Combining Cybersecurity and Cyber Defense to achieve Cyber Resilience

Darko Galinec
Department of Informatics and Computing
Zagreb University of Applied Sciences Zagreb
Zagreb, Croatia
Email: darko.galinec@tvz.hr

William Steingartner
Faculty of Electrical Engineering and Informatics
Technical University of Košice
Košice, Slovakia
Email: william.steingartner@tuke.sk

***Abstract*—Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries. Use of the term ”cybersecurity” as a key challenge and a synonym for information security or IT security confuses customers and security practitioners, and obscures critical differences between these disciplines. Recommendation for security leaders is that they should use the term ”cybersecurity” 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]. Within this paper, we investigate how cybersecurity and cyber defense combined may lead to cyber resilience and describe the relationships among cybersecurity, information security, operational technology (OT) security, IT security, and other related disciplines and practices e.g. cyber defense. In this regard ends, ways (processes) and means for achieving cyber resilience in today's conditions of emerging security risks are examined. Within the context of cyber resilience the novel model of cyber resilience is presented.**

***Index Terms*—cyber-attack, cyber defense, cyber resilience, cybersecurity**

I. Introduction

Cybersecurity 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 cybersecurity a superset of information security, operational technology (OT) security and IT security practices related to digital assets.

The aim of this paper is to examine ways, processes and means for achieving cyber resilience in today's conditions of emerging security risks. Secondly, the aim is to create the novel model of cyber resilience that encompasses information security and cybersecurity within the context of cyber resilience (cybersecurity and emerging risks).

With the understanding of the specific environment, cyber defense analyzes 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. 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 could target [3].

II. Basic Notions about Cybersecurity and Cyber Defence

Military terminology has migrated into nonmilitary contexts in the same fashion that military technology has migrated into civilian enterprises (e.g., the Advanced Research Projects Agency Network (ARPANET) becoming the Internet). Other terms, such as advanced persistent threat (APT; originally a euphemism for network attacks supported by the government of the People's Republic of China) [12], have endured similar transitions. In many cases, a migration of terminology is beneficial, as it develops better specificity in discussions of technology operations. However, the utility of a term is reduced when its distinctive meaning is eroded or destroyed as part of the migration to a new context.

A. Cybersecurity

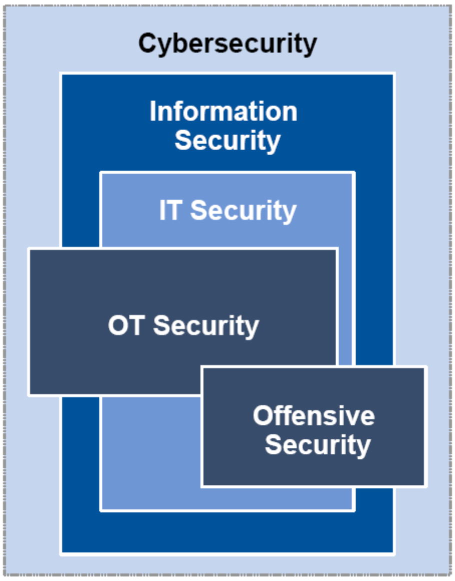
Definition: Cybersecurity is the governance, development, management and use of information security, OT security, and IT security tools and techniques for achieving regulatory compliance, defending assets and compromising the assets of adversaries [2].

According to above mentioned authors, cybersecurity:

- is a superset of the practices embodied in IT security, information security, OT security and offensive security (see Figure 1);
- uses the tools and techniques of IT security, OT security and information security to minimize vulnerabilities, maintain system integrity, allow access only to approved users and defend assets;
- includes the development and use of offensive IT- or OT-based attacks against adversaries;

978-1-5386-0889-0/17/$31.00 ©2017 IEEE

- supports information assurance objectives within a digital context but does not extend to analog media security (for example, paper documents).



