SCIENCE & MILITARY

No 2 | Volume 12 | 2017

Dear readers,

Nowadays, more and more emphasis is being placed on publishing science and research outputs in high-quality scientific journals, which, according to reviewers, are only the journals registered in the most significant international databases, such as Current Contents, WOS or SCOPUS. And we cannot object to this fact, which, however, affects our journal to a great extent. Even though the journal Science & Military has a long tradition and it is registered in international databases, such as ProQuest and EBSCO, it is difficult to obtain quality scientific papers for such an"ordinary journal". However, I am pleased to say that so far our editorial office has succeeded in doing so.

Taking the above mentioned facts into consideration, the Science & Military editorial board naturally attempts to register this journal in the prestigious database SCOPUS, and later also in the Current Contents database. To achieve this, the editorial board has already made quite a lot of steps. The Science & Military journal is published regularly two times a year and the quality of papers written in English is checked by the international editorial board. What is more, every article undergoes a demanding review process before being published. Furthermore, the Science & Military journal has its own website, which is regularly updated, and some other things have been taken for granted for a long time.

Dear reads, a quality scientific journal is made up especially of quality papers. Therefore, I would like to invite all university scientific and teaching staff as well as doctoral students to publish their scientific outputs in the Science & Military journal. This journal focuses on the military science (technical sciences, natural sciences, humanities, security sciences and management).

Dear readers, let me briefly introduce the second issue of the Science & Military journal in 2017.

Among the peer-reviewed articles in this issue, you can find the article written by József Kis-Bendek titled "The ISIS and the Global Terrorism", which analyses the European jihadist problems, the growing radicalization and the modus operandi of the European jihadist organizations. The author deals with the ISIS as a terrorist organization by analyzing its appearance and the threats it poses to the world.

The second article, written by Lubomir Almer and Petr Hruza titled "Information Security Management System Implementation", describes technologies and documents which help us decrease the level of cyber threats. If we implement all of these, we can talk about an acceptable level of cyber security.

Another article titled "ICT Support of Decision Making Process in the Network of Tactical Command Posts" was written by Grzegorz Pilarski. The author presents the solution to support soldiers working on command posts to organize them with appropriate tools to communicate through information relations in the network of tactical command posts.

The author Peter Rindzák wrote the article titled "Optimal Sensor Array and Probability of Detection in 2D and 3D Area". The paper continues the previous study, in which the model of the dislocation of sensors in 2D and 3D area was mathematically expressed. The main goal of the paper 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.

In his article "Optimizing Windows 10 and Windows Server 2016 Logging to Detect Network Security Threats", the author Julius Barath focused on the selection and optimization of event logs for the Microsoft Windows workstation and server operating system.

The final article was written by Martin Droppa, Boris Matej and Marcel Harakaľ and titled "Cyber Threat Assessment Report in Selected Environment Conducted by Chosen Technology of Firewalls". Its purpose is to provide a cyber threat assessment report through chosen environment.

Dear readers, in conclusion, I would like to wish you all the best in the coming year 2018 and thank you for your previous attention on behalf of myself and the Editorial Board.

Col. (ret.). Assoc. Prof. Eng. Marcel HARAKAĽ, PhD.
Chairman of the editorial board

Reviewers

Eng. Vladimír **ANDRASSY**, PhD.	Armed Forces Academy of General M. R. Štefánik Liptovský Mikuláš (SK)
Eng. Július **BARÁTH**, PhD.	Armed Forces Academy of General M. R. Štefánik Liptovský Mikuláš (SK)
Assoc. Prof. Eng. Marcel **HARAKAĽ**, PhD.	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš (SK)
Assoc. Prof. RNDr. Ľubomír **DEDERA**, PhD.	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš (SK)
Eng. Miroslav **ĎULÍK**, PhD.	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš (SK)
Eng. Ján **MAREK**	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš (SK)
Prof. Eng. Pavel **NEČAS**, PhD. MBA	Matej Bel University in Banská Bystrica (SK)
Eng. Michal **TURČANÍK**, PhD.	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš (SK)
Assoc. Prof. Inga V. **URIADNIKOVA**, PhD.	Odessa National Polytechnic University (UA)

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.

1 INTRODUCTION

The ISIS[1] poses a grave threat not only in the Middle East but almost in the whole world. The wrong dealing of the Iraqi and Syrian crisis, the expansion of the radical political Islam and the growing jihadism all contributed to the spreading of the ISIS. If we pose the question whether the ISIS is really a state I think that this not a state, it is a terrorist organization seeking to be a state by using guerrilla and terrorist warfare. Nobody in the world accepted a state like this. Taking into consideration the methods followed by this entity it is not Islam at all.

However thousands of recruits reportedly have joined the organization since the start of coalition military operations in 2014, but U.S. officials have reported uncertainty about casualty to replacement ratios and the overall extent and effects of attrition in ISIS ranks [1]. As of July 2015, the Office of the Director of National Intelligence (ODNI) estimated publicly that as many as 25,000 individuals from more than 100 countries have travelled to Syria to engage in combat with various groups since 2011, including more than 4,500 Europeans and some U.S. citizens [2].

The religious extremism and transnational tendencies represented by ISIS is the result of historic dynamics in the changing Arab civilization. Any long term look at the performance of the Arab states could reach the conclusion that their societies are poor and there is a political instability for a long while yet. The unsuccessfully handling of the Iraq and Syrian crisis played an important role to its come into existence [3].

The ISIS came out of nowhere in June 2014, when it conquered Mosul, Iraq's second-largest city. However, the Islamic State of today is the direct descendant of a group that Iraq, the United States, and their partners once fought as al-Qaida in Iraq and then as the Islamic State of Iraq.

In the fall of 2016, the group commands tens of thousands of fighters in Iraq and Syria, and has received pledges of support from affiliated groups in several countries across the Middle East, Africa, Caucasus and South Asia. The Islamic State's apocalyptic ideology, its revolutionary intent toward the strategically important Middle East, and its embrace of transnational terrorism have alarmed policy makers around the world and spurred global debate over strategies and policy options. I would like to emphasize the rapid emergence of affiliated organizations in the Middle East and Africa having (or not having) direct or indirect contacts with ISIS. In case of destruction (more exactly restriction) of ISIS in Iraq and Syria, the next challenge will be the activities of affiliate organizations such as Al Qaida in Islamic Maghreb, Boko Haram, al Qaida in Sinai Peninsula, al Qaida in Islamic Maghreb, al Shabaab and so on). Thanks to the persistent military actions of the different coalition forces since the spring of 2016 the ISIS lost more than 40 percent of its occupied territories in Iraq and Syria and the financial support of the organization is diminishing day by day.

We cannot count with the rapid cessation of the ISIS because the huge differences of political interests of the great powers and the participating countries. With purely military means the organization could be destroyed, but the affiliates and adherents terrorist organizations will remain.

2 ISIS AFFILIATES AND ADHERENTS

Since 2014, some armed groups have recognized the ISIS [4] and pledged loyalty to the caliph Abu Bakr al Baghdadi. Groups in Yemen, Egypt, Algeria, Saudi Arabia, Libya, Afghanistan, and Nigeria have used the Arabic word "*wilayah*" (state/province) to describe themselves as constituent members of a broader ISIS-led caliphate.

As of late 2016, the following ISIS adherents are the most significant and capable to realize terror attack.

[1] ISIS: Islamic State in Iraq and Syria, known as ISIL (Islamic State in Iraq and the Levant) or IS (Islamic State), or DAESH.

2.1 The Islamic State in Egypt (Sinai Province, Wilayah Sinai)

The Islamic State's local affiliate in the northern Sinai Peninsula was formerly known as *Ansar Bayt al Maqdis* (Supporters of the Holy House or Partisans of Jerusalem). It emerged after the Egyptian revolution of 2011 and affiliated with the Islamic State in 2014. Estimates of its membership range from 500 to 1,000, and it is comprised of radicalized indigenous Bedouin Arabs, foreign fighters, and Palestinian militants. Among his armaments are man-portable air defence systems (MANPADS) such as the 9K338 Igla-S and Kornet anti-tank guided missile (ATGM) systems. The organization has claimed credit for destroying Metrojet Flight 9268, which exploded in mid-air over the Sinai Peninsula on October 31, killing all 224 passengers aboard. Nowadays the organization commits a terror attack almost every week. Among targets are the Egyptian military and police forces and the Christian population.

2.2 The Islamic State in Saudi Arabia (Wilayah Najd/Haramayn/Hijaz)

IS leaders have threatened the kingdom's rulers directly and called on the group's supporters there to attack Shiites, Saudi security forces, and foreigners. IS supporters have claimed responsibility for several attacks e.g. suicide bombing attacks on Shia mosques in different parts of Saudi Arabia, in a Kuwaiti mosque, killing more than two dozen people and wounding hundreds. Saudi officials have arrested more than 1,600 suspected IS supporters (including more than 400 in July 2015) and claim to have foiled several planned attacks.

The Islamic State poses a unique political threat to Saudi Arabia in addition to the tangible security threats demonstrated by a series of deadly attacks inside the kingdom since late 2014. IS leaders claim to have established a caliphate to which all religious Sunni Muslims owe allegiance, directly challenging the legitimacy of Saudi leaders who have long claimed a unique role as Sunni leaders and supporters of particular Salafist interpretations of Sunni Islam. IS critiques of Saudi leaders may have resonance among some Saudis who have volunteered to fight for or contributed on behalf of Muslims in several conflicts involving other Muslims over the last three decades.

2.3 The Islamic State in Libya (Wilayah Tarabalus/Barqa/Fezzan)

Supporters of the Islamic State in Libya have announced *three* affiliated wilayah (provinces) corresponding to the country's three historic regions–*Wilayah Tarabalus* in the west, *Wilayah Barqa* in the east, and *Wilayah Fezzan* in the southwest. Some observers put the group's strength in Libya at several hundred to a few thousand fighters among a much larger community of Salafi-jihadist activists and fighters. Since late 2014, IS supporters have taken control of Muammar al Qadhafi's hometown Sirte and committed a series of atrocities against Christians and Libyan Muslim opponents. They also have launched attacks against forces from Misrata and neighboring towns in an effort to push westward and southward. IS backers sought to impose their control on the eastern city of Darnah. There is no concrete data, but we can suppose that this organization can train people who could appear in Europe.

