Cybersecurity and Cyber Defense Insights: The Complementary Conceptual model of Cyber resilience

Darko Možnik
Zagreb University of Applied Sciences, Croatia
Damir Delija
Zagreb University of Applied Sciences, Croatia
Domagoj Tuličić
Zagreb University of Applied Sciences, Croatia
Darko Galinec
Zagreb University of Applied Sciences, Croatia

Abstract

Cybersecurity planning within a complex system and applying its principles aims to achieve system resilience in cyberspace. The purpose of a complex system is to carry out a mission as a set of abilities and preferences concerning the internal and external circumstances of the system. Achieving cyber resistance requires organizational, human, material, and financial resources to implement measures, activities, and procedures to reduce residual (remaining) security risk. This part of the security risk must be accepted within the system since it is impossible to achieve its further reduction. The research in this paper analyzes ways and means to achieve cyber resistance in the conditions of today's growing security risks. This research aims to create a new model of cyber resistance, which includes cyber and information security. This also considers that the methods of separating previously unseen threats and attacks of the past day are unknown today in a large number of business cases. To confront the challenges, there is a need to create "knowledge about ignorance" and the development of cyber capabilities based on the principles of cyber security and defense.

Keywords: attribution, cyber defense, cyber resilience, cyber security, conceptual model
JEL classification: A12, O14, R11

Paper type: Research article
Received: 04 April 2023
Accepted: 01 May 2023

DOI: 10.54820/entrenova-2023-0001

Introduction

This paper aims to create a conceptual model of cyber resistance as a capability of a complex system in cyberspace. The model was created by structuring information protection measures and determining the mutual conditionality and connection of its components (cyber security as a process, information security as a state, and cyber defense as a procedure and mechanism). The work aims to investigate the vulnerability, threats, and risks that come from cyberspace every day and to enable and contribute to awareness of the need to achieve the cyber resilience of a complex system through knowledge of the behaviour and interaction of its components. In doing so, risk management is particularly highlighted: a process that should reduce the level of unfamiliarity and unknowingness of the behavioural system to the minimum possible extent. To achieve the goal, a conceptual modelling process was used to create a system resilience model in cyberspace based on the criterion of the type of cyber threat.

By applying different scenarios, observing the behaviour of the system and comparing the results, the model becomes suitable for determining the state (known knowns, known unknowns, unknown unknowns) of the system during cyber threats, as well as choosing a strategy for action and timing, supporting decision-making about tactics/actions to be taken within the system.

Literature review

According to the Croatian Parliament (2007) specific terms in terms of this Act have the following meaning:

- Information security is the state of confidentiality, completeness, and availability of data, which achieves the application of prescribed measures and standards of information security and organizational support for planning, implementation, verification and refinement of measures and standards.
- Information security measures are general data protection rules implemented at the physical, technical, or organizational level.
- Information security standards are organizational and technical procedures and solutions intended to implement prescribed information security measures systematically and uniformly.
- Areas of information security represent a part of information security in five areas with the aim of systematic and practical realization of adoption, application and monitoring of information security measures and standards.
- Security accreditation of an information system is a procedure in which the ability of bodies and legal entities to manage the security of an information system is determined, and it is carried out by determining the applied measures and standards of information security.
- A cyber threat is any possible circumstance, event, or action that could damage, disrupt or otherwise negatively affect network and information systems, users, and other persons.
- Cyber threats are continuously increasing globally, and different cyber attacks in cyberspace are becoming more sophisticated and complex, affecting our daily lives and business.
- Cybersecurity includes activities and measures that achieve the credibility, integrity and availability of data and systems in cyberspace.
- Cyber security is a system of organizational and technical activities and measures that achieve the authenticity, confidentiality, integrity and availability of data and network and information systems in cyberspace.

- Cyberspace is a virtual space within which communication occurs between network and information systems and includes all network and information systems, regardless of whether they are connected to the Internet.

According to Braman and Vincenti (2009) information Space is a collection of information not limited by source, form, process, semantics, or application.