Source: Gartner (June 2013)

Fig. 1. Components of Cybersecurity

But, in the same time, cybersecurity is not:

- merely a synonym for information security, OT security or IT security;
- use of information security to defend an enterprise against crime;
- Cyberwarfare – although the definition of this term is still controversial, the consensus is that ”cyberwarfare” refers to the use of cybersecurity capabilities in a warfare context. This is a complex area and should not be confused with physical attacks against infrastructure (e.g. destruction of property and machinery) and information warfare (e. g. applying psychological operations through propaganda and misinformation techniques).
- Cyberterrorism – In a similar fashion to cyberwarfare, ”cyberterrorism” refers to the use of cybersecurity techniques as part of a terrorist campaign or activity.
- Cybercrime – Cybercrime is merely an affected or pretentious term for criminal attacks using IT infrastructure. It is not related to cybersecurity.

Appropriate uses of ”cybersecurity” [12] would be:

- in response to threat risk assessments, the department increased its cybersecurity investment to enable reductions in vulnerabilities and increased capabilities for counterattacks against identified attackers (integration of IT security and offensive capabilities in a single program).
- Integration of the IT and OT security programs within the cybersecurity team enables more holistic responses to threats (integration of IT and OT in a single program).
- The ”hacktivist” organization Anonymous employs a variety of cybersecurity techniques to forward its agenda (use of offensive capabilities).

However, we could face with some inappropriate uses of ”cybersecurity”:

- In order to mitigate the theft of laptops, the store’s cybersecurity plan calls for the use of whole drive encryption. (This describes a basic IT security action.)
- The cybersecurity policy mandates the use of complex passwords for all CAM systems on the factory floor. (This describes a basic OT security requirement.)

B. *Cyber Defense*

There are no common definitions for Cyber terms - they are understood to mean different things by different nations/organizations, despite prevalence in mainstream media and in national and international organizational statements [9].

However, [3] gives definition and further explanation of term cyber defense as follows: 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.

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 complexity of cyber-attacks, cyber defense is essential for most entities in order to protect sensitive information as well as to safeguard assets.

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. Cyber defense also helps in improving the effectiveness of the security resources and security expenses, especially in critical locations.

By the recognition of the need to accelerate detection and response to malicious network actors, the United States (US) Department of Defense (DoD) has defined a new concept, Active Cyber Defense (ACD) as DoD’s synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities [14].

III. Cybersecurity Starategy and Risk Management

While the cost of defending cyber structures as well as the payoffs from successful attacks keeps rising, the cost of launching an attack simultaneously keeps decreasing [7].

By the standard military definition, ”strategy” is the utilization of all of a nation’s forces, through large-scale, long-range planning and development, to ensure security or victory. For traditional wars against traditional monolithic opponents, that approach worked.

However, for today’s world of asymmetric warfare and rapidly changing threats, the medical definition of strategy from Merriam-Webster’s dictionary is more appropriate for addressing cybersecurity: ”an adaptation or complex of adaptations (as of behavior, metabolism or structure) that serves or appears to serve an important function in achieving evolutionary success."

The key to increasing cybersecurity is getting to lower levels of vulnerability. Although threat awareness is important, by reducing vulnerabilities, all attacks are made more difficult [10].

A. Cybersecurity Risk Management

Cyber security breaches, such as those at Ashley Madison, the US Office of Personnel Management and JP Morgan Chase have demonstrated the real and present threat from cyber breaches. Director of the National Security Agency and head of the United States Cyber Command, Admiral Mike Rodgers has been moved to state that "It's not about if you will be penetrated but when" [8].

If there isn't sufficient visibility of cyber security status, organizations won't be able to manage cyber security risks and they will almost certainly suffer a breach. "Visibility of cyber security status" means having the complete picture, with measurements so that we can answer the following questions:

- What are our current measured levels of cyber security risk across the Enterprise from the multiple threats that we face?
- Are these cyber security risks tolerable?
- If not, what is our justified and prioritized plan for managing these risks down to tolerable levels?
- Who is responsible and by when?

The ability to measure cyber security status is fundamental; if we can't measure then we can't manage. Security incident and event management (SIEM) and data analytics solutions can provide valuable indications of actual or potential compromise on the network but these are partial views, indicators of our overall risk status but not measurements of our risk status.

Similarly, threat intelligence services can identify data losses and provide valuable indications of actual or impending attacks but again these are not measurements of our risk status. The same can be said individually about outputs from compliance management, vulnerability management, penetration testing and audits.