2.4 The Islamic State in Nigeria [West Africa Province (Wilayah Gharb Afriqiyyah)]

Two of the most significant African insurgent groups – Boko Haram in Nigeria and al-Shabaab in Somalia – are looking to ISIS, possibly to gain momentum as both groups face the increased pressure of successful military operations against them. The Islamist group Boko Haram pledged its allegiance to ISIS in early March 2015, more specifically to the 'Caliph of Muslims' Abu Bakr al-Baghdadi. The pledge coincided with successful operations against Boko Haram carried out by a coalition of Nigerian forces and neighboring countries affected by Boko Haram violence [5]. This northeast Nigeria-based Sunni insurgent terrorist group widely known by the name *Boko Haram* ("western education is forbidden"). 5,500 in 2014 alone and more than 1.5 million people have been displaced by related violence, which increasingly spread into neighboring Cameroon, Chad and Niger in 2015. The group threatens civilian, state and international targets, including Western citizens being in the region. Boko Haram's announcement of allegiance to ISIS coincides with its ousting from key towns in north-eastern Nigeria. Meanwhile, Somalia's al-Shabaab also appears to be flirting with the idea of associating itself with ISIS, having been seriously weakened by the African Union-led *Operation Indian Ocean* and US airstrikes targeting its leaders.

2.5 The Islamic State in Yemen (Wilayah al Yemen, Wilayah Al Bayda, Wilayah Aden-Abyan, Wilayah Shabwah)

In Yemen, militants who claim allegiance to the Islamic State have taken advantage of ongoing war to repeatedly bomb mosques known for attracting worshippers of Zaydi Islam, an offshoot of Shia Islam (with legal traditions and religious practices which are similar to Sunni Islam). Islamic State terrorists have targeted supporters of the Houthi Movement, a predominately Zaydi armed militia and political group that aims to rule wide swaths of northern Yemen and restore the "Imamate."

2.6 The Islamic State in Afghanistan and Pakistan (Wilayah Khorasan)

The Islamic State attempts to expand its reach in Afghanistan and Pakistan as well. The Islamic State presence in Afghanistan and Pakistan appears to consist of individuals of more mainstream insurgent groups, particularly the Afghan Taliban, showing themselves as members of "The Islamic State of Khorasan Province," or *Wilayah Khorasan*. This group differs from the so called Khorasan Group identified by U.S. officials as being an Al Qaeda affiliated cell seeking to conduct transnational terrorist attacks. It does not appear that Islamic State leadership has sent substantial numbers of fighters from Iraq and Syria into Afghanistan or Pakistan. The Islamic State's presence and influence in Afghanistan remains in the exploratory stage." It is known that there is a growing competition and conflict between the Taliban and Islamic State fighters.

3 EUROPE'S JIHADIST PROBLEM, THE ROOTS OF RADICALIZATION

In Europe there are about 60 million Muslims out of this 25-30 million live in the territories of the European Union (with the migration flow in 2015 this number is growing. In 2015 roughly 1, 5 million refugees arrived in Europe who intend to stay mainly in Germany and Sweden. Beyond the handling of so many refugees (security checking, accommodation, provision and so on) an enormous problem is the radicalization of some people. Terrorism researchers are trying to understand how young people in Europe become radicalized, by looking for clues in the life histories of those who have committed or planned terrorist acts in recent years, left the continent to join ISIS, or are suspected of wanting to become jihadists.

Jihadism still poses a significant threat to the security of most European countries. Over the last couple of years, there has been realized that the global jihadist movement is anything but vanished.

Rather, it has been experiencing resurgence worldwide, including in Europe. The best indicator of this dynamic is the unprecedented number of European-based fighters who have reached Syria and Iraq since 2001. "According to Europol in January 2015 the number of foreign fighter in Iraq and Syria reached 5,000. Larger countries like France and the United Kingdom have contributed to this number with 1,000 and 800 respectively, but smaller country like Belgium provided 400 fighters. The vast majority of these European volunteers join jihadist groups, in particular the ISIS. Concerning the threat, the European authorities are worried. British authorities have described this phenomenon as "a game-changer" and "the most profound shift in the threat we have seen since 2003" [6].

Research suggests that most extremists are either people who returned suddenly to Islam or converts with no Islamic background. It is difficult to make generalizations about how people become radicalized in Europe. According to Olivier Roy[2], "many extremists come from broken families or deprived areas, lack education and are unemployed". The European jihadism is transnational, the main drivers are armed conflicts and militant groups involved in those conflicts.

We think in Europe that radicalization is a socialization process in which group dynamics (kinship and friendship) are more important than ideology. The process of political radicalization into extremism and eventually, into terrorism, happens gradually and requires a more or less prolonged group process. Feelings of frustration and inequity first have to be interiorized and then lead to a mental separation from society which is considered responsible for those feelings). Individuals then reach out to others who share the same feelings, and create an 'in-group'. Within such a group, personal feelings get politicized (what are we going to do about it?). As Mark Sedgwick reminds us, "the concept of radicalization emphasizes the individual and, to some extent, the ideology and the group, and significantly de-emphasizes the wider circumstances' and the context in which it arises" [7].

The enduring economic and labor market stagnation is certainly part of the explanation for why youngsters today have the impression that they are without decent job prospects. The youth suicide rate (age 15-24 – broadly, the same age range as the foreign fighters) is much higher. The generation coming of age in the 2010s faces high unemployment and uncertain job situations.

The economic and financial crisis has further eroded confidence in the future. Other motives can also be identified. They want to look up to heroes – or to be one themselves. More malicious motives are at play too: some try to escape prison sentences by fleeing to Syria. Some are undoubtedly psychopaths, while still others are adventure seekers, looking for something more thrilling than everyday life in Europe.

At the same time religious motivations play a crucial role. Most foreign fighters who join jihadist groups are driven by a deep hatred for Alawites and Shias in general and see fighting what they consider deviant Islamic sects a religious duty.

European jihadist networks in Syria are characterized by the extreme diversity in origin, age, background, and socio-economic conditions of the individuals fighting there. Some of them have a long track record of militancy and fighting experience.

[2] Olivier Roy is a professor of political Islam and the Middle East at Italy's European University Institute near Florence.

Others have no previous battlefield experience. Many of them belonged to militant networks or were active in the salafist scene in their countries of origin. Others were individuals without any sign of sympathy with jihadist ideology. And another characteristic is the growing number of females who decide to travel to Syria with their husbands or to get married to mujaheddin they meet online. There are indications that some of these women are also involved in actual fighting, a relatively new development in the world of jihadism.

"The question of why some of Europe's young Muslims become radicalized, fight in Syria and kill their own fellow-citizens is a question that worries all governments. France has more Muslim citizens than any other country in the European Union and the largest number of foreign fighters in Syria; but Belgium has the highest proportion of those fighters as a share of its population" [8].

"The causes are not only Islamic puritanism and economic marginalisation. Those heading for Syria are often petty criminals. But there are also middle-class youngsters, young girls and converts**.** Some who have travelled to Syria and Iraq, for example, are nationalists, non-jihadist Islamists or even anti-jihadist fighters. The majority, however, are jihadists or have joined jihadist groups" [9].

4 THE MODUS OPERANDI OF JIHADI TERRORISM IN EUROPE

Jihadi terrorist plots in Europe involve cells controlled by al-Qaida, ISIS or cells controlled by other jihadi groups, as well as independent cells, or individuals. Even self-radicalized individuals who plot attacks on their own are sensitive to broad ideological and strategic guidelines emanating from al-Qaida's central leadership.

The ongoing conflict in Iraq and Syria is going to affect the jihadi threat to Europe in coming years. Returning foreign fighters from Syria have already staged plots in Europe and more will come. A majority of plots will follow the trend toward more discriminate targeting and more diverse attack methods. However, we will also see plots targeting European society at large, especially when European nations contribute more to the U.S.-led coalition in Syria or Iraq.

Jihadi terrorism in Europe is becoming more discriminate in its targeting while attack types and weapons are becoming progressively more diverse. The most likely scenarios in the coming three to five years are bomb attacks and armed assaults against sub-national entities, communities and individuals. A majority of the terrorist attacks will be limited in scope, but mass-casualty terrorism cannot be excluded. Foreign fighters from Syria are likely to influence the threat level in Europe we do not expect them to alter patterns in modus operandi dramatically.

If we go back into the history of Jihadist attack in Europe we can find out that in the 1990s and early 2000s, jihadi terrorism was dominated by random mass casualty attacks on transportation, (a typical example was the Madrid bombings). In recent years it has become more common to target Jews, artists involved in the Prophet Mohammed cartoons affair, or soldiers in uniform, albeit recently different soft targets. Weapons and tactics are becoming more diverse. In the 1990s and early 2000s, jihadists in Europe operated in groups and planned bomb attacks with certain types of explosives. In recent years, more terrorists have worked alone and they used a broader repertoire of weapons, including knives, axes and handguns. The majority of jihadists in Europe still prefer to work in groups and carry out bomb attacks, but that an increasing number resort to single actor terrorism and crude weapons to avoid detection.

The most likely mass-casualty scenario is a bomb attack in a crowded area. A tactical innovation is a combination of several crude methods such as arson, armed assaults and small bomb attacks. We expect that jihadists in Europe will prefer attacking sub-national entities, communities and individuals with symbolic value, rather than societies at large. However, certain elements within al-Qaida and like-minded groups will continue to plot indiscriminate mass killings.