Cyber Defense

There are no universally accepted definitions of cyber terms - they are used in different circumstances, given that they have different meanings (The NATO Cooperative Cyber Defense Center of Excellence, 2017).

Cyber defense is aimed at preventing, detecting and providing a quick response to attacks and threats so that there are no changes to infrastructure or information. With the increased volume and complexity of cyber-attacks, the defense has become essential for most entities to protect sensitive information and safeguard assets (Galinec et al., 2017a).

Cybersecurity strategy and risk management

The European Union has taken some measures to regulate relations in cyberspace while increasing resilience and strengthening its cyber security preparedness. Contemporary aspects of cyber security are subject to rapid change. The speed, variety and sophistication of cyber-attacks are changing dramatically. Many states consider cyber capabilities, diplomacy, and economic and military power as strategic tools.

Attribution

Establishing attribution for cyber operations is difficult but not impossible. There is no simple technical process or automated solution for determining responsibility for cyber operations. The painstaking, complex work often requires intelligence and forensic analysis over weeks or months to assess guilt. In some cases, the international community can determine online attribution within hours of the incident, but the accuracy and reliability of the attribution are based on available data. Analysts can assess responsibility for a cyber-attack in three ways: (i) by place of origin, such as a specific country; (ii) to a specific digital device or person on the Internet; and (iii) according to the individual or organization that performed the activity.

The third category is often the most difficult to assess because it is necessary to link malicious cyber activities to specific individuals and assess their sponsors and motivators.

Attributing an attack to a specific country or actor requires collecting as much data as possible to link online actors, individuals and other entities. Since this often results in hundreds of conflicting indicators, key indicators are identified for timely and accurate attribution. For are:

- Intention. It also relies on indicators from external sources, such as open-source reports from private cybersecurity companies.
- Behaviour in terms of applying techniques, methods and technologies is often used to carry out a cyber-attack or espionage. This is the most important indicator because it is more difficult to change habits than technical tools.
- Infrastructure: physical and/or virtual communication structure used to deliver cyber capabilities or to maintain and control capabilities.
- Malware: Malicious software designed to enable unauthorized functions on a compromised computer system, such as key logging, screen capture, audio recording, remote control, and persistent access control.

- Intent: An attacker's commitment to performing specific actions based on context. Covert, deniable cyberattacks are often launched against adversaries before or during regional conflicts or serve to suppress or harass an adversary state.

Indicators from external sources: reports from private industry, the media, academia and research centres are also used to provide such data or share hypotheses about perpetrators.

Best practices for determining attribution are looking for human error, timely cooperation, sharing of information and documentation, and a strictly analytical approach.

The context of cyber resilience

Cyber capabilities

Espionage enabled in cyberspace, whether at the strategic or operational level, can compromise the credibility of information and information systems, potentially revealing secret and sensitive information to adversaries. Second, sabotage enabled in cyberspace can have significant physical consequences, especially regarding critical infrastructure or manipulating data to confuse and undermine decision-making and command.

Bearing this in mind, it is necessary to systematically develop cyber defense capabilities based on an action plan that will define the bearers of individual measures, deadlines, necessary financial resources, and indicators of implementing individual measures.

Measures for the development of cyber capabilities can be divided into three areas:

- cyber defense policy and strategy
- organization and capabilities of cyber defense
- education and training for cyber defense.

Conceptual model of cyber resilience

The cyber risk that must be accepted at the moment of observation can no longer be acted upon in terms of reduction is determined by assessing the lack of risk/compliance.

According to Galinec et al. (2017a), cyber security alone is no longer enough to reduce risk: there is a need for a defense strategy, prevention and response. In its basic form, resilience is an assessment of what will happen before, during and after a networked system is faced with a threat. Resilience should not be synonymous with "recovery". It is not specific to the event but grows long-term and should be included in the overall organizational and business strategy. Resilience in the context of a system's and an organization's ability to withstand cyber events refers to the preparations concerning threats and vulnerabilities, the defenses put in place, and the resources allocated to mitigate security incidents once they occur. The key is normalization.