Only by pulling together all of the relevant indicators and partial views we can develop overall risk-based measurement and visibility of our cyber security status [8]. When confidence in our cybersecurity risk measurements exists it is possible to respond to events and make decisions quickly, e. g.:

- Be able to identify risks that we aren't prepared to tolerate and have a clear and prioritized risk-based action plan for the control improvements necessary to reduce these risks to an acceptable level
- To have a better understanding of the implications from threat intelligence or outputs from SIEM and data analytics allowing faster, better targeted responses
- To develop risk-based justifications for investment in cyber security solutions and services.

But with the very high level of threat and high rates of change in both the threat and control landscapes we need to be able to refresh our view of our cyber security status on an almost daily basis.

Cybersecurity risk management which previously might have been an annual process as part of planning and budgeting is now a critical real-time facilitator in the battle against cyber breaches [8]. Cyber security breaches occur when people, processes, technology or other components of the cyber security risk management system are missing, inadequate or fail in some way. So we need to understand all of the important components and how they inter-relate.

This doesn't mean that risk management system needs to hold details of (for example) every end point and the status of every vulnerability on the network because there are other tools which will do that but the risk management system does need to know that all end points on the network have been (and are being) identified and that critical vulnerabilities are being addressed quickly.

Cybersecurity success is essentially the result of an effective risk management process. However, this process is being challenged by the inherent complexity of systems, developed with vulnerable components and protocols, and the crescent sophistication of attackers, now backed by well-resourced criminal organizations and nations.

B. Cyber Resilience

With this scenario of uncertainties and high volume of events, it is essential the ability of cyber resilience.

Cyber resilience is the ability of a system, organization, mission, or business process to anticipate, withstand, recover from, and adapt capabilities in the face of adversary conditions, stresses, or attacks on the cyber resources it needs to function.

Cyber resilience from an organizational perspective is defined as "the ability to continuously deliver the intended outcome despite adverse cyber events", and this definition is systematically described and justified [1].

Starting with the 2012 World Economic Forum meeting in Davos, cyber resilience [1] has been not only an area of growing importance for individuals, businesses and societies, but also a concept that has gained in attention and usage.

Cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events. The notion of continuously, means that the ability to deliver the intended outcome should be working even when regular delivery mechanisms have failed, during a crisis and after a security breach. The notion also denotes the ability to restore the regular delivery mechanisms after such events as well as the ability to continuously change or modify these delivery mechanisms if needed in the face of changing risks. The intended outcome refers to that which the unit-of-analysis (e.g. the nation, organization or IT system) is intended to achieve, such as the goals of a business or business process or the services delivered by an online service [1].

IV. Cyber Resilience Context

Cybersecurity is an inherently distributed problem that will continue to evolve at the speed of technology. According to the

11th Annual Global Information Security Survey, conducted by PriceWaterhouseCoopers and CSO Online [6], executives remain confident in the robustness of their security initiatives. In the survey, 84% of CEOs and 82% of CIOs contend their cyber security programs are effective, while 78% of chief information security officers express full confidence in their existing cyber security programs. With breaches on the rise, companies should focus on cyber resilience, not just cyber security. The number of security incidents detected is rising significantly year-over-year climbing from 2,989 reported in 2012 to 3,741 in 2013. Add to that the fact that the average losses per incident are up 23% year-over-year, and that the number of organizations reporting losses of more than $10 million per incident is up 75% from just two years ago [5].

Cyber security isn't going far enough so Cyber Resilience must be taken into consideration. Once businesses accept that cyber attacks will be made against their organizations and will be successful, they can move to the next step: implementing a Cyber Resilience Program (CRP). A CRP encompasses the ideas of defense and prevention, but goes beyond those measures to emphasize response and resilience in moments of crisis [5].

A. *Emerging Risks in Cybersecurity*

Today's security professionals battle threats from outside the organization as well as those from their own employees. But what about threats that they already know exist? The next few years will see a variety of attacks as well as progress in the technologies and processes that prevent them. Gartner's predictions focus on how organizations can prepare for future cybersecurity risk while taking appropriate action today.