Looking ahead, effects of the war in Syria and Iraq may influence jihadi terrorism in Europe in several ways. Returning foreign fighters may bring with them new technologies and tactics, or they may introduce a sectarian dimension to attacks, targeting Shias or Kurds. The most dangerous scenario is that IS or like-minded groups launch a top-down organized campaign of international terrorism as a response to Western military involvement in the conflict. But the most likely effect in the short to medium-term is contagion of attack methods broadcast widely in media, such as public beheadings and other revenge-driven executions.

Considering the type of attacks, bombing was the dominant attack type, occurring in 65 % of all plots after 2008. A few hostage situations have been created by jihadis in Europe. During the period 1994-2013, there were a total of three hostage incidents. All of them occurred after 2008 and involved "Mumbai-style" plots where hostages were supposed to be held by teams of mobile gunmen inside buildings [10]. A relatively high proportion of the single-actor plots are launched attacks. However in many cases it is not entirely clear how many members of the group would participate in the attack. There is a slight increase in attacks on military targets after 2008. Before 2008 there were six plots to attack military targets, but none were launched. After 2008 there were seven plots of which five were launched. Four of the launched attacks targeted soldiers in public places, and a fifth was aimed at a military base in Italy. Attacking military personnel in public places is a new modus operandi among jihadis in Europe.

A second targeting trend is that plots against aviation and public transportation have become less frequent. After 2008, there were only three plots targeting aviation and three plots targeting buses, trains or metro systems. But this assessment must be handled carefully since the attack against the metro station in Brussels in 2015 and the plot against the Egyptian airline in 2016.[3] This example shows very clearly that it is very hard to drawn forecasts on the terrorist trends.

The rise of knife and firearm plots is part of a more general trend towards diversification of attack types and choice of weapons among jihadis in Europe.

The majority of the plots was aimed at targets such as shopping centers, nightclubs, restaurants, crowded streets and even schools, and was bound to cause random mass deaths. There has been a steep increase in single-actor terrorism among jihadis in Europe since 2008. Single-actor terrorism is usually traced to 19th century anarchists and their strategy of leaderless resistance, but right-wing extremists have been behind most single-actor incidents since the 1980s. Today, the call for individual terrorism is a main feature of jihadi propaganda aimed at followers in the West.

"The rise in single-actor plots in Europe is linked to this propaganda, but we need to consider the underlying causes. The literature on single-actor terrorism distinguishes between "solo-terrorists" and 'lone wolves.' The former operate alone, but are linked to and may receive support from an organized terrorist group. The latter act completely on their own and only draw inspiration from political movements" [11].

5 CONCLUSION

The ISIS as a continuation of al Qaeda means a threat against the whole world. The intention to become a world caliphate remains only a dream. In 2016 the organization has lost significant territories in Iraq and Syria and this tendency will continue. Unfortunately the ideology represented by the organization is spreading in the Middle East, Africa and Asia as well. The ISIS has taken the fight globally with their threats and intents to go beyond the Middle East battlegrounds.

Military actions against ISIS must be a well-coordinated air, ground, counterinsurgency, and unconventional warfare approach, including the use of psychological operations against the opposing force.

One of the most significant dimensions of ISIS is the recruitment of foreign fighters from different countries around the world. After the start of the operation, ISIS can use these attacks as a rallying ground in order to recruit more people. Such a threat can only be prevented by an effective intelligence operation, however.

ISIS does not seem like a passing phenomenon. It will appear in many countries mainly with weak governments. It is embedded in the Sunni population causing the fight and the intelligence against this organisation very difficult.

References

[1] BLANCHARD, C. M., HUMUD, C. E.: *The Islamic State and U.S. policy.* Congressional Research Service, February 2, 2017. Available at: https://fas.org/sgp/crs/mideast/R43612.pdf

[2] STARR, B.: *'A few dozen Americans' in ISIS ranks.* CNN, July 15, 2015. Available at: http://edition.cnn.com/2015/07/15/politics/isis-american-recruits/

[3] BESENYŐ, J., PRANTNER, Z., SPEIDL, B., VOGEL, D.: *Az Iszlám Állam – Terrorizmus 2.0.* Kossuth Kiadó, Budapest, 2016. pp. 11-28. ISBN 978-963-09-8441-6.

[4] BLANCHARD, C. M., HUMUD, C. E.: *The Islamic State and U.S. policy.* Congressional Research Service, February 2, 2017. Available at: https://fas.org/sgp/crs/mideast/R43612.pdf

[5] NEILL, H. U.: *African insurgent groups look to ISIS as they face increasing pressure.* IISS, 24 March 2015. Available at: https://www.iiss.org/en/Topics/islamic-state/african-groups-isis-f2d1

[6] SHERLOCK, R., WHITEHEAD, T.: *Al-Qaeda training British and European 'jihadists' in Syria to set up terror cells at home.* The Telegraph, 19 Jan 2014. Available at: http://www.telegraph.co.uk/news/worldnews/middleeast/syria/10582945/Al-Qaeda-training-British-and-European-jihadists-in-Syria-to-set-up-terror-cells-at-home.html

[7] COOLSAET, R.: *What Drives Europeans to Syria, and to IS? Insights from the Belgian Case.* Egmont Paper 75, Academia Press, March 2015. Available at: http://aei.pitt.edu/63583/1/75.pdf

[8] Security co-operation: *Jihad at the heart of Europe*. Brussels is not just Europe's political and military capital – it is also the centre of its terrorist. The Economist, Nov 21st 2015. Available at: http://www.economist.com/news/briefing/21678840-brussels-not-just-europes-political-and-military-capitalit-also-centre-its

[3] The exact cause of the catastrophe of the flight MS804 is in the time of the writing of the paper is not yet known.

[9] STEWART, S.: *Europe's Chronic Jihadist Problem*. Stratfor, Apr 5 2016. Available at: https://www.stratfor.com/analysis/europes-chronic-jihadist-problem

[10] HORVÁTH, A.: *A terrorizmus csapdájában.* Zrínyi Kiadó, Budapest, 2014. pp. 125-130. ISBN 978 963 327 600 6

[11] NESSER, P.: *Single Actor Terrorism: Scope, Characteristics and Explanations*. Perspectives on Terrorism, Vol 6, No 6 (2012). Available at: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/231/html

Col. (ret.) József Kis-Benedek, PhD. is a honorary professor in Budapest, National University of Public Service, Hungary. His background is military intelligence. He possesses a PhD degree in military sciences. Actually he gives lectures at many universities in Hungary. His areas of research are the Middle East, terrorism, intelligence and crisis management.

Col. (ret.) József KIS-BENEDEK, PhD.
National University of Public Service
Ludovika sqr. 2
1083 Budapest
Hungary
E-mail: kbjozsef48@gmail.com

FSTA 2018

THE FOURTEENTH INTERNATIONAL CONFERENCE ON FUZZY SET THEORY AND APPLICATIONS

January 28 - February 2, 2018
Liptovský Ján, Slovak Republic

The 14-th Conference on Fuzzy Set Theory and Applications FSTA 2018 will take place under auspices of the Department of Mathematics and Descriptive Geometry of Faculty of Civil Engineering of Slovak University of Technology in Bratislava, the Armed Forces Academy of General Milan Rastislav Štefánik in Liptovský Mikuláš and the Working Group for Fuzzy Set Theory and Applications of the Slovak Mathematical and Physical Association, in co-operation with EUSFLAT working group AGOP and SIPKES s.r.o.

INTERNATIONAL SCIENTIFIC PROGRAMME COMMITTEE
Chair persons: MESIAR Radko (Slovak Republic), SAMINGER-PLATZ Susanne (Austria)

SCIENTIFIC PROGRAMME
The Conference Scientific Programme will consist of special invited plenary lectures, invited and contributed parallel sessions. Rooms can be provided for workshops and special invited sessions during the conference. Please, send all suggestions for workshops and invited sessions to Prof. Radko Mesiar (radko.mesiar@stuba.sk) no later than September 15, 2017.

More details: See the Conference website: **www.math.sk/fsta**

INFORMATION SECURITY MANAGEMENT SYSTEM IMPLEMENTATION

Lubomír ALMER, Petr HRŮZA

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.

1 INTRODUCTION

Nowadays, there are many security tools, which we can mark as a preventive tool. First and key point of cyber threats prevention is to follow currently valid legislation. In Czech Republic, we are talking about Cyber Security Law and legislative decree. Implementation of Information Security Management System according to Cyber Security Law is the one of the key preventive tools. Next preventive steps should be securing the network infrastructure sectors. These sectors can be secured by many ways, one of the ways how to secure our infrastructure around sectors is shown below. In the second instance, the penetration tests and various information audits take place. These processes illustrate basic steps how to secure our infrastructure. Every infrastructure is unique, so this procedure is not mentioned to be applied across the board – in terms that it has to be moderated according to the specific requirements of the infrastructure security [1].

2 CRITICAL INFRASTRUCTURE PROTECTION ISSUES

Modern society depends on good working infrastructure, specifically their technical part as supply of water and food, electricity, heat, fuels, communication, mobility, etc. Non-working infrastructure had bad impacts on fulfilling of human basic needs and quality of human life. Technological infrastructure together with management infrastructure creates society infrastructure. Trends of increase complexities of infrastructure had consequences. These consequences could be increase of uneasiness and no determinacy future sustainable evolution. These facts put big demands on public administration, specifically on strategic thinking and system stance. Reason of this is simple, main purpose of public administration is satisfaction of value and necessity of public. The first protection problem of critical infrastructure is complexity [2, 3].

Next issue with protection is owner issue. If owner of critical infrastructure object is subject, is difficult to control their level of security, eventually intervene it. In case of state ownership, this problem disappears. Other issues with protection could be legislative issue and their enforcement. Cyber security law and following regulations set us requirements for safety system, but these requirements has general characteristic with link on family of norms 27 000. Example of this could be security policy. In Cyber security law is set you have to have security policy, but nowhere is specification how she has to look like.

