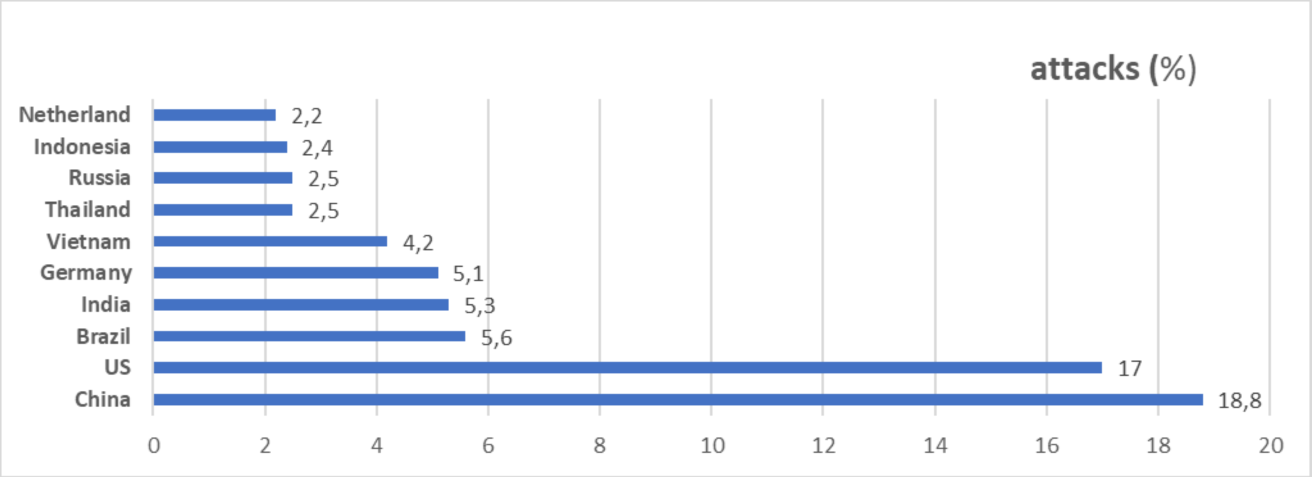

Fig. 4 The origin of the most frequent cyber attacks

Source: (DavidPur, 2022)

- A study conducted by Avira in 2021 (Avira) reveals that in 2020 the number of cyber-attacks reaches an average of 100 million per month. (Gatefy, 2021) According to the study, Germany, U.S. and France are the countries most targeted by attackers. The 10 countries most targeted by hackers in the first half of 2020 in fig. 5.

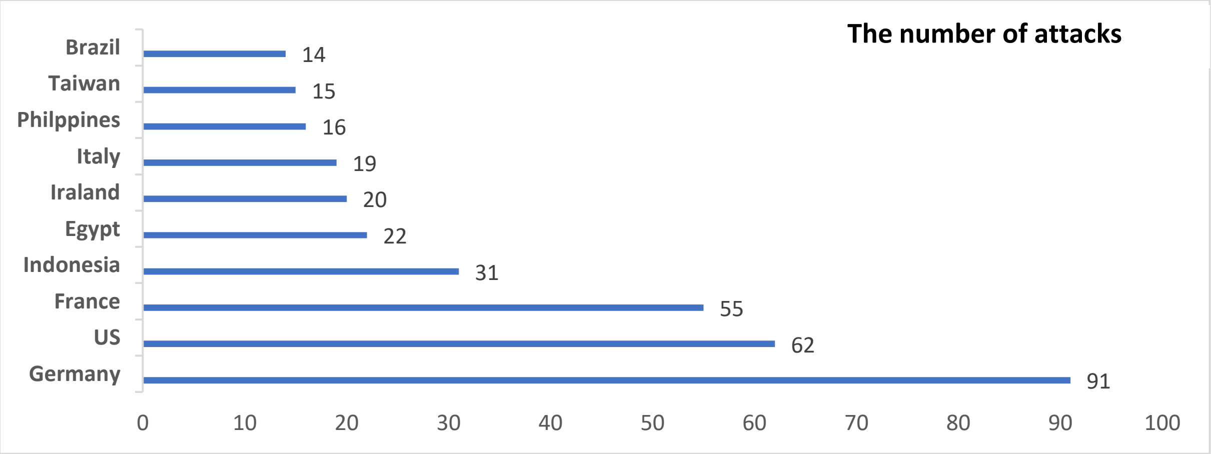

Fig. 5 The 10 countries most targeted by hackers

Source: (Gatefy, 2021)

It is also important that the Australian government announced that the market for IoT security is expected to reach 18.6 billion in 2022, a significant increase from 15.8 billion in

2021. This is due to the increasing number of connected devices which will require serious protection. According to Cybercrime Studies, 43% of cyberattacks are aimed at small businesses in; Australia, but only 14% are prepared to defend themselves (Editorial desk).

