Cyber Security and Cyber Defense: Challenges and Building of Cyber Resilience Conceptual Model

DARKO GALINEC
Department of Informatics and Computing
Zagreb University of Applied Sciences
Vrbik 8, Zagreb
CROATIA

Abstract: - Cyber security encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cyber security is distinctive in its inclusion of the offensive use of information technology to attack adversaries. Use of the term cyber security as a key challenge and a synonym for information security or IT security misleads customers and security practitioners and obscures critical differences between these disciplines. Recommendation for security leaders is that they should use the term cyber security to designate only security practices related to the defensive actions involving or relying upon information technology and/or operational technology environments and systems. Cyber defense is a computer network defense mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks [3]. In this paper, we investigate how cyber security and cyber defense may lead to cyber resilience with the novel model of cyber resilience designed and presented. Furthermore, within the same model authors investigate actions for cyber security and cyber defense in conditions of increasing challenge of cyber-attacks and the limited capabilities to respond to this threat describing the process of creation, performance and future of EU Cyber Rapid Response Teams (abbr. CRRT) and Mutual Assistance in Cyber Security, introducing novel approach to cyber security and cyber defense at the EU level.

KeyWords: - CRRT, Cyber Defense, Cyber security, Cyber Resilience, Conceptual Model, Rapid Response Team

Received: April 16, 2022. Revised: November 6, 2022. Accepted: November 28, 2022. Published: December 31, 2022.

1 Introduction

Cyber security has been practiced in military circles for over a decade. In recent years, the term has appeared in a variety of contexts, many of which have little or no relationship to the original meaning of the term. Misuse of the term obscures the significance of the practices that make cyber security a super set of information security, operational technology (OT) security and IT security practices related to digital assets.

A wide range of different activities is involved in cyber defense for protecting the concerned entity as well as for the rapid response to a threat landscape. These could include reducing the appeal of the environment to the possible attackers, understanding the critical locations & sensitive information, enacting preventative controls to ensure attacks would be expensive, attack detection capability and reaction and response capabilities. Cyber defense also carries out technical analysis to identify the paths and areas the attackers can target ,[3].

Awareness along with resilience and response are at the heart of EU action to counter cyber threats. EU is improving the capacity to detect and understand malicious activities at an early stage. At the same time, the EU enhances the resilience of critical infrastructure, society and institutions. This is fundamental to improving the ability to withstand and recover from attacks. Countering cyber threats requires action mainly from the Member States, as well as closer cooperation between the EU, the Member States, partner countries and NATO.

2 Problem Formulation

The aim of this paper is to investigate how cyber security and cyber defense may lead to cyber resilience in today's conditions of emerging security

risks and the limited capabilities to respond to cyber threats. Secondly, the aim is to describe the process of creation and performance of EU Cyber Rapid Response Teams and Mutual Assistance in Cyber Security, introducing a novel approach to cyber security and cyber defense at the EU level.

2.1. Methodology

With the understanding of the specific environment, cyber defense analyses the different threats possible to the given environment. It then helps in devising and driving the strategies necessary to counter the malicious attacks or threats. In this regard the goal is to give perspectives for achieving cyber resilience in today's information-communication environment. Model-driven methodology and method have been used in the creation of the model scheme.

Perspectives for cyber security and cyber defense engagement, aiming to achieve cyber resilience in today's information-communication environment, are given and the novel Conceptual Cyber Resilience Model is created. The paper provides an innovative approach to the modelling of cyber resilience taking into account EU Cyber Rapid Response Teams, CRRT(s) in Cyber Security as one of the possible solutions sharing people (through mutual assistance), processes and technology introducing novel approach to cybersecurity and cyber defense at the EU level.

2.2. Cyber defense

In the run-up to his special operation, the attacker will presumably make wide use of non-military (indirect) moves and techniques, including targeted cyber-attacks against the communications systems of the enemy's control bodies at all levels. Decisive battles in new-generation wars will rage in the information environment, in which the attacker's computer operator manipulating the "intelligent machines" at a distance will be the key figure in the battle-space. Encrypted data flowing in public communication channels will be among the coveted targets for cyber-attacks ,[15].