A cyber-resilient approach ensures greater readiness and less repetition, making it more efficient and effective overall. In contrast to resilience, security can be viewed in a binary way. Something is or is not safe. It is usually assigned to a single, limited technical function, keeping unauthorized users out of a networked system.

While there are many definitions of cybersecurity, there is a difference between access control and the long-term, more focused strategic mindset that cyber resilience should foster (Galinec et al., 2017a).

Combating known threats is a vital part of a cybersecurity strategy. It goes hand in hand with advanced capabilities to predict, capture and learn from unknown threats. Systems have different weak points and processes (challenges) and manage risk in their own way (solutions). In other words, every security challenge (assessed as "known" or "unknown") has a corresponding solution. By including the values of the models obtained during the security risk assessment, we get "known acquaintances" related to cyber security and "unknown unknowns" related to cyber resilience.

An APT typically refers to an organization (e.g. a government) with the intent, goal, and capability to persistently, effectively, and efficiently attack a specific target. The techniques and tactics used by attackers are constantly evolving, and cyber threats encompass a range of malicious activities.

To cope with the growing challenges that today manifest as unknown unknowns, systems strive to train personnel and develop new organizational processes and technologies. The starting point of the breakdown for the design and creation of the model is the criterion of the type of cyber threat (CIA, APT, zero-day) of the complex system. The model is shown in Figure 1. According to Galinec et al. (2017b), we observe and distinguish the following terms:

Cyberspace: the virtual space within which communication occurs between network and information systems and includes all network and information systems, regardless of whether they are connected to the Internet (Croatian Parliament, 2018).

Cyber-resilience: the ability of a system, organization, mission or business process to predict a cyber-attack, withstand, recover and adapt its capabilities when facing an adversary in cyberspace (Galinec et al., 2017b).

Cybersecurity: a system of organizational and technical activities and measures that achieve the authenticity, confidentiality, integrity, and availability of data, as well as network and information systems in cyberspace (Croatian Parliament, 2018).

Information security: confidentiality, completeness, and data availability (Galinec et al., 2017b).

Network and information system:

(a) an electronic communication network defined by the law governing electronic communications.

(b) any device or group of connected or related devices, one or more of which programmatically performs automatic processing of digital data or

(c) digital data that is stored, processed, obtained or transmitted by the elements described in points (a) and (b) for their operation, use, protection and maintenance (Croatian Parliament, 2018).

Security of network and information systems: the ability of network and information systems to resist, at a certain level of reliability, any action that threatens the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or related services that these network and information systems offer or provide access to (Croatian Parliament, 2018).

Information security (CIA trinity of threats and response to them, i.e. known knowns), cyber security (not CIA complex threats, APTs and corresponding responses, i.e. known unknowns) and cyber resilience (unpredictable threats and responses, i.e. unknown unknowns) represent types of attacks as criteria according to which we distinguish information security from cyber defense, cyber security as a superset of information security and, ultimately, cyber resilience as a goal and a superset of all previously mentioned terms.

The areas of information security with prescribed security measures and standards are:

- security check,
- physical security,
- security information,
- information system security,
- security of business cooperation (Croatian Parliament, 2007).

Information system security refers to the protection of the communication and information system through the implementation of information security measures and standards, and it includes:

- fulfilment of information security requirements
- security of operating systems and user programs and development safety,
- are security-related architecture,
- technological research and development in the communication and information system
- planning with constitutional requirements for security
- testing and evaluation
- system development.

Further insight into the processes leads to cyber defense against threats and risks coming from cyberspace.

Cyber Defense: A computer network defense mechanism that includes responding to actions and protecting critical infrastructure and information protection for organizations, government entities and other possible networks (Galinec et al., 2017b).

A cyber-attack is an act or action initiated in cyberspace to disrupt, deny, degrade or destroy by compromising communication, information and other electronic systems or data stored, processed or transmitted on these systems.

Cyber operations consist of many functions, processes, and activities encompassing cyber governance, cyber-attack, cyber exploitation, and cyber defense. By their nature, these activities are proactive, defensive, and regenerative.