1) Through 2020, 99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year. Recommended Action: Companies should focus on fixing the vulnerabilities they know exist. While these vulnerabilities are easy to ignore, they're also easier and more inexpensive to fix than to mitigate.
2) By 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources. Recommended Action: Business units deal with the reality of the enterprise and will engage with any tool that helps them do the job. Companies should find a way to track shadow IT, and create a culture of acceptance and protection versus detection and punishment.
3) By 2018, the need to prevent data breaches from public clouds will drive 20% of organizations to develop data security governance programs. Recommended Action: Develop an enterprise-wide data security governance (DSG) program. Identify data security policy gaps, develop a roadmap to address the issues and seek cyber insurance when appropriate.
4) By 2020, 40% of enterprises engaged in DevOps will secure developed applications by adopting application security self-testing, self-diagnosing and self-protection technologies. Recommended Action: Adopt Runtime application self protection (RASP) for DevOps. Evaluate less mature vendors and providers for potential security options.
5) By 2020, 80% of new deals for Cloud Access Security Broker (CASB) technology will be packaged with network firewall, secure web gateway (SWG) and web application firewall (WAF) platforms. Recommended Action: While concerns exist about customer migration to the cloud and bundling purchases, companies should assess the application deployment roadmap and decide whether investment is justified.
6) By 2018, enterprises that leverage native mobile containment rather than third-party options will rise from 20% to 60%. Recommended Action: Experiment and become familiar with native containment solutions. Keep in mind that enterprise with average security requirements should plan to move gradually to native containment.
7) By 2019, 40% of IDaaS implementations will replace on-premises IAM implementations, up from 10% today. Recommended Action: Enough limitations have disappeared on Identity as a Service (IDaaS) that companies should start experimenting on small-scale projects. While a clash of regulations could derail the increased implementation, companies should work to recognize the current limitations and benefits.
8) By 2019, use of passwords and tokens in medium-risk use cases will drop 55%, due to the introduction of recognition technologies. Recommended Action: Passwords are too entrenched in business practices to disappear completely, but companies should look for products that focus on development of an environment of continuous trust with good user experience. Begin by identifying use cases, and press vendors for biometric and analytic capabilities.
9) Through 2018, over 50% of IoT device manufacturers will not be able to address threats from weak authentication practices. Recommended Action: By changing the enterprise architecture, IoT introduces new threats. Early IoT security failures might force the industry towards authentication standards, but companies should identify authentication risks, establish identity assurance requirements, and employ metrics.
10) By 2020, more than 25% of identified enterprise attacks will involve IoT, though IoT will account for only 10% of IT security budgets. Recommended Action: As IoT continues to grow, vendors will favor usability over security and IT security practitioners remain unsure of the correct amount of acceptable risk. Companies should assign business ownership of IoT security, focus on vulnerable or unpatchable IoT devices, and increase IoT-focused budget [13].

B. *Information Security, Cybersecurity and Cyber Resilience*

Cybersecurity 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. Normalization is the key. Cyber risk should be viewed just like any other risk that an organization must contend with in order to fulfil 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].

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 our 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].

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].

While there are many broader definitions of cybersecurity, there is a difference between the access control of cybersecurity 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]. The real cybersecurity 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 knowns. 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].

Combating known threats is an essential part of a cybersecurity 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 ”knowns” or ”unknowns”). By incorporating values obtained during the system security assessment process into the model we get ”known knowns” relating to information security, ”known unknowns” relating to cyber security and ”unknown unknowns” related to cyber resilience [4].

Example: There is a known crisis in the cybersecurity 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 2), consisting of information security (CIA triad threats and responses to them i.e. - known knowns), cybersecurity (non-CIA complex threats, APTs 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 cybersecurity 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].

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. Technologies are being developed

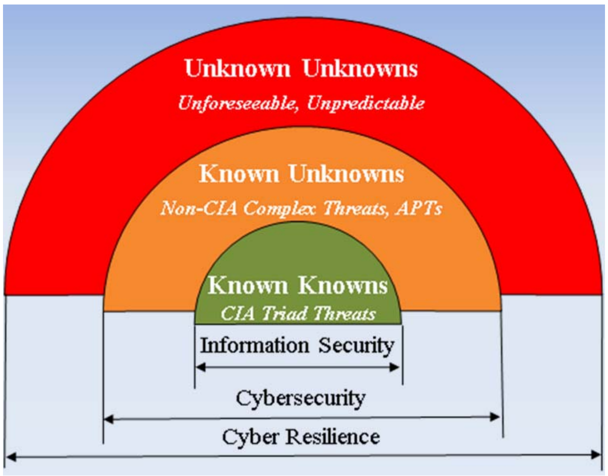


Fig. 2. Cyber Resilience Model

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.