Cyber defense focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with. With the growth in volume as well as the complexity of cyber-attacks, cyber defense is essential for most entities in order to protect sensitive information as well as to safeguard assets ,[15]. Cyber defense provides the much-needed assurance to run the processes and activities, free from worries about threats. It helps in enhancing the security strategy utilizations and resources in the most effective fashion. The cyber defense also helps in improving the effectiveness of security resources and security expenses, especially in critical locations ,[6].

2.3. Cyber Rapid Response Teams – CRRT(s) – and Mutual Assistance in Cyber Security project

Understanding an increasing challenge of cyber defense and the limited capabilities to respond to this threat, Lithuania proposed to the EU Council on Defense a project on Cyber Rapid Response Teams and Mutual Assistance in Cyber Security which aims not only to strengthen own security but as well to increase cyber defense capabilities on the European level. By the project, it's intended to create multinational rapid response cyber teams composed of participating countries' cyber defense experts.

The value-added of the project is that different from many other existing multinational initiatives in cyber defense which concentrate on the exchange of information this project will include sharing of the human resources. The project will cover research on various legal procedures in the domain of cyber security in the EU, organization of table top exercises (cyber crisis simulation exercises) and development of cyber defense tools ,[15]. Six EU countries have joined the project (Croatia, Estonia, Lithuania, Netherlands, Poland, Romania), with seven states observing it (Belgium, Finland, France, Greece, Italy, Slovenia, Spain).

3 Problem Solution

Cyber security is no longer enough: there is a need for strategy of defense, prevention and response. The idea of resilience, in its most basic form, is an evaluation of what happens before, during and after a digitally networked system encounters a threat. Resilience should not be taken to be synonymous with recovery. It is not event-specific: it accrues over the long term and should be included in overall business or organizational strategy. Resilience in context of ability of systems and organizations to withstand cyber events means the preparations that an organization has made with regard to threats and vulnerabilities, the defenses that have been developed, and the resources available for mitigating a security failure after it happens.

3.1. Conceptual Cyber Resilience Model

The first point, that a long-term view and durability are key factors in ensuring cyber resilience, does not need further explanation. A plan that encompasses actions and outcomes before, during and after the emergence of a threat will generally be superior to a plan that only considers one instance in time.

The second point, that leaders must broaden the conversation, merits more attention. It is vital to economic and societal resilience that we think beyond information security to overall network resilience that ensures we can deal with existing risks and face new risks that will come with such things as artificial intelligence, the internet of things or quantum computing. In order to ensure long-term cyber resilience, organizations must include in their strategic planning the ability to iterate based on evolving threats from rapidly evolving disruptive technologies ,[2].

While there are many broader definitions of cyber security, there is a difference between the access control of cyber security and the more strategic, long-term thinking cyber resilience should evoke. Additionally, since vulnerability in one area can compromise the entire network, resilience requires a conversation focused on systems rather than individual organizations. For networked technologies, vulnerability in one node can affect the security and resilience of the entire network.

Therefore, resilience is best considered in the context of a public good or commons. That's why partnerships are keys. These can be between businesses as well as with regulators, prosecutors and policy-makers ,[2]. Since cyber resilience is really a matter of risk management, there isn't a single point at which it begins or ends. Instead, it comes from building strategy and working to ensure that the risk-transfer mechanisms that work for more traditional threats are also brought to bear on new cyber threats. Responsibility for cyber resilience is question of strategy rather than tactics. Being resilient requires those at the highest levels of a company, organization or government to recognize the importance of avoiding and mitigating risks. While it is everyone's responsibility to cooperate in order to ensure greater cyber resilience, leaders who set the strategy for an organization are ultimately responsible, and have increasingly been held accountable for including cyber resilience in organizational strategy ,[2].

Combating known threats is an essential part of a cyber security strategy. It goes alongside advanced capabilities to anticipate, capture and ultimately learn from unknown threats.

Systems have different weak spots and different processes (challenges) and they each manage risk in different ways (solutions). In other words, to each security challenge (evaluated as "known" or "unknown") corresponding solution to that challenge exists (evaluated as "known(s)" or "unknowns").