The cybersecurity management faced new challenges due to remote work during the pandemic.

- The 2021 Ponemon Institute report presents the main problems encountered due to the low responsibility of remote employees, the lack of necessary skills and physical security, causing damage by infecting the devices used (table 5).

Table 5 The security risks organizations are most concerned about with having half of their workforce working remotely

Security risks	**%**
A lack of physical security in the teleworker's workplace	47
Teleworkers lose or have their devices stolen	32
Criminals could gain control of teleworkers' devices to steal sensitive and confidential data	24
Criminals could leverage the devices to gain access to the enterprise network	24
The inability to secure communications on external networks outside your organization's control	23
The difficulty in securing external access to internal-only resources	20
Phishing and social engineering scams directed at teleworkers	15
Teleworkers' devices become infected with malware	12
The difficulty in securing your organization's network	8

Source: (Report 2021, provided by Ponemon Institute)

In the period Q4 2021 and Q1 2022, which includes Russia's invasion of Ukraine, campaigns of weaponizing cyberthreats against Ukrainian infrastructure. The Trelix Report (2022) reveals "a wide variety of ransomware threats, including families, techniques, countries, sectors, and vectors that increased from Q4 of 2021 to 289%." Threat actors attempt to remain undetected and are abusing what is already present on a system to deliver payloads including ransomware, beacons, information stealers, and reconnaissance tools". Also, "multi-stage espionage attack on high-ranking government officials, and recently, new threats were identified during Q1 2022 (Trellix, 2022).

- Cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015. The average cost of a single ransomware attack is $1.85 million (McLean, 2022).

Trends regarding cyber threats

Despite all the efforts made by companies specialized in cyber security techniques and methods, specialists believe that the risks of digital attacks are increasing. We mention some of these predictions:

- "IoT attacks alone are expected to double by 2025" (Beamer, 2022).
- Cybersecurity Ventures reports that cybercrime represents the greatest transfer of economic wealth in history. Cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015, at a growth rate of 15 percent year over year (McLean, 2022).
- It is estimated that by 2025, there will be more than 55.7 billion connected devices, and 75% will feature IoT connectivity (Stefanini.com).
- According to the estimates of Cisco, the DoS attacks will increase to 15 million by 2023 (Stefanini).

The 4-5 G Internet connection and the progress in the communication technique used in production, e-commerce, military activity, finance and banks, civil life and all others facilitate the hacker community to find new techniques of cyber weapons against ransom in increasing amounts big. However, it is predicted that by 2030 the 6 G connection system will be perfected, which is designed to introduce much safer security elements (Abdel Hakeem et.al., 2022).

The European Union's strategy reinforces cyber defence coordination and cooperation and building cyber defence capabilities, invests much effort in protecting itself against cyber threats coming from third countries, especially through a joint diplomatic response, and it is 2021-2027, the EU has committed to invest €1.6 billion into cybersecurity capacity and the wide deployment of cybersecurity infrastructures and tools across the EU, for public administrations, businesses, and individuals. (European Union, 2022).

Conclusion

The digital activities allow the emergence and continuous growth of risks for any type of organization. The hackers are grouped in the paper into three categories: useful, enemy and dangerous criminals. Organized criminal groups and terrorists are among the most dangerous in the hacker community. They are located in different countries around the world, especially in China, North Korea and Russia.

Among the most affected industries by the cyber-attacks are e-commerce, health, banks and government institutions.

Among the most frequently used types of attacks are: viruses, trojan hors, worms, ransomware, data breaches, spyware and denial of service (DoS) attacks.

Their detection is possible by analyzing specific symptoms in the functioning of the devices. Practice shows that most organizations do not use means and procedures to ensure them against malicious attacks.

A proper cyber risk management system will certainly protect IoT and make them less susceptible to data loss, financial loss and other unpleasantness. In addition, this system educates the staff to identify vulnerabilities, to prevent and avoid the risks of infection of any digitized devices.

The 10 proposed actions can form the basis of designing a cybersecurity management process.

In the coming years, the cybercrime is expected to increase, but the organizations at all levels became more aware of these threats and take increasingly effective preventive measures.

The paper's objectives are achieved, even if in summary, but they can be the subject of further research, such as the issues of jamming, spoofing, meaconing in military security (how they change and affect military operation).

References

Abdel Hakeem, S.A.; Hussein, H.H.; Kim, H. (2022) Security Requirements and Challenges of 6G Technologies and Applications. Sensors 2022, 22, 1969. https://doi.org/10.3390/s22051969.