Namely, the following types of cyber operations take place in cyberspace:

- defensive, i.e., defensive cyber operations,
- offensive,
- intelligence,
- operational preparation of the environment.

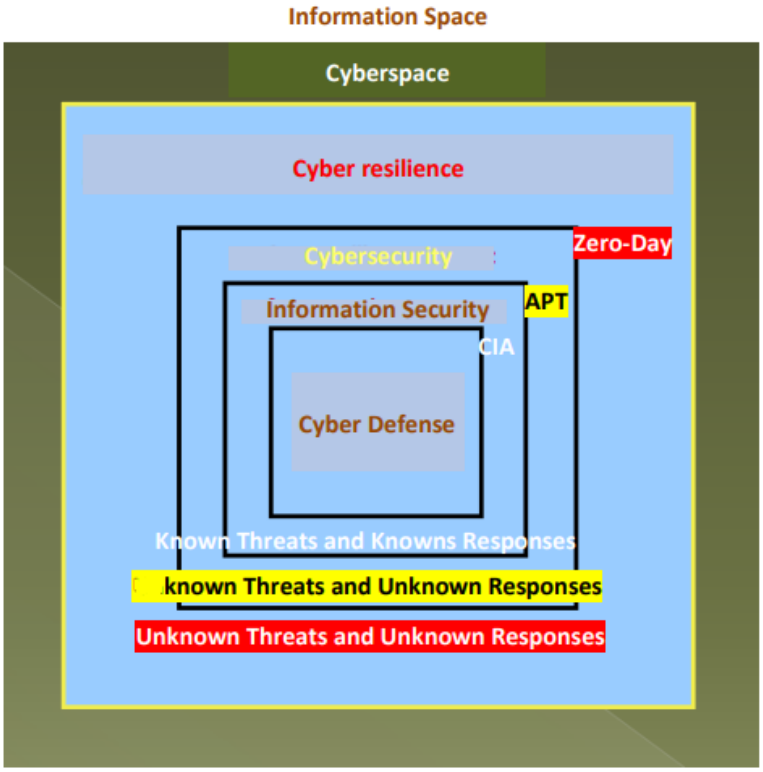
Furthermore, DCOs contain active and passive measures for maintaining the ability to use cyberspace, and we distinguish between:

- Active defense, refers to activities aimed at mutual offensive cyber operations to maintain freedom of maneuver (movement) within cyberspace and
- Passive defense refers to measures of the corresponding type of threat to reduce the effectiveness of the adversary's cyber activities.

Active cyber defense, as a subset of cyber defense focuses on integrating and automating many services and mechanisms for executing operational responses in cyber time.

Among the many needs of combat personnel, there is the need for security, which includes the concepts of reinforcement, protection, attack, and defense between combat personnel domains by land, sea, air, space, and cyberspace. Cyber capability is integrative to other domains. At the same time, it is an independent domain with unique cyber defense needs (Herring and Willett, 2014).

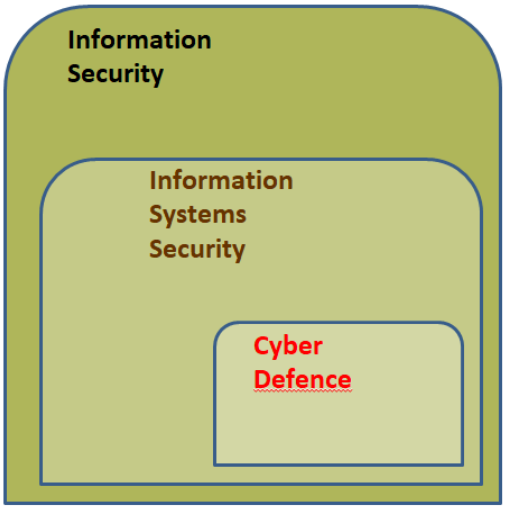
Figure 1
Conceptual model of cyber resilience



Source: Author's illustration

We recognize it as part of the conceptual model of cyber resilience, and it is in information system security (Figure 2).