By incorporating values obtained during the system security assessment process into the model we get "known known(s)" relating to information security, "known known(s)" relating to cyber security and "unknown unknowns" related to cyber resilience ,[4].

Example: There is a known crisis in the cyber security workforce: a massive shortfall in qualified and trained security professionals. There is also an unknown solution to this crisis. The broad and growing scope of the challenge requires a corresponding broadening of skill sets that are both known and unknown ,[11].

Finally, Cyber Resilience Model structure and content is presented (Figure 1), consisting of information security (Confidentiality, Integrity and Availability, abbr. CIA, triad threats and responses to them i.e. - known known(s), cyber security (non-CIA complex threats, Advanced Persistent Threats, abbr. APT(s) and corresponding responses to them i.e. known unknowns) and cyber resilience (unforeseeable and unpredictable threats and responses to them unknown unknowns).

There are opportunities around those cyber security solutions that can take the fear factor out of unknown quantities, and make them "known". But there continue to be significant opportunities around those protection measures that apply the universe of known cyber threat knowledge, to keep the system continuously secure ,[4].

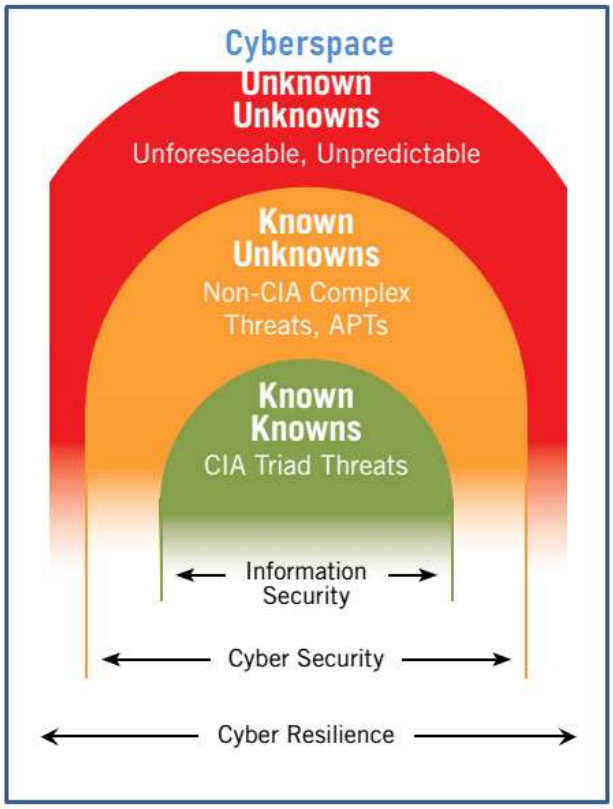

Fig. 1
Conceptual Cyber Resilience Model

In order to cope with the growing challenges, which today are manifested as unknown unknowns, systems tend to enable personnel and adjust existing and develop new processes, organization and technology.

3.2. Creation, Performance and CRRT Capability

So, as the part of aforementioned conceptual model, the initiative on creation of joint EU CRRT(s) and Mutual Assistance in Cyber Security project is among the most advanced projects out of the overall 17 approved in late 2017 under the EU Permanent Structured Cooperation (abbr. PESCO) framework. PESCO is an instrument laid out in the Treaty of Lisbon, for deepening the cooperation in security and defense area for those EU member states that have military capabilities meeting higher criteria and are bound by greater commitments ,[10].

Declaration of Intent in the Field of Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: The Ministers of Defense of the Member States and the Minister of National Defense of the Republic of Lithuania are welcoming the Joint Communication on cyber resilience, deterrence and defense adopted on September 13th, 2017. Emphasizing opportunities in developing cyber projects through PESCO, they have expressed the intention: to develop and deepen voluntary cooperation in the cyber field through mutual assistance in response to major cyber incidents, including information sharing, joint training, mutual operational support, research and development and creation of joint capabilities.

Designated experts combine work in their original Computer Emergency and response Team (abbr. CSIRT) and CRRT. CRRT(s) should closely cooperate with EU institutions, including CSIRT Network, European Union Agency for Network and Information Security (abbr. ENISA) and CERT-EU in order to ensure complement with existing cyber security initiatives.

