THE ISIS AND THE GLOBAL TERRORISM

József KIS-BENEDEK

Abstract: The ISIS is a terrorist organization seeking to be a state by using guerrilla methods as well. The author deals with the ISIS as a terrorist organization by analyzing its appearance, the threats represented by itself for the world. The essay refers to the affiliates and adherents of the ISIS which can continue and spread the terrorism all over the world. The paper analyses the European jihadist problems, the growing radicalization and the modus operandi of the European jihadist organizations.

Keywords: ISIS, terrorism, jihadism, radicalism, Europe.

INFORMATION SECURITY MANAGEMENT SYSTEM IMPLEMENTATION

Lubomír ALMER, Petr HRUZA

Abstract: Currently there are plenty of new technologies, which provide us new opportunity for Protection against cyber threats. More precisely, we register unstoppable growth of information security, which provides us new options of security. Hand in hand with new technology go threats. One way how to protect our infrastructure is to follow few basic steps and implement Information security management system together with cyber security law. These two documents describe technologies and documents, which help us, decrease the level of cyber threats. These two documents cannot provide us complete cyber security. We have to extend it by few more technological solutions. We have to cover all of sectors for complex cyber security.

Keywords: cyber security, cyber security law, cyber threats, cyber defense, information security management system.

ICT SUPPORT OF DECISION MAKING PROCESS IN THE NETWORK OF TACTICAL COMMAND POSTS

Grzegorz PILARSKI

Abstract: The most important aspect of operations in the network of tactical command posts is communication and flow of information. The information which is correct, check and authentic is most important on current and future battel field. It is very important to support this undertaking to guarantee commander and commander's group possibility to provide military decision making process. The author presents in this article solution to support soldiers working on command posts to organize them appropriate tools to communicate through information relations in the network of tactical command posts.

Keywords: information communication technology (ICT), military decision making process (MDMP), tactical command post.

OPTIMAL SENSOR ARRAY AND PROBABILITY OF DETECTION IN 3D AREA

Peter RINDZÁK

Abstract: The paper continues in the previous study, in which the model of the dislocation of sensors in 2D and 3D area was mathematically expressed. In addition, the theoretical assumptions of the individual optimization strategies in 2D area were simulated. The main goal of the work is to verify the optimization strategies in 3D area by simulation and based on the results to determine initial assumptions for application of the probability model and the model of maximal entropy. The conclusion of the paper contains an example of thesis for possible future studies.

Keywords: NEC, Network enabled capability, UAV, sensors, TDOA.

OPTIMIZING WINDOWS 10 AND WINDOWS SERVER 2016 LOGGING TO DETECT NETWORK SECURITY THREATS

Július BARÁTH

Abstract: The collection and analysis of event logs allows detection and debugging of operating system and application configuration errors. An appropriate selection of event logs allows you to detect cyber-attacks and prevent potential damage. In the article, we focused on the selection and optimization of event logs for the Microsoft Windows workstation and server operating system. We have experimentally verified the structure and amount of produced logs and we proposed their optimization.

Keywords: event logs, Microsoft windows, attack detection.

CYBER THREAT ASSESSMENT REPORT IN SELECTED ENVIRONMENT CONDUCTED BY CHOOSEN TECHNOLOGY OF FIREWALLS

Martin DROPPA, Boris MATEJ, Marcel HARAKAĽ

Abstract: The purpose of this document is to provide a cyber threat assessment report through choosen environment. There are many methodologies that exist today on how to perform a risk and threat assessment. But all these methodologies try to answer the following questions: What needs to be protected? What (who) are the threats and vulnerabilities? What is the value to the organisation? What can be done to minimize exposure to the loss or damage?

Threats are described as anything that would contribute to the tampering, destruction or interruption of any service or item of value. The analysis will look at every element of risk that could conceivably happen. Threats go hand in hand with vulnerabilities and can be graded in a similar manner, measured in terms of motivation and capability.

The threat and risk assessment process is not a means to an end. It is a continual process that once started should be reviewed regularly to ensure that the protection mechanisms currently in place still meet the required objectives. The assessment should adequately address the security requirements of the organization in terms of integrity, availability and confidentiality. The threat and risk assessment should be an integral part of the overall life cycle of the infrastructure [8].

Keywords: detection, threat, assessment, malware, attack, network, vulnerability, exploits.