Figure 2
Cyber defense in the context of security



Source: Author's illustration

Development and achievement of cyber resilience

Successful implementation of cyber security and cyber defense measures and procedures will result in an effective risk management process, i.e. a reduction in the

level of risk that must be accepted since it cannot be eliminated within the information and communication system, increasing cyber resistance.

Cyber security is an integral part of the development of the digital society; the development of personnel, processes, rules and technologies is necessary to perform interconnected, complete business processes "from end to end" of the organization.

To enable all of the above, it is necessary to achieve technical, semantic, procedural and legal interoperability between entities exchanging data, information and knowledge, taking into account and applying the principles of cyber security and cyber defense at all mentioned levels of interoperability within the architecture of information and communication systems of triggered events, architecture aimed at the provision of services or some combination thereof (EDSOA), for the development of the digital society.

The security operations center was created to increase the security of information and communication systems and achieve appropriate protection against advanced threats.

To respond to new requirements and achieve safe processing of complex business (security) events, there is a need to establish appropriate processes, rules and technologies, as well as a dedicated team in charge of security supervision, security systems and security incident management for the establishment of a security operations center at the level of the organization.

Selected new research results on digital transformation and security

Account takeover

In F5 (2022) it is stated that account hijacking remains the most widespread and costly attack targeting financial institutions, e-commerce companies and many other organizations. Once the account is compromised, the fraudster can drain their bank accounts of funds, purchase goods or services, access payment information for use on other sites, or engage in other malicious activity.

Security Strategy Status Report

According to F5 (2022), nearly 1,500 IT decision-makers from organizations worldwide responded to an eight-year survey on the current state of strategy implementation. The data was collected over three weeks in September and October 2021.

This year's results include priorities from a wide range of industries, with cloud service providers, manufacturing, and education more represented than in the past. Technology, financial services and retail, distribution or professional services firms were also well represented. Individuals from organizations of all sizes participated, providing insight into their current IT activities, challenges, and expectations for the next few years. While the results reflect a few exciting variations between regions or industries, they provide a reliable snapshot of the perspective, needs and direction of a typical IT organization today.

The research findings show how IT decision-makers still face constraints related to modernization, business imperatives and implementation methods while reaping the benefits of digital transformation. Organizations continuously search for a balance between control, cost, user experience and security of applications and application programming interfaces.

The main findings include:

- modernization is spreading to less visible business processes and "back office" functions,

- data-centric information systems and operational technology systems are converging,
- almost all respondents state that they lack critical insights from existing systems,
- complexity becomes unsustainable, hinders performance and degrades the user experience,
- safety evolves in risk management because performance is still the most important,
- repatriation is increasing, moving applications back into the data centre from the cloud.

Security has become a significant trend. The trend is partly a response to the explosion of microservices that merge into queues of "users" whose identities require verification, even if those workloads only communicate within a single data centre. API security is also maturing, with organizations taking different approaches, which can be grouped into traditional, modern and adaptive:

- Less than half of respondents said they value traditional methods, including encryption and decryption, speed limit checking, and checking procedures to reduce the most critical security risks for web applications (OWASP Top Ten), which were mentioned by 45%, 33%, and 30% of respondents, respectively.
- The modern approach to user authentication and authorization (AuthN/AuthZ) is considered valuable by 68% of respondents, while 58% appreciate another modern approach, traffic inspection.
- Finally, 59% of respondents appreciate that it is used analysis of behaviour to determine the legitimacy of the user.

In the context of risk reduction, API-centric security is essential today – a security model with the last committee and web protection of applications and APIs.
During the COVID-19 disease, and as part of an attempt to reduce complexity, nine out of 10 organizations are actively adjusting their security postures, raising awareness through training and researching additional solutions and approaches. Key tactics include adopting cloud security, additional employee training, and vendor security consolidation. In the days ahead, most organizations must employ several combined tactics to manage the risk of a security breach adequately.