V. Conclusion

Nowhere has technological development been more dynamic and comprehensive than in the area of communication and information technology. The focus has always been on the rapid development and introduction of new services and products, while the security-related aspects usually had little influence on the broad acceptance of new technologies.

The life cycles of modern-day information systems, from the process of planning, introduction and usage to their withdrawal from use are very short, which often makes their systematic testing impossible and is most commonly applied as an exception, in expressly prescribed cases.

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 (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 cybersecurity.

In our 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 (cybersecurity and emerging risks) the novel model of cyber resilience that encompasses information security and cybersecurity 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. Key roles related to that goal have people (actors) and their performance at all levels of systems hierarchy (cybersecurity combined with cyber defence).

Acknowledgment

This work has been supported by Grant No. 002TUKE-4/2017: Innovative didactic methods of education process at university and their importance in increasing education mastership of teachers and development of students' competences.

References

[1] Björck F. et al.: 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 https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know/, Accessed: 21st June 2017.
[3] Cyber Defense, available at https://www.techopedia.com/definition/6705/cyber-defense, Accessed: 10th February 2017.
[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 June 2017.
[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 June 2017.
[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: 3rd June 2017.
[7] Infosecurity, available at http://infosecurityinc.net/wp-content/uploads/2011/07/Consult-Cyber-1Cyber-Threats-Diminishing-Attack-Costs-gaIncreasing-Complexity4.jpg, Accessed: 15th November 2016.
[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 Defence Center of Excellence Tallin Estonia, available at https://ccdcoe.org/cyber-definitions.html, Accessed: 10th February 2017.
[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 2017.
[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 2017.
[14] United States Department of Defense: Strategy for Operating in Cyberspace, Department of Defense, 2011.

Zusammenfassung

Die Internetsicherheit umfasst viele Verfahren, Testinstrumente und Begriffe, die in einem engen Zusammenhang mit der Informations-und Operationssicherheit in Technologien sind. Das Risiko der Internetsicherheit besteht darin, dass sie auch offensive Benutzung der Informationstechnologien zu den Angriffen umfasst. Die Benutzung des Begriffs Internetsicherheit als eine Hauptherausforderung und das Synonym

für die Informationssicherheit oder IT-Sicherheit verwirrt die Kunden und die IT-Spezialisten und verheimlicht kritische Unterschiede zwischen diesen Disziplinen. Man empfiehlt den Experten im Bereich der Sicherheit, den Begriff ”Cybersecurity” zu benutzen, damit sie nur die Sicherheitsverfahren bestimmen. Diese sind in einem engen Zusammenhang mit den Abwehrprozessen. Diese Abwehrprozesse umfassen oder verlassen sich auf die Informationstechnologien oder auf die Systeme und die Umfelder der Operationstechnologien. Der Internetabwehr ist der Abwehrmechanismus des Computernetzes, der die Reaktion auf Angriffe umfasst, Schutz gegen eine gefährliche Netzinfrastruktur und Informationsschutz für Organisationen, Regierungsorganisationen und andere mögliche Netze. Im Rahmen dieses Artikels forschen wir, wie die Internetsicherheit in der Verbindung mit den Angriffen in Internet zu der Widerstandsfähigkeit führt. Zugleich beschreiben wir die Beziehungen zwischen der Internetsicherheit, Informationssicherheit und anderen verwandten Disziplinen und Verfahren, wie z. B. Angriffe in Internet. In dieser Hinsicht werden die Ziele, Verfahren und Testinstrumente geforscht, die zum Erzielen von Cyber-Widerstandsfähigkeit in heutigen Bedingungen der zunehmenden Sicherheitsrisiken dienen. Im Kontext der Cyber-Widerstandsfähigkeit wird ein neuer Model der Cyber-Widerstandsfähigkeit präsentiert.