3 INFORMATION SECURITY MANAGEMENT SYSTEM IMPLEMENTATION

Implementation Information security management system according to cyber security law, regulations no. 317, standards ISOI/IEC 27001 and 27002 is really complicated and lengthy process. Implementation process according to previous thinks shows following chart. For clarity, entire implementation process merged into several sub-parts. First phase is Preparing phase, it includes four activities. Second phase is Risk management phase, which also includes four activities. Third and Fourth phases is Creation of security policy together with Plan of implementation security measures according to Cyber security law. Fifth phase is Project implementation of security measures. Sixth phase Information security management system implementation. Seventh phase Operational tasks of Cyber security law. Eighth phase is Audit and control, which includes three activities, in this case we are talking about internal audit and control. Last, the ninth phase is Control audit from department. Each of these phases is indispensable in process of implementing Information security management system. Typical for each phases there are input and output documents, which help, using decision-making processes focused in cyber security field [4].

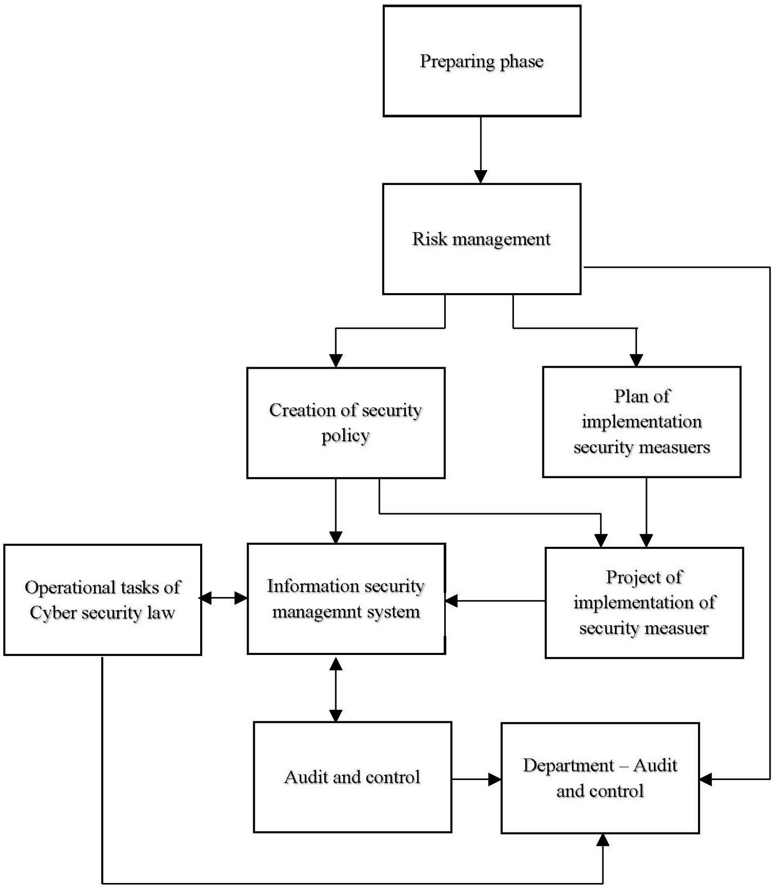

Preparing phase
Risk management
Creation of security policy
Plan of implementation security measuers
Operational tasks of Cyber security law
Information security managemnt system
Project of implementation of security measuer
Audit and control
Department – Audit and control

Fig. 1 Information security management system implementation scheme

Before preparation phase there is an important step. This step is identification of authorities and persons, which have duties in the cyber security field. This authorities and persons is determined by cyber security law (provider of electronic communications, an authority or a person ensuring important network, information system of critical infrastructure administrator, communication system of critical infrastructure administrator, administrator of important information system, etc.).

Preparing phase includes four steps. First, the duties of subjects are identified, if these duties are set, they have to be reported to National Security Agency. Second step is the establishment of the committee and the role of cyber security. The entry into the second step is methodology creation of the cyber security. Output of this step is the cyber security strategy. We recognize four roles of cyber security: the manager of cyber security, architect of cyber security, auditor of cyber security and guarantor assets. Afterwards the assessment to Cyber security law is confirmed. In this step, we validate the currently implemented measures with the measures set in the Cyber security law.

Risk management phase includes four steps. First step is the Identification and evaluation of assets. Input document for this phase is the methodology of identifying a range of system and assets. The one of the most important outputs of the risk management phases is the asset register. Second step is the identification and evaluation of risks. Input for this step is the methodology of identification of risks. Third step is preparation statement of applicability and fourth step is preparation risk management plan. Output of the fourth step is the risk management plan. As primary threats, there are considered, for example: cyber attack from communication network, malware, violation of security policy and many more.

Creation of security policy, security policy is the necessary part of basic management plans. This policy includes wide and highest organization policies leading to protection of personal and assets. Information system administrator in cooperation with important system administrator has created this policy. The subject who creates security policy is responsible for updates.

Plan of implementation security measures according to Cyber security law and project implementation of security measures, input for this is model plan for introducing security measures. This plan is a partial input for project implementation of information security. Without this plan, we are not able to create the project. Output of this plan is the specific security documentation [6].

Information security management system implementation. After the previous steps are applied, everything necessary is thus ready for the implementation of Information security management system into operation. When the Information security management system is implemented, our system is thereby prepared for the first part of an audit. This system must adhere to operational tasks from Cyber security law.

Audit and control this is internal part of audit and controlling process. First step is the assessment of conformity, followed by corrective measures. Unless there is a compliance with established measures, the corrective measures will be, followed by the internal audit of entire system. All corrective measures must be properly recorded. Input for this audit is Cyber security law. This internal audit and control process are followed by the audit from department [6].

4 SECURITY NETWORK INFRASTRUTURE

Secured infrastructure is one of the primary points to ensuring cyber security. For clarity, lucidity is network infrastructure divided into three sectors. Security tools used in various sectors form a comprehensive security measures for the overall security and visibility of the network incidents. These tools enable to us much easier handling with security incidents and general network management. Usually is made for network administrators or for those engaged in computer network security. Network infrastructure are divided into different sectors, it is a sector of perimeter security, network visibility and security and endpoint security. Not all security tools can be integrated into only one specific sector. The reason is the interdependence of the various security tools and sectors. Each sector contains a number of security tools, some of these elements are useful for detection, some of the prevention against cyber attacks and some for both. In case of second sector, there are no security tools there is standards, which provide us opportunity for network monitoring and visibility. For coverage from all three sectors, we can talk about achieving an acceptable level of network security [6].

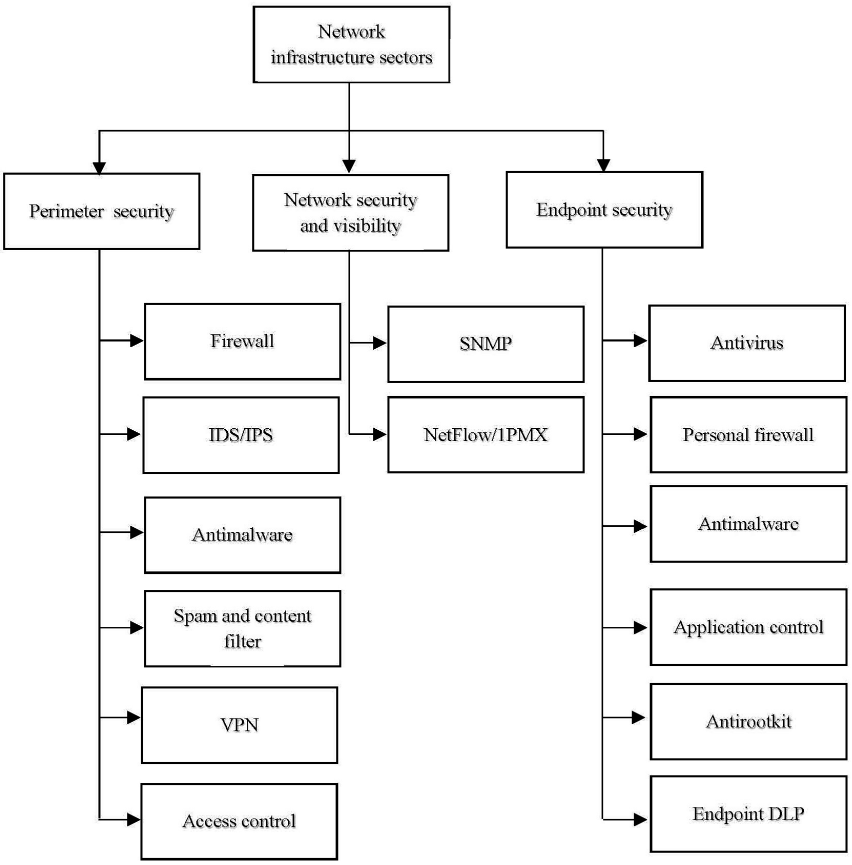


Fig. 2 Network infrastructure sectors

Opportunities for detection of cyber attacks are many. In each perimeter contains detection tools, for detection together with mitigation tools for redirection or elimination of cyber attacks. Every infrastructure is different so we have to implement different security tools. In every case, we do not have to use all of upper mentioned security tools [5].

Perimeter security is provided by six security tools. We are talking about firewall, IDS/IPS system, Antimalware, Spam and content filter, VPN and access control. This security tools can be extended by others. Extension of these can be UTM system, the fact that UTM system is an upgrade we mean it contains almost all of the above tools and form a single harvest security tools with central management. UTM system can be extended by load balancing, quality of services, SSL and SSH inspection, application awareness etc. Each of perimeter security tools has a unique and indispensable role in perimeter security, also as every harvest is used to detect different type of attack [6].

Network security and visibility sector, basic monitoring includes availability monitoring services and servers, CPU load, memory or disc full, status of network interfaces but also the number of transmitted packets. Such monitoring corresponds to the current infrastructure monitoring usually based on SNMP. Such monitoring can be considered as mandatory equipment of the data network manager. Nowadays more and more sophisticated and complex attacks, however, such monitoring is not enough. We required monitoring network traffic, which is known as next-generation monitoring. This monitoring creates aggregate statistics about transmission of all data, leads to abstraction from individual and communication content is not monitored. Many features could extend the network monitoring. Good example of this extension is the protection against volumetric denial of services attacks. Current market provides many ways how to protect our network against this threat. As an example, the use of the scrubbing center, which redirects harmful traffic e.g. into the black hole and releases the legitimate traffic. So our network is safe and normal traffic has not been affected. The next extension feature could be the Application Performance Monitoring. This type of monitoring is based on the service level agreement. The time of each transaction has to be set. This monitoring helps to identify where the problem on our network is, and to optimize it.