Further research

By creating a conceptual model, assumptions are made for the determination of all classes and objects (attributes, methods and states), features and processes of a complex system that are important for the successful operation of the specific system to achieve cyber resilience and the gradual evolution of the created model into the logical and physical data model.

The proposal of the new Directive on the security of network and information systems 2 (the "NIS2 Directive") in Article 5, which refers to the national cyber security strategy, requires that the Strategy of the EU member states specifically include:

- Goals and priorities of cyber security
- Consistent management frameworks in cyber security (cyber crises, information sharing, training) and by levels (technical, operational, strategic-political) to achieve the desired goals and priorities, including the policies and responsibilities of various actors, bodies and strategies involved in the implementation.
- Guidelines for identifying relevant cybersecurity assets and risks.
- Determining measures that ensure preparedness, response and recovery from incidents, including cooperation between the public and private sectors

- A policy framework to improve coordination between competent authorities under the NIS2 Directive and the Critical Entity Resilience Directive (to be adopted) to share information on cyber threats, cyber security risks and incidents, as well as on non-cyber threats, risks and incidents and carrying out oversight tasks, as needed.
- Policy framework for coordination and cooperation between competent authorities under the NIS Directive and competent authorities appointed following sectoral legislation.

As part of the national cyber security strategy, the EU member states, in particular, need to adopt specific policies. Operational policies (supply chain for ICT products) must be implemented legislatively (by transposition of the NIS2 Directive). Strategic policies (promoting and developing education and training) must be implemented through a strategy and an action plan. These are the policies:

- Dealing with cyber security in the supply chain for ICT products and services entities use to provide their services.
- Regarding the inclusion and specification of cybersecurity requirements for ICT products and services in public procurement, including cybersecurity certification.
- Vulnerability management includes receiving and facilitating the voluntary coordinated disclosure of vulnerabilities.
- Maintenance of the general availability, integrity, and confidentiality (CIA) of the public core of the open Internet
- Promoting and developing cyber security education and training, skills, awareness and research and development initiatives
- Support to academic and research institutions in the development of tools for cyber security and network infrastructure
- Relevant procedures and appropriate information-sharing tools to support the voluntary exchange of cybersecurity information between companies under EU law.

The above elements address the unique needs of SMEs, particularly those excluded from the scope of the NIS2 Directive, regarding guidance and support in improving their resilience to cyber threats.

Conclusion

Actors of cyber threats, threats and attacks today differ significantly in terms of motivation, sophistication, level of resources at their disposal and depth of specialization. At the same time, applications are becoming increasingly distributed and decentralized, creating a new world of challenges and harms. Cyber security represents effort and action as a game in which no organization can win ultimately. Staying in that game is only possible with a long-term strategy, persistence and constant innovation.

Rapid modernization, under conditions of security convergence, continues in all companies around the world to achieve success, including a complete, reliable, available (accessible) and reliable digital experience, i.e. robust data and business protection, Continuous advances include a more intelligence-based and risk-management approach to security. Sustaining the current momentum of digital transformation requires changes in the areas of people, processes and technology:

- Addressing skills gaps and building expertise in artificial intelligence, machine learning, data management and compliance and creating capable teams for rapid response.

- Process, which includes a broader improvement in adopting security practices to increase the operational efficiency of IT.
- Consolidating a telemetry and management toolset for comprehensive visibility and monitoring, with added security and delivery of technology applications to operate in diverse environments.

This work provides insight into ways, processes and means to achieve cyber security in today's growing security threats and the latest trends in digital transformation, including them. In the context of cyber resilience, a new conceptual model of cyber resilience is presented, including cyber security, information security and information system security and cyber defense. Further research, following the NIS2 and EU Directive, is aimed at finding and using effective processes for agile (adaptive, aware, flexible and productive) cyber resilience of the information system and the attribution, planning, development and implementation of cyber capability equipment and training, training and staff training. The goal is to achieve a state where the system can successfully face unpredictable events (unknown unknowns). The above applies both to its internal and external environment. The same is achieved by continuous and consistent implementation of the described E2E procedures and processes and, consequently, by reducing the level of acceptable risk - by reducing unknown unknowns first to known unknowns and then to be aware of the known systems that work in real-time. During the research, the conceptual modelling method was applied with associated procedures, and a new model of cyber resistance of a complex system in cyberspace was created.