The work of the CRRT(s) is only within the scope, agreed by the member states (MS). Civil-Military nature: CRRT(s) is a civil-military capability that should help foster civil-military culture in cyber domain and broaden cyber defense concept in the EU. The civilian-military nature of CRRT(s) could also facilitate further cooperation between military and civilian CSIRT(s). It is up to each MS to decide, which national CERT (civil or military) will participate in the project.

Equipment: In order to reach better operational capabilities of CRRT(s), the Participants could explore and set the baseline of common Cyber Toolkit designed to detect, recognize and mitigate cyber threats. To start operational activities CRRT(s) could use available on the market or nationally developed tools. However, to expand cyber security activities there is a need to develop a second generation unified toolkit for deployment. European Defense Fund co-funding and funding from other EU sources are considered in this regard. It facilitates industrial cooperation between participating MS and foster European cyber security industry.

The signatories signed the Memorandum of Understanding in January 2020 and the CRRT reached full operational capabilities (abbr. FOC) in 2021.

The Signatories participate on an equal basis in the process of creation of CRRT(s). The Ministry of National Defense of the Republic of Lithuania is a lead nation of a project ,[11].

3.3 Discussion

Modern societies are deeply imbued with communication and information technology. People are nowadays connected using various technologies for the transmission of text, image and sound, including the increasing Internet of Things (abbr.

IoT) trend. Deviations in the proper operation of these interconnected systems or their parts are no longer merely technical difficulties; they pose a danger with a global security impact. Modern societies counter them with a range of activities and measures collectively called cyber security.

Normalization is the key and cyber risk should be viewed just like any other risk that an organization must contend with in order to fulfill its goals. Leaders of business and government need to think about resilience for two reasons: first, by doing so they avoid the catastrophic failure threatened by an all-or-nothing approach to cyber risks (i.e. preventing network entry as the only plan), and second, it ensures that the conversation goes beyond information technology or information security ,[2].

By promoting an overall cyber-resilience approach, long term strategy (including which technologies a business will implement over the next five, 10 or more years) is a continual strategic conversation involving both technology and strategic leaders within an organization. The cyber-resilience approach ensures greater readiness and less repetition making it, on the whole, more efficient and more effective. Security, in contrast to resilience, can be seen as binary. Either something is secure or it isn't. It is often relegated to a single, limited technical function, keeping unauthorized users out of a networked system ,[2].

The real cyber security challenge is the unknown. Former US Secretary of Defense Donald Rumsfeld gave the explanation of this during a news briefing in 2002:"There are known known(s). These are the things that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns; these are things we don't know we don't know" ,[11].

Technologies are being developed which, unlike traditional approaches, have the ability to protect system from serious threats by learning what is normal for the organization and its people and thereby spotting emerging anomalies. Unlike, the traditional rules and signature based approach, the technology can spot threats that could harm organization and network that the traditional approaches are unable to detect. It can deal with uncertainty and delivers adaptive protection for organizations from both insider threats and advanced cyber-attacks.

The project of developing the European Union Cyber Rapid Response Teams is close to completion of its development phase. Representatives of European Union member states participating in the projects exchanged ideas and discussed the common cyber-toolkit to be developed. The cyber-toolkit for the CRRT(s) will give the participating countries a capability for cyber-incident management. Participants addressed needs of every participant and the common vision. Representatives of the participating countries discussed funding mechanisms of the toolkit and created development plan. The toolkit will ensure the CRRT(s) have the basic technical equipment which is one of the factors for the lasting success of the project.

Future research is directed towards finding and enabling efficient and effective processes for agile (adaptable, aware, flexible and productive) cyber resilience of the security information system able to cope with unforeseeable and unpredictable events (unknown unknowns) in inner and outer environment of the system as a whole. In this regard, following the establishment of the Rapid Response Team as the first step, future research will focus on building opportunities and providing mutual assistance and cooperation in responding to major cyber incidents through information sharing, joint training, mutual operational assistance and creation of shared capabilities.