Endpoint security sector ensure generally famous security tools, such as antivirus, personal firewall, antimalware, application control, Antirootkit and endpoint DLP. All of these security tools are used for detection. We cannot say that without these security tools must not talk about secured end stations. In case the correct set previous security tools, it is possible that the assault end station will be avoided [7].

5 PENETRATION TEST AND INFORMATION AUDITS

Penetration test together with information audits are the next step of cyber security prevention. There is lot of opportunities how to make a penetration test or an information audit. As a first step of penetration test can be OWASP Top10 methodology which demonstrate us 10 most frequent bugs, or more precisely sectors where we blunders. Penetration test can be divided into basic tools and others tools. Basic tools are the web browser extended by pluginsand testing proxy. Other tools are downloading files for example wget, curl, scripting language shell, python, php and many more for mapping and scanning. In case of using the web browser for penetration testing, we have to configure our browser. It means the form of appearance and behavior of our browser, work, reading and manipulation with HTML and JavaScript code, control communication between browser and server, make easier access to information remembered in browser, tools for automatization tests, tools for coding and decoding, etc. Example of extension of our browser, are firebug, web developer for work, reading and manipulation with HTML and JavaScript code. For controlling of communication between browser and server: User Agent Switcher, RefControl and Modify Headers. For facilitation to access to information: Cache Viewer, CookeSwap and Cookies Managers. For effectivity of work in testing process: Unhide Passwords, Skip Cert Error, FoxyProxy. These are a few basic plugins for penetration testing in web browser. These “basic” tools can be of course extended for many others. Of course, the penetration testing must be customized according to our infrastructure [7].

6 CONCLUSION

Implementation of Information security management system by Cyber security law and ISO/IEC standards together with sector security tools and penetration test and information audits could be considered as a prevention steps against cyber threats. If we implement all of these, we can talk about acceptable level of cyber security. Unfortunately, the cyber threats can change within minutes, the process is never ending. Generally, we can say that the cyber threats are constantly one-step ahead before the cyber security. We should update our security tools every day, and keep our solutions updated. All of these prevention steps and tools must be modified according to our requirements. Every infrastructure is different so we cannot apply the same measure in every case. We have to modify all tools mentioned above.

Acknowledgment

This work was supported by the project no. VI20152019049 "RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems" supported by the Ministry of the Interior Security Research Programme of the Czech Republic in the years 2015-2020.

References

[1] Act No. 181/2014 Coll. on the Cyber Security and on the Amendments of the Related Acts (Cyber Security Law).

[2] Regulation No. 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures (Cyber Security Regulation).

[3] LUKÁŠ, L., HROMADA, M.: Valuating the Resistance of Critical Infrastructure. In: *Bezpečnost v informační společnosti*, Brno, 2009, p. 56, ISBN 978-80-7231-653-3.

[4] Regulation No. 317/2014 Coll. on the Determination of Important Information Systems and their Determination Criteria.

[5] Decision of the Government No. 315/2014 Coll. Which amends the Decision of the Government No. 432/2010 Coll. on the Criteria for the Determination of the Elements of the Critical Infrastructure.

[6] ISO/IEC, (2013). ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements.

[7] ISO/IEC, (2013). ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls.

Eng. Lubomir ALMER
University of Defence
Faculty of Military Leadership
Kounicova 65
662 10 Brno
Czech Republic
E-mail: lubomir.almer@unob.cz

LTC Eng. Petr HRŮZA, Ph.D.
University of Defence
Faculty of Military Leadership
Kounicova 65
662 10 Brno
Czech Republic
E-mail: petr.hruza@unob.cz

Eng. Lubomír Almer – He received the Ing. Degree in Security management from the Faculty of Military Leadership, University of Defence in Brno in 2016 (master thesis: Cyber-attacks and protection of critical infrastructure subjects). In 2014 he successfully finished his Bc. Degree in Cyber security management at the same university (bachelor thesis: Cyber attacks in CZ). From 2016 to present, Lubomir is on Doctoral studies and his doctoral thesis is: Organizations Cybersecurity. Since 2013 he has been a member of AFCEA and after few years he has been in the position of Vice President for University of Defence student's chapter. During AFCEA membership Lubomír won two awards: Distinguished Young AFCEAN Award and Emerging Leadership Award, both in San Diego, California and published many articles about cyber security topics. Since 2013 he has been a member of Cyber Security Working group. In 2015 Lubomir was cooperating with Flowmon Networks Company for one year as a Junior Product Manager. From April 2017 to September 2017 he was cooperating with Deloitte Advisory as a Cyber Security Consultant. Currently he is working for AEC as an IT Security Consultant. Lubomir focuses on security of information systems and cyber security. He specialises in analysing the current state, compliance of IT security with technical norms and legal requirements (ISO IEC 2700x, Cyber Security Act, GDPR, etc.) and suggesting measures for achieving compliance with the requirements and increasing security.

LTC Eng. Petr Hrůza, Ph.D. is a teacher at the Department of Tactic, University of Defence, Brno, The Czech Republic (e-mail: petr.hruza@unob.cz). Hrůza was born in Znojmo, 1969, The Czech Republic and became an Engineer of Information system at the Military Academy in Brno, The Czech Republic in 1995. In 2005 he earned a Ph.D. at the University of Defence in Brno, The Czech Republic. Since 2008 Hrůzas' major field of study has been cyber security management.

From 1988 he served on various military posts. Since 1995 he has worked as a teacher, since 2008 as cyber security Lecturer at the University of Defence in Brno. He is a member of AFCEA.

Petr Hrůza has published and cooperated on tens of articles and eight books, above all "Cyber security" (Brno, The Czech Republic, University of Defence, 2012), „ Cyber security II" (Brno, The Czech Republic, University of Defence, 2013). At the centre of his previous research interest have been methods of decision making support in command and control, nowadays he focuses on cyber security management, laws in cyber security, security standards and Internet of Things.

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

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.

1 INTRODUCTION

In the present world up-to-date, reliable information and the ability of its processing is the key to success and a guarantee of effective performance [1].

Information is the basic element used in the process of decision making. The process is quiet often realized in the condition of significant uncertainty and time restrictions. The process can be supported by proper tools which enable the creation, transfer, processing as well as storing of information, which might exert a significant influence on the pace and aptness of the made decisions.

In land forces, the process of decision making is carried out during the decision cycle realized in the framework of military decision making process (MDMP) [2]. In this process information is created, gathered, prepared, processed and sent.

During this process with the use of modest base of tools, the user equipped with modest base of tools, is able to master the set and choose proper applications which are needed at a given moment to attain the set goals, e.g. assessment of the combat potential, calculation of artillery support, etc. However, it is quiet problematic when there is one complex application without intuitive interface or a big set of singular applications, in such case finding the one which is needed at a given moment is rather difficult for the user [10].

Soldiers have some distinctive features, namely the speed of action in the first place, mobility, as well as the security of the undertaken actions. Support of these activities need the necessity of research focused on finding certain solutions which enable the creation of conditions proper for the implementation of tools supporting information relations in the network of tactical command posts.

2 THE CHARACTERISTICS OF THE NETWORK TACTICAL COMMAND POSTS

Military Decision Making Process is realized in the network of tactical command posts. Human, organizational, and technological elements constitute the basis of the process; they are interrelated by defined relations within the command and control system [3].

In the Polish literature on the theory and practice of command and control [8] one can find the following division of the key components of the command and control system (Fig. 1):

- organization of command and control (OC2),
- military decision making process (MDMP),
- command and control measures (C2M).

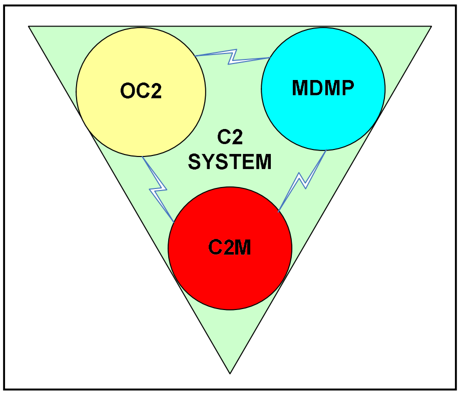


Fig. 1 Command and control components

Making decisions is the basic domain of human activity in a military organization [14].

In this process there are similar common stages regardless of the contents of the discussed problem. L. Chatelier is the pioneer of this kind of approach. He invented the concept of organized action cycle, according to which the effectiveness of performance is determined by proceeding which should be realized in an organized way. According to the theory, the organized action cycle should be carried out in line with five stages:

- setting the goal,
- checking the measures and methods,
- cumulating measures,
- carrying out the action,
- controlling the results.

It has been assumed that in a military organization decisions are made within one of the three components of command and control system, i.e. in the military decision making process (MDMP). The automated information-decision process is realized by the command and control bodies located in the network of command posts at a given organizational level with the aim of making the final decision and passing it to the executors [8].

The decision cycle is realized in accordance with a certain plan accepted in a military organization, which has been presented below on Fig. 2.