Adrian, F. (2012) National and international security objectives: some correlations, Journal of Defense Resources Management, Vol.3, Iss.1 (4), 2012, pp. 113-116.

Akpan F, Bendiab G, Shiaeles S, Karamperidis S, Michaloliakos M. Cybersecurity Challenges in the Maritime Sector. Network. 2022; 2(1):123-138. https://doi.org/10.3390/network2010009.

Borek, R., Woźnica, J. and Malawski, M. (2022) The role of eu public diplomacy in affecting international security in the context of the development of the outer space traffic management, Defence science review, DOI: 10.37055/pno/153381.

Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. Netw. Secur. 2016, 5–9. doi: 10.1016/S1353-4858(16)30086-1.

Carey, M.J. & Jin, J. (2019) Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World, Wiley.

Dahiya, A., and Gupta, B. B. (2020). An economic incentive-based risk transfer approach for defending against DDoS attacks. Intl. J. E-Serv. Mob. Appl. 12, 60–84. doi: 10.4018/IJESMA.2020070104.

Kraus, R., Barber, B., Borkin, M., Alpern, N.J. (2010) Seven Deadliest Microsoft Attacks, ch 7, pp 129-145. https://doi.org/10.1016/B978-1-59749-551-6.00007-8.

Liu, X., Ahmad,S.F., Anser, M.K., Ke, J., Irshad, M., Ul-Haq, J. and Abbas, S. (2022) Cyber security threats: A never-ending challenge for e-commerce, Front. Psychol., 19 October 2022, Sec. Organizational Psychology, https://doi.org/10.3389/fpsyg.2022.927398.

Monnappa K. A. (2018) Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, Packt Publishing.

Negulescu, O. (2015) Threats and opportunities in actual defence management in Proceedings of The 10th International Scientific Conference "Defence resources management in the 21st century" Braşov, 2015, National Defence University „Carol I" publishing house Braşov, pp. 205-214.

Radomska, A. (2021) Development directions of cybersecurity in aerospace, Defence science review, DOI: 10.37055/pno/147400.

Sikorski, M. & Honig, A. (2012) Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press.

Szyłkowska, M. (2022) Attributes of cyber conflict in the context of armed conflict – an outline of the problem, Defence science review, DOI: 10.37055/pno/148424.

Electronic sources

Aura, Types of cyber attacks, Available at: https://www.aura.com/learn/types-of-cyber-attacks.

Avast, What Is a Computer Virus and How Does It Work? Available at: https://www.avast.com/c-computer-virus.

Avira, Available at: https://www.avira.com, Study, in Gatafy, 2021.

Beamer, T. (2022) What Industries Are Most Vulnerable to Cyber Attacks In 2022?, Available at: https://www.techbusinessnews.com.au/what-industries-are-most-vulnerable-to-cyberattacks-in-2022/.

Bedell, C., Loshin, P., Hanna, K.T. (2022) Computer Worm, Available at: https://www.techtarget.com/searchsecurity/definition/worm.

Bsigroup, Standards for IT and cyber security, Available at: https://www.bsigroup.com/en-GB/Cyber-Security/Standards-for-IT-and-cyber-security/.

Checkpoints, What is Ransomware?, Available at: Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/.

Cloudmask, Data Breaches: Threats and Consequences, Available at: www.cloudmask.com/blog/data-breaches-threats-and-consequences.

Corero Marketing (2021) The Damaging Impacts of DDoS Attacks, Available at: https://www.corero.com/the-damaging-impacts-of-ddos-attacks/

Cyberproof, Managed threat intelligence, Cyber Threat Intelligence (CTI) team, pdf, Available at: https://www.cyberproof.com/managed-threat-intelligence/.

Cyber war and Ukraine, Available at: https://www.csis.org/analysis/cyber-war-and-ukraine.

DavidPur, N. 2022, Which Countries are Most Dangerous? Cyber Attack Origin – by Country, Available at: https://blog.cyberproof.com/blog/which-countries-are-most-dangerous.

Editorial Desk 2022, Australian Cyber Security Concerns Continue to Rise In 2022, Available at: https://www.techbusinessnews.com.au/australian-cyber-security-concerns-continue-to-rise-in-2022/

Embroker, Top 10 Cybersecurity Threats in 2022. Available at: https://www.embroker.com/blog/top-10-cybersecurity-threats-2022/.

European Union (2022) Cyber Defence: EU boosts action against cyber threats (European Commission). Available at: https://www.consilium.europa.eu/en/policies/cybersecurity/.

Ethical Hacking tutorial, https://www.javatpoint.com/ethical-hacking.

Famous hackers, https://www.javatpoint.com/famous-hackers.

Fortinet, What is Spyware? Available at: https://www.fortinet.com/resources/cyberglossary/spyware.

Fruhlinger, J. (2020), Ransomware explained: How it works and how to remove it, Available at: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

Gatafy (2021) Which countries are most targeted by hackers?, Available at: https://gatefy.com/blog/which-countries-are-most-targeted-hackers/.

Generally Accepted Information Security Principles (GAISP), https://www.lawinsider.com/dictionary/gaisp.

Gillis, A.S., Bush, K, Teravainer, T. Spyware, Available at: https://www.techtarget.com/searchsecurity/definition/spyware.

Gutiérrez, N. (2021) Top 5 Cyber Security Threats Today, Available at: https://preyproject.com/blog/top-5-current-cyber-threats-in-2020-malware-phishing-ransomware.

Harisaiprasad, K. (2020) COBIT 2019 and COBIT 5 Comparison, Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison.

Hyperproof, Cybersecurity Risk Management: Frameworks, Plans, & Best Practices, Available at: https://hyperproof.io/resource/cybersecurity-risk-management-process/.

ISO/IEC Standard 15408, Available at: https://www.enisa.europa.eu/topics/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-15408.

ISO/IEC 15408-1:2022, Available at: https://www.iso.org/standard/72891.html.

ITSEC, Available at: https://itsec.group/.

Kasperky, Ransomware attacks and types, Available at: https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types.

Kirvan, P & Granneman, J. (2021) Top 10 IT security frameworks and standards explained, Available at: https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one.

Komnenic, M. 2022, 98 Biggest Data Breaches, Hacks, and Exposures [2022 Update], Available at: https://termly.io/resources/articles/biggest-data-breaches/.

Levine, N. (2022) How to Tell if Your Computer Is Infected by a Trojan Horse, Available at: https://www.wikihow.com/Tell-if-Your-Computer-Is-Infected-by-a-Trojan-Horse.

Malwarebytes a., Trojan horse – Virus or malware? Available at: https://www.malwarebytes.com/trojan.

Malwarebytes b., What is a computer worm? Available at: https://www.malwarebytes.com/computer-worm.

Malwarebytes c., Randsomware, Available at: https://www.malwarebytes.com/ransomware.

Manship, R. (2022) The Top 6 Industries At Risk For Cyber Attacks, Available at: https://www.redteamsecure.com/blog/the-top-6-industries-at-risk-for-cyber-attacks.

McLean, M. (2022), Must-Know Cyber Attack Statistics and Trends, Available at: https://www.embroker.com/blog/cyber-attack-statistics/.

Nibusinessinfo, Cyber security risk management, Available at: https://www.nibusinessinfo.co.uk/content/cyber-security-risk-management.

OECD Guidelines for the Security of Information Systems of Government Commerce, Available at: https://www.oecd.org/sti/ieconomy/2494779.pdf.

Onelogin, What is a DDoS Attack? Available at: https://www.onelogin.com/learn/ddos-attack.

Paloaltonetworks, What is a denial of service attack DoS, Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

Patents, System and method of detecting computer worms, Available at: https://patents.google.com/patent/US8528086B1/en.

Redteamsecure, The top 6 industries at risk for cyber attacks, Available at: https://www.redteamsecure.com/blog/the-top-6-industries-at-risk-for-cyber-attacks.

Stefanini, Cyber Security Statistics For 2022: List Of Data And Trends, Available at: https://stefanini.com/en/insights/articles/cyber-security-statistics-for-2022-data-and-trends.

Stop ransomware, Available at: https://www.cisa.gov/stopransomware.

Taylor, H. (2021) What Are Cyber Threats and What to Do About Them, Available at: https://preyproject.com/blog/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them.

Techtarget, Available at: https://www.techtarget.com/searchsecurity/definition/worm.

Tietsort, J.R. (2022) The 15 Types of Hackers You Didn’t Know About, https://www.aura.com/learn/types-of-hackers.

Trellix, What Is Ransomware? Available at: https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html.

Trendmicro, Data Breach, Available at: https://www.trendmicro.com/vinfo/us/security/definition/data-breach.

Trusted Computer System Evaluation Criteria (TCSEC), Available at: https://www.techopedia.com/definition/2623/trusted-computer-system-evaluation-criteria-tcsec.

Veracode, Spyware, Available at: https://www.veracode.com/security/spyware.

Vigderman, A. and Turner, G. (2022) What Is a Computer Worm?, Available at: https://www.security.org/antivirus/computer-worm/.

Ward, M. & Subramanian, S. (2021) States at risk: The cybersecurity imperative in uncertain times, Available at: https://www2.deloitte.com/us/en/insights/industry/public-sector/nascio-survey-government-cybersecurity-strategies.html.