4 Conclusion

In this paper the ways, processes and means for achieving cyber resilience in today's conditions of emerging security risks are examined. Within the context of cyber resilience (cyber security and emerging risks) the novel Conceptual Cyber Resilience Model that encompasses information security and cyber security is presented. Further investigations of ours are directed towards finding and enabling efficient and effective processes for agile (adaptable, aware, flexible and productive) cyber resilience of the security information system able to cope with unforeseeable and unpredictable events (unknown unknowns) in inner and outer environment of the system as a whole.

Within the process of novel conceptual model building the process of creation and performance of EU Cyber Rapid Response Teams and Mutual Assistance in Cyber Security is described, introducing novel approach to cyber security and cyber defense at the EU level putting it into the context of the Cyber Resilience Model. Key roles related to that goal have people (actors) and their performance at all levels of systems hierarchy (cyber security and cyber defense).

4.1 Future Developments

Future research encompasses personal, network and organizational cyber security management. Given conceptual model of cyber resilience is crucial through inserting knowledge and consequently achieving the increase of efficient and effective cyber security and cyber defense processes, decreasing level of "unknown unknowns", moving them towards and turning them gradually into "known unknowns" and "known known(s)".

References:

[1] Björck F., Henkel M., Stirna J., Zdravkovic J. Cyber Resilience – Fundamentals for a Definition. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham, 2015.

[2] Dobrygowski, D.: Cyber resilience: everything you (really) need to know, available at http:// https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know/, Accessed: 21st September 2022.

[3] Cyber Defense, available at https://www.techopedia.com/definition/6705/cyber-defense, Accessed: 10th April 2022.

[4] Exclusive Networks: Unknown Unknowns – The Ultimate Test for Cybersecurity, available at http://www.exclusive-networks.com/uk/blog/unknown-unknowns-ultimate-test-cybersecurity/, Accessed: 1st August 2022.

[5] Goche, M., Gouveia, W.: Why Cyber Security Is Not Enough: You Need Cyber Resilience, available at https://www.forbes.com/sites/sungardas/2014/01/15/why-cyber-security-is-not-enough-you-need-cyber-resilience/#562402a21bc4, Accessed: 1st July 2022.

[6] Hulme, G.V: Security spending continues to run a step behind the threats, available at http://www.csoonline.com/article/2134074/strategic-planning-erm/security-spending-continues-to-run-a-step-behind-the-threats.html, Accessed: 13th June 2022.

[7] Infosecurity, available at http://infosecurityinc.net/wp-content/uploads/2011/07/Consult-Cyber-1Cyber-Threats-Diminishing-Attack-Costs-gaIncreasing-Complexity4.jpg, Accessed: 18th September 2022.

[8] Marvell, S.: The real and present threat of a cyber breach demands real-time risk management, Acuity Risk Management, 2015.

[9] NATO Cyber Cooperative Cyber Defense Center of Excellence Tallin Estonia, available at https://ccdcoe.org/cyber-definitions.html, Accessed: 10th April 2022.

[10] Pescatore, J.: Toward a National Cybersecurity Strategy, G00167598, Gartner, Inc., 2009.

[11] Tucker, E.: Official: FBI probing attempted cyber breach of NY Times, available at http://www.federaltimes.com/articles/official-fbi-probing-attempted-cyber-breach-of-ny-times, Accessed: 31st May 2022.

[12] Walls, A., Perkins, E., Weiss, J.: Definition: "Cybersecurity", G00252816, Gartner, Inc., 2013.

[13] Wheeler, J. A.: Emerging Risks in Cybersecurity: Gartner's Top Ten Predicitons, available at http://blogs.gartner.com/john-wheeler/gartner-top-ten-cybersecurity-predicts/, Accessed: 2nd June 2022.

[14] United States Department of Defense: Strategy for Operating in Cyberspace, Department of Defense, 2011.

[15] Galinec, D., Steingartner, W., Zebić, V.: Cyber Rapid Response Team: An Option within Hybrid Threats. 2019 IEEE 15th International Scientific Conference on Informatics, INFORMATICS' 2019, November 20th-22nd, 2019, Poprad, Slovakia, PROCEEDINGS, Institute of Electrical and Electronics Engineers, Inc.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Darko Galinec has organized, performed and executed the research and the model building.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0 https://creativecommons.org/licenses/by/4.0/deed.en_US