As a scientific contribution, this paper develops and improves the theoretical perspective of cyber resistance. The paper synthesizes existing knowledge, presents it in a new context to stimulate thinking, and proposes a new model for the application.

References

1. Braman, J. & Vincenti, G. (2009). Visual Analytics and Conceptual Blending Theory. Handbook of Research on Computational Arts and Creative Informatics. IGI Global, Inc.
2. Croatian Parliament (2007). Law on Information Security, Official Gazette 79/07.
3. Croatian Parliament (2018). Law on cyber security of operators of key services and providers of digital services. National Gazette 64/18.
4. F5 (2022). Overview. 2022 State of Application Strategy Report. Retrieved from https://www.f5.com/pdf/report/global-state-of-application-services-2022.pdf
5. Galinec, D., Možnik, D., & Guberina, B. (2017a). Cyber Security and Cyber Defense: A Strategic Approach at the National Level. Automatika magazine for automation, measurement, electronics, computing and communications, 8(3), 266-272. doi:10.1080/00051144.2017.1407022
6. Galinec, D. & Steingartner, W. (2017b). A combination of cyber security and cyber defense to achieve cyber resilience. IEEE 14th International Scientific Conference on Informatics - INFORMATICS 2017 (pp. 87-93, 2017). Institute of Electrical and Electronics Engineers, Inc., Poprad Slovakia.
7. Herring, M.J., & Willett, K.D. (2014). Active Cyber Defense: A Real-Time Cyber Defense Vision. Journal of Information Warfare, 13(2), 46–55
8. The NATO Cooperative Cyber Defense Center of Excellence (2017). Cyber definitions. Retrieved from https://ccdcoe.org

About the authors

Darko Možnik, PhD, is an Assistant Professor at the Zagreb University of Applied Sciences, Department of Informatics and Computing. He received PhD in Information Systems at the Faculty of Electrical Engineering and Computing. He received Assistant Professor at the Zagreb University. He works in information security, cyber security and cyber resilience. Darko Možnik published several scientific and professional papers in international and national journals and participated in many scientific international conferences. The author can be contacted at **darko.moznik@tvz.hr**

Damir Delija, PhD, is a senior lecturer at TVZ in digital forensics and cybersecurity. While working in INsig2, he specialized in Guidance Software Encase Enterprise, UNIX, and network forensics. Damir is an EnCase trainer with extensive knowledge of the entire life cycle of Guidance forensics products. He has EnCe and UFED certifications, as requested for the digital forensic trainer, and certifications in Cybersecurity, eDiscovery and EnScript. He has a Ph.D. in Electrical Engineering. He was an AIX system trainer and dealt with ship automatization systems, AIX and UNIX systems administration, and network administration. The author can be contacted at **damir.delija@tvz.hr**

Domagoj Tuličić graduated in Zagreb and founded an IT company. In 2007, he completed his professional studies in Computer Science, majoring in programming at the University of Split. He was employed at the State Administration for Protection and Rescue and completed a university graduate study in Databases and Knowledge Bases in Varaždin. He worked at TVZ as a teacher in Information Security and Digital Forensics. Since 2022, he has been employed at the University of Information Technology as the head of the Department of Computer Systems and Networks and an information security commissioner. The author can be contacted at **domagoj.tulicic@tvz.hr**

Darko Galinec, PhD, is an assistant professor at the Military Study Programmes, University of Zagreb, Croatia. His education includes a BSc in Economic Cybernetics, an MSc Program in Information Engineering, and a PhD in Information and Communications Science at the University of Zagreb. Darko has been in the positions of Programmer, Data processing organizer, Information Systems Designer, Senior Informatics Advisor, Information Systems Design Department Head, and Information and Communications Technology Sector Deputy Head. Current research focus is Cyber Defense, Security and Resilience. The author can be contacted at **darko.galinec@tvz.hr**