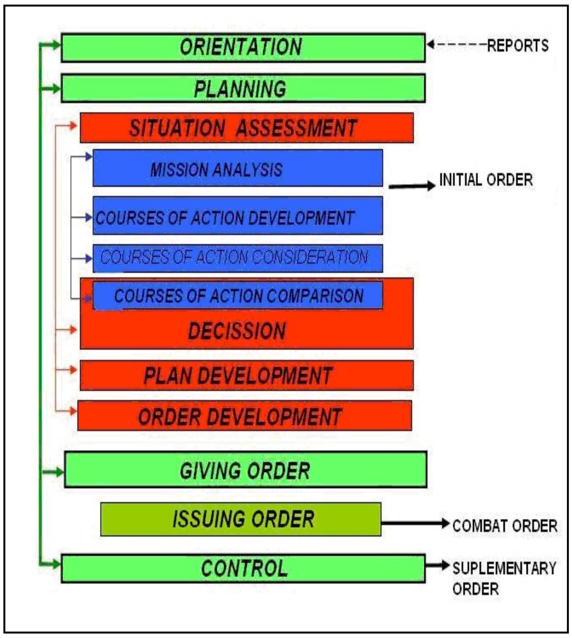


Fig. 2 Scheme of conduct of the command and control body in accordance with the military decision making process [8]

The military decision making process and the structure of command and control body are inseparable. In the land forces the mechanized brigade is the core unit and its structure has the following characteristics:

- commander and commander's group,
- chief of staff of the command and control body,
- commandant of command post,
- command and control team with specialized groups,
- planning team with specialized groups,
- reconnaissance team with specialized groups,
- support team with specialized groups.

Information supply constitutes the basis of functioning of any organization. The process of information exchange in such organization requires proper routs for information flow, the so called information bounds. Fig. 3 presented below indicates the relations of information flow in a mechanized brigade in a constellation with the superiors and subordinates.

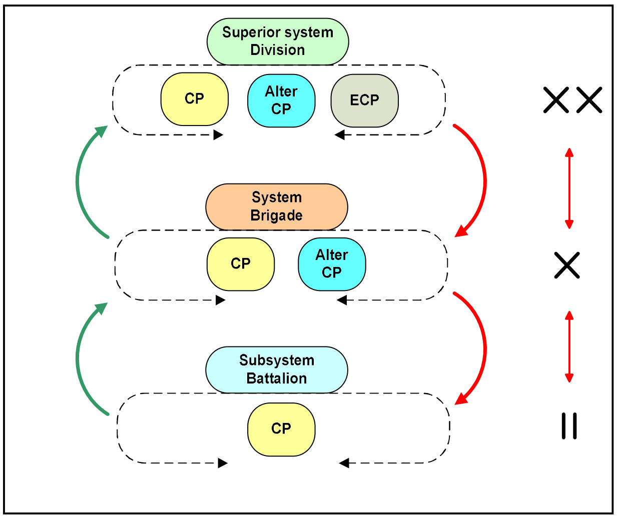


Fig. 3 Information relations brigade in a mechanized between the superiors and subordinates [3]

The subject literature provides their different division, the author uses the division in accordance with the criteria presented below [8]:

- organizational structure,
- the direction of information flow,
- the direction of bounds.

In accordance with the first criterion, the organizational structure, the following division is assumed:

- official – reporting bounds (Fig. 3),
- coordination – cooperation bounds within the same level or between different levels without the participation of superiors,
- cooperation – bounds between the elements which do not have the reporting bounds.

According to the next criterion namely the direction of information flow, the following types of information bounds are distinguished:

- external incoming – concern the information gathered from different official sources and others,
- internal – information passed inside the command post,
- external outgoing – information sent outside the command post.

The last criterion: the direction of bounds, indicates the following division:

- official – concern decision-related authorization,
- functional – concern professional competences,
- informational – concern information exchange.

3 THE CONDITIONING OF THE SUPPORT OF INFORMATION RELATIONS IN THE NETWORK OF TACTICAL COMMAND POSTS

The pursuit of network centric capabilities by the NATO member states emphasizes the existence of the transition state between the search for new solutions being in line with the network-centric requirements and solutions which improve the tools being used now [1]. In the author's opinion it is impossible to avoid this state, though it can disorganize the operation and trigger certain problems connected with the implementation of new solutions among the recipients.

The carried out research indicates the dissatisfaction with the tools (applications) used to support the military decision making process, in particular lack of such tools or their unsatisfactory effectiveness.

As for the transition state, research here is vital for a fluent passage to the new conditioning as well as overcoming mental resistance of users or recipients to apply new solutions. Moreover, a cyclic research in this field can help to specify the needs of the interest groups who the solutions are earmarked for. It is unacceptable to create tools which not only fail to support the military decision making process at a tactical level but even prolong it.

In a military organization it is vital to differentiate precisely the roles of two basic parties which are involved in ICT support, namely: the recipient and provider of services [6].

The differentiation is necessary due to the fact that in the command and control system the main tasks of the provider of services and of the recipient i.e. the command and control body are different. Taking allocation as the example, the command and control body is responsible for the preparation of plans and their implementation in order to carry out operations; while the provider's task is to support, render ICT services which enable the command and control body to attain its goals.

The research on ICT support was carried out in the functional area of command and control system, namely in personnel, organizational and technical aspect. However, in this article the author presented only part of research results referring to a system including the application supporting the military decision making process in information relations in the network of tactical command posts.

In the recipient aspect, first off all the focus was put on the possibilities of providing IT support to the people performing given functions, where 43 % of respondents said that it is insufficient, while 39 % of them expressed their satisfaction (Fig. 4). At the same time, 68 % asked about the usefulness of computer-assisted applications in a military decision making process voiced such a need. The above shows that the users prefer applications which support the military decision making process to the traditional mode.

As the example we can present the result of research where 57 % of respondents said that they have never used such an application but at the same time they said that it would be useful in their scope of interest (Fig. 5).

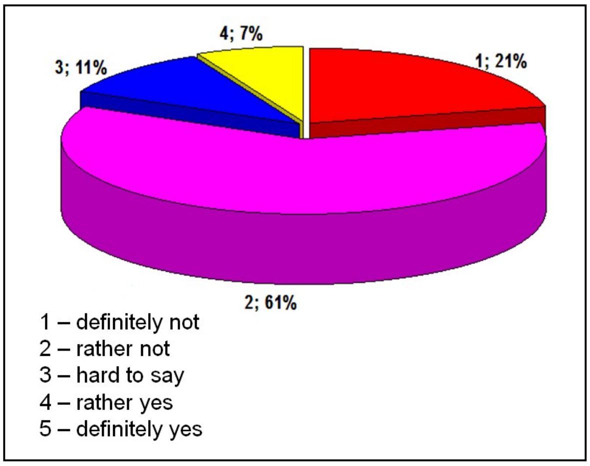


Fig. 4 The division of respondents' opinion who have never used the computer-assisted applications but express their usefulness in their scope of interest [3]

At the same time it should be mentioned that the respondents assessed the level of difficulty of such an application (application's intuitiveness) as average (71 %) or high (18 %).

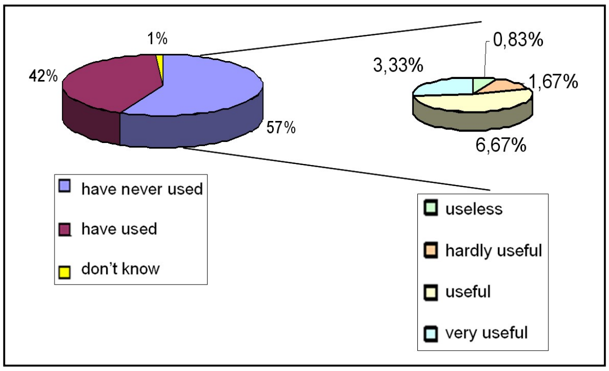


Fig. 5 The division of respondents' opinion concerning the functioning of the application supporting the military decision making process [4]

One of the difficulties pertaining to the application usage is the manual which is not useful and clear enough, only 30 % of the surveyed had positive opinion about the clarity of the application's manual. A significant group of respondents – 50 % gave the answer *"hard to say"* and 21 % assessed the manual negatively. The fact clearly confirms the tendency that users do not want to read a manual, they prefer to discover the application personally by a trial and error method. The fact emphasizes the need to modernize the application so that it is intuitive as far as its usage is concerned.

A separate issue is the level of satisfaction of the application users, since 82 % of respondents indicated different types of problems concerning the application functioning (reliability of software) and only 7 % of the surveyed did not voice difficulties in this scope (Fig. 4).

As far as ergonomics of the user's interface is concerned, over half of the users (57 %) were positive about it while 32 % had negative opinion. It shows that, in spite of faults and problems with proper functioning, computer-assisted applications are needed, and further work should be continued in terms of the improvement of the quality.

As for the usefulness of applications supporting the military decision making process, the experts determined the importance of the services rendered to the command and control body, where unanimous operational picture as well as the automated command and control systems were indicated most often. Additionally, the experts who have participated in missions abroad emphasized the important role of *"WWW"* service in the form of informational portal and data base access interface.

An interesting issue stemming from the carried out research is the relation between the respondents' declaration concerning the usefulness of the application in their scope of interest and the participation in a training as well as the usage of application supporting the military decision making process (Fig. 6).

The graph shows a favourable correlation between the respondents who used the application and participated in a training concerning its usage.

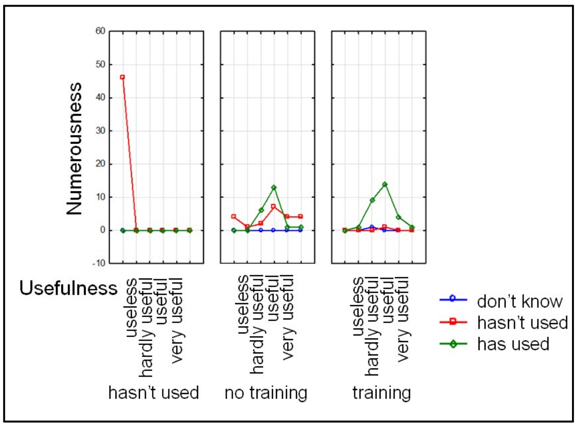


Fig. 6 An interaction graph in relation to work with computer-assisted application, participation in a training and application's usefulness in the military decision making process [3]

In the author's opinion, taking into consideration the above analysis, there is a need for research in the scope of computer-assisted applications, their implementation and organization of trainings which teach how to use such applications. All this can contribute to the effectiveness of work carried out by the command and control body on a command post.

As for the recipient aspect in the scope of computer-assisted application's functionality in the military decision making process, the opinion of respondents and experts allowed to define a set of needs referring inter alia to the following factors:

- easily operated and intuitive user's interface,
- easy access of subordinates to network resources in case of having proper access rights e.g. for the commander of unit,
- surveillance of the realized undertakings within the military decision making process,
- group work with command and control documents, planning and informative documents within the same section as well as different sections,
- simple and advanced search for information;
- preparing the work plan of the functional sections on the basis of the plan of the chief of staff,
- possibility of notification about break-downs or about the need for technical support,
- easy access to information for the organizational sections of the command post,
- running and electronic log of combat activities;
- support of the process of preparation and carrying out briefings,
- clear set of functionalities, convenient for the operator in the military decision making process;
- easy communication within the command post and outside,
- simple and clear manuals,
- surveillance of the reaction to incidents.

As for the provider aspect, in the technical area which assures the functioning of the application supporting the military decision making process the respondents and experts indicated the need for solution which should guarantee the realization of inter alia the following factors:

- additionally, assurance of constant cooperation between the command post and alter command post,
- users' access to the ICT network resources from any place of the command post,
- assurance of operations reliability (proper resources redundancy),
- easy management of server and client environment,
- guarantee of reliability as far as the functioning is concerned and assurance of the necessary application resources which belong to the command and control supporting system e.g. domain server

"Active Directory", "DNS" server, data base server, server for data exchange, etc.,

- easily done back-up copy of ICT network resources,
- explicit monitoring of ICT network resources, reporting, alarming, etc.,
- easy and fast environment recovery,
- solution's flexibility i.e. assuring ICT network resources in line with the needs of the command and control body (fast configuration),
- limitation of the number of equipment inflicted by the place and possibilities of power supply.

4 THE SOLUTIONS TO SUPPORT INFORMATION RELATIONS IN THE NETWORK OF TACTICAL COMMAND POSTS

The research as well as the experience gained by the author in the scope of ICT networks implementation [5] [7] enabled the preparation of the final solution in the framework of network platform enabling the implementation of an application supporting the military decision making process based on the ICT virtual environment (presently there are a few leading producers of such technology on the market, inter alia: "*VMware*", "*Citrix*", "*Red Hat*" as well as "*Microsoft*").

Proper hardwired platform together with dedicated software fashion the concept of this solution; this assures the cooperation of physical resources for the benefit of virtual ICT environment (Fig. 7).

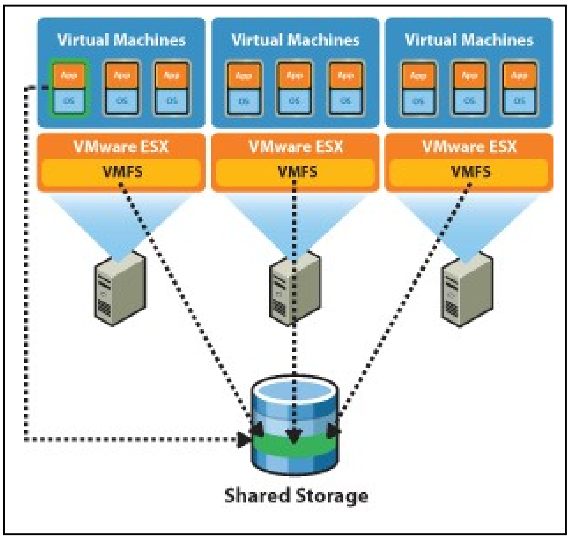


Fig. 7 The scheme of functional structure of the presented virtual environment [12]

The environment consists of the following elements:

- virtualization platform - "*hypervisora*", which task to manage the physical resources (processor, upper memory, disc storage, etc) and provide the virtual elements with access to the resources,
- virtual machines – elements in the structure of virtualization platform reflect physical servers which include varied operating systems (e.g.: „MS Server 2003", „MS Server 2008 R2", "Linux" systems),
- virtual desktops - desktops – elements in the structure of virtualization platform reflecting the physical workstations of the system operators, they include operating systems (e.g.: „MS Windows XP", „MS Windows 7") [13],
- virtual ICT resources – elements of virtual platform which enable to connect virtual machines, desktops between one another on the virtual platform as well as communication between the virtual platform and physical infrastructure of the ICT network.

Applying the suggested solution concerning the virtualization of the ICT environment brings inter alia the following benefits:

- consolidation and optimization of the ICT infrastructure – optimization of the previous infrastructure by the transformation of physical elements into the virtual ones e.g. physical servers in a virtual machine etc.,
- improvement of activities continuity – assurance of high availability understood as the ability of data recovery and migration of applications at work ("*vMotion migration*" service),
- optimization of virtual environment – automated allocation of resources by mechanisms which assure even load, power management and resistance of virtual environment to the breakdown of a single physical host,
- dynamic adjustment of ICT resources to the needs of the command and control body – scalability of virtual environment dependant on the pool of virtual resources and not on particular resources of physical servers,
- easy management of the virtual environment by transparent control and scalability of virtual machines network,
- provision of application services in the scope of high availability – assurance of constant operation of the command and control body as well as surveillance of the potential loss of data, security – simplified security mechanisms concerning the security policy on a logical level within distinguished logical spheres of the virtual environment; scalability – the possibility of environment's calibration due to the functions of central management of virtual machines and hosts "ESXi",

- open architecture – possibility of integration of solutions provided by other companies which are based on „API" interface which match the producer's products.

The author's experience in implementing and handling of applications supporting the military decision making process as well as the carried out research allowed to prepare the final shape of the presented solution in the framework of application platform, based on the system supporting military decision making process with the informational portal of the command post ("*WWW*" service).

The structure of the informational portal of the command post is divided into two-parts.

The first part of the portal namely the IT part is dedicated to all users who typed "*IP"* address or the name of the website of a given organizational unit in a web browser. In order to prevent the access of unauthorized people, only a site from trusted networks with proper reliability certificates can be displayed. In this part, basic information about the organizational unit, namely the name, status, task, location, contact data, etc. is displayed. Moreover, there is a form to log for people who are authorized to visit the second part of the portal (intranet). Every user account for logging has certain access rights to particular portal functions. A good example is the differentiated access to the calendar module of organizational section which can be modified only from the account of the chief of the organizational section, the other users can only read the contents or are not allowed to display it at all.

The second part of the portal is earmarked for the command and control body of the command post and for the users authorized to use the resources places in this portal. The structure of the intranet part of this portal is illustrated below in Fig. 8.

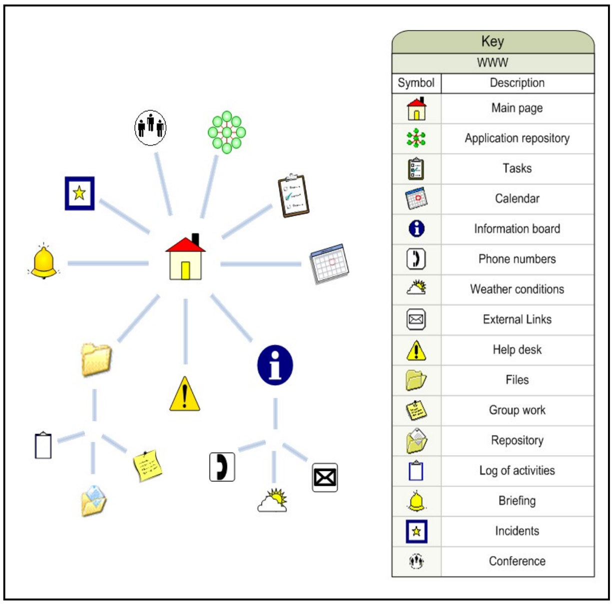


Fig. 8 A map of informational portal of the command post [3]

Applications repository is a vital element of the informational portal structure.

The research indicates that it is a must to study the ergonomics of user's interface, thus, the author suggests to create the repository of different applications (which often have a single function) to be downloaded and installed by the user. The operator decides what is needed and useful. If the application does not meet the requirements or is no longer useful it can be uninstalled. The service provider can study the statistics of applications' usage which provides information about the most and the least frequently used applications, thus the latter ones can be changed or removed from the repository.

The application repository is a platform with different applications falling into certain categories dedicated to the command and control body with the aim to support the military decision making process. The categorized applications available in the system facilitate the fulfilment of different tasks, which allow the operator to work faster, e.g. calculate something, browse the data base in search for information, plan the marching column, compare the potential of the national and the opponent's troops, etc.

In order to group certain functionalities which enable the automation of operator's activities, the applications are classified in accordance with the topics presented below [3]:

1) Common Operational Picture (COP).
2) Documentation.
3) Communication.
4) Organization and planning.
5) Specialized (types of military occupational specialities).

Depending on the functionality of a given application it can be placed in several places in the repository. They are displayed on the basis of the assigned category stated in the description, e.g. COP and specialized.

In order to provide the operator with a rough description of the application's possibilities, each of them is equipped with a metrics including the description in accordance with the below presented template [3]:

1) Application's name (logo).
2) Application's purpose – the result which can be achieved when using the given application
3) Description of the application possibilities – how the application should be used.
4) Usefulness in the military decision making process – in what scope the application can be used.
5) Category – which category the given application falls in (COP, specialized itp.).

Applications repository is equipped with the function of simple and advanced search (giving additional criteria).

Another solution to support information relations in the network of tactical command posts is using software like document management system (DMS) called Knowledge-Tree (K-T).

The basic purpose of the chosen software is a document management system – (DMS). Knowledge-Tree is a system of documents' management of an open-source class under the licence of GNU (General Public License). The platform enables the creation of a repository of documents created in the process of support of information relations. The functions of the software support command body in the network of tactical command posts most of all in the scope of documents. Moreover, the implemented mechanisms of information flow make it possible for the platform to initiate e.g. the procedure of documents' approval by many recipients. The platform, supplemented by additional rules connected with the archive and the circulation of documents, can be a priceless tool used by a command body on the command post.

The basic functionalities of the software include: [15]:

- dashboard,
- advanced search,
- documents history,
- repository,
- workflow,
- group work on the documents,
- viewing document permissions,
- version control,
- viewing users permissions,
- starting DMS platform only through server installation; remote access through a webpage.

DMS user, depending on the possessed permissions, has different possibilities of using the functions connected with documents' management in a system. The functions can be divided into two basic groups [15]:

- actions on folders,
- document actions.

Functions connected with folders [15]:

- adding folders,
- adding documents,
- renaming folders,
- assigning tasks to groups and users,
- permissions on viewing and editing,
- viewing the history of operations performed on a given folder,
- configuration of the course of work (if the functions of automatic steering commenced by the administrator),
- performing on the user's local computer operations of mass import of documents (in the form of a zip file) to the system of documents management.

Functions connected with documents [15]:

- editing document's metadata,
- transferring a document into a different localization,
- viewing detailed document's data,
- changing a document's name,
- downloading a document in order to quickly go through it,
- sending the document back (re-activation) into the system – check-in,
- downloading (temporary blockage) of a document from the system in order to edit it – check-out,
- annulling the operation of downloading a document from the system,
- sending a document via an e-mail to groups or an individual user within an organization,
- displaying the history of changes to a document,
- document's archives,
- creating a thread of discussion or adding information to an existing thread,
- displaying document's workflow,
- displaying permissions (of a group or of users who are to perform a given task) which are set for a document,
- displaying or creating links to another document in a repository for a presently chosen document,
- displaying the history of action (transferring, deleting, downloading a document from the system in order to perform some operation, etc.) performed on a document.

All applications included in the repository are integrated with database structure of the system supporting the military decision making process. Such solution is based on the so called *web services*, applications are started on the server and the user is only equipped with a connector owing to which it is possible to read and write data from the application and data bases (Fig. 9).

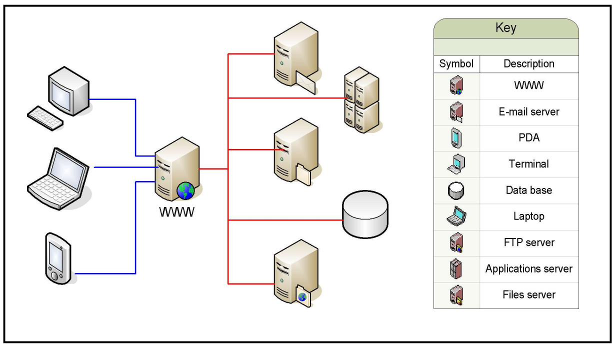


Fig. 9 The structure of the recipient's access to the ICT network resources [3]

The informational portal of command post allows the recipient to use ICT network resources of the post. The operator does not have to be aware what elements are used, functionality of the applications provided through the portal interface is what counts here. All elements at the disposal of the provider can be realized by the solutions described within the network platform, based on the virtualization of ICT environment.

5 CONCLUSIONS

Research on the functionality of the system supporting the military decision making process based on the informational portal was carried out in the scope of the needs of the command and control body of a mechanized brigade, however most of the above solutions can be successfully used also on different levels of command and control.

According to the author, however, the human factor cannot be forgotten, since even the best application will not be used by operators if they are not convinced about their functionality and usefulness.

The assessment of relation between the human and technical factor is a critical condition which leads to a challenge of both social and technical nature. Without the adjustment of the way of thinking and the patterns of human behaviour as well as organizational structures, making use of the potential hidden in the new technology can be hardly possible. On the other hand, new ICT technology can exceed the human possibility of information processing (information flow), and as a result weaken the performance and efficiency of a human being and the command and control system, regardless of the improvement of technical parameters.

The challenge connected with the adjustment of technological possibilities to the possibilities of a human being as well as the requirements of the process of social interaction of commanders, staffs, as well as civilians demands the socio-technical assessment of different attitude pattern to the discussed issue stemming from social and technical sciences.

Owing to the carried out research in the scope of information relations support in the network of tactical posts, the author gives the following recommendations:

- the research concerning the command and control body as well as the ICT support revealed the need of change of the solutions in the framework of information transfer and exchange within the command post and beyond it,
- the carried out research indicates that the technology which can be applied in this case is the virtualization of the ICT environment as well as rendering services via web services,
- hardware platform enables an easy and calibrated management of the ICT infrastructure by the system's administrators,
- the portal consists of many small applications which support the command and control body and allow for an easy and fast use of the offered services.

References

[1] PILARSKI, G.: Kierunki transformacji systemu dowodzenia w środowisku sieciocentrycznym. Article on a scientific conference: *System dowodzenia w środowisku sieciocentrycznym.* Warsaw : NDU, 2007.

[2] PILARSKI, G.: The management of ICT support for the purpose of decision making process. Article on a international scientific conference: *Manažment – teória, výučba a prax 2009*. Liptovsky Mikulas : 2009. pp 300-307. ISBN 978-80-8040-373-7.

[3] PILARSKI, G.: *Wsparcie teleinformatyczne procesu dowodzenia w brygadzie zmechanizowanej, rozprawa doktorska.* Warsaw : NDU, 2012.

[4] PILARSKI, G.: *Wsparcie teleinformatyczne procesu dowodzenia w brygadzie zmechanizowanej, załączniki do rozprawy doktorskiej.* Warsaw : AON, 2012.

[5] PILARSKI, G.: *Wykorzystanie protokołu IP w sieciach teleinformatycznych szczebla taktycznego wojsk lądowych.* Warsaw : NDU, 2007.

[6] PILARSKI, G., JANCZAK, J.: ICT Support in a military decision making process in land forces – chosen aspects. Article on a international scientific conference: *Communication and Information Technologies - 7th International Scientific Conference.* Starý Smokovec, Slovakia, 2013. ISBN 978-80-8040-464-2.

[7] PILARSKI, G.: *Wybrane problemy funkcjonowania sieci teleinformatycznej PKW w Iraku.* Przegląd Wojsk Lądowych nr 10, Warsaw, 2006.

[8] KRĘCIKIJ, J., WOŁEJSZO, J.: *Podstawy dowodzenia.* Warsaw : NDU, 2007.

[9] MANDELES, M. D., HONE, T.C., TERRY, S. S: *Managing Command and Control in the Persian Gulf War.* Westport, CT: Greenwood Publishing Group, 1996, ISBN 0-275-952614.

[10] NATO CWIX – North Atlantic Treaty Organization – Coalition Warrior Interoperability eXercise, eXamine, eXperiment, eXplore. NATO UNCLASSIFIED REL PUBLIC, 2010.

[11] RTO Technical Report TR-081", NATO Code of Best Practice for Command and Control Assessment, RTO/NATO, 2004.
[12] VMware ESXi™ 5.0 Operations Guide, Technical white paper, 2011 VMware, Inc.
[13] Vblock™ solution for VMware View 4.5 solution architecture. VCE Company 2011.
[14] KIEŻUN, W. Sprawne zarządzanie organizacją. WSoE, Warsaw, 1997.
[15] KnowledgeTree User Manual V3.5.4, 2008 KnowledgeTree Inc.

Lt. Col. Eng. Grzegorz PILARSKI, PhD.
Faculty of Military Studies
War Studies University
Al. gen. Antoniego Chrusciela "Montera" 103
00 910 Warsaw
Poland
E-mail: g.pilarski@akademia.mil.pl

Lt. Col. Eng. Grzegorz Pilarski, PhD. - academic and didactic worker, head of the Branch of Cyber Security at the Institute of Information Operations of the Military Faculty of the War Studies University in Warsaw. Research interests: cybersecurity, information protection in the Polish IT systems and networks, automated command systems, project management. He received the MSc degree in signal Systems at Military Academy of Technology in Warsaw in 2001. In 2013 he successfully finished his PhD studies in management in ICT environment at National Defense University in Warsaw. He is alumnus of the Institute of World Politics in Washington D.C in strategic studies in statecraft and integrated strategy (2017).

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.

1 INTRODUCTION

Current mass deployment of the unmanned aerial reconnaissance vehicles to the equipment of the state armies represents qualitatively different situation characterized by the possibility to deliver significantly more information about the enemies. The quality of the aerial reconnaissance results is influenced by the quality of the installed high-tech sensors. The UAVs are also installed and provided with special electronic devices, focusing also on the quality of the control systems, remote control systems, data processing, data compression algorithms and data transfer.

Furthermore, once the NEC architecture and its necessary services are implemented across the armed forces, information gathered from those sensors could be easily used across different level of command.

Advantages of the task solution in the NEC area:

- high-speed network for data transfer,
- minimal failure of data transfer ratio,
- maximum level of data transfer security,
- cnfidentiality,
- real-time transfer of data.

In the literature [2] and [3], the authors performed the research on TDOA position determination, especially on the situations from real world. Secondly, the authors in [4] and [5] tried to measure the accuracy of the localization by TDOA. Next in [6] and [7] describe the Cramer-Rao inequality method which is often used while testing target position estimation. The optimal geometry for TDOA localization was introduced in [8].

2 SENSOR DISLOCATION OPTIMIZATION IN 2D AREA

The principal of the TDOA method was described in the previous paper [1]. The main focus of the paper was taken to the factors which influence the sensors dislocation and their dislocation optimization for the most accurate location estimation of the target.

Cramer-Rao inequality is used during the testing and evaluation of effectiveness of estimate. The main objective is to formulate a lower bound on the variance of estimators.

Cramer-Rao inequality (CRB) for target vector $\bar{p} \in R^D$ and sensors $\bar{q_i} \in R^D$, where D expresses 2 or 3 dimensional area and M expresses the quantity of sensors, can be defined by [6]:

$$CRB = J^{-1} = (v\sigma)^2 (GG^T)^{-1} \qquad (1)$$

where:

$G = [g_{ij\dots}]$, (i,j)∈ I, $\quad \bar{g}_{ij} = \bar{g}_i - \bar{g}_j, \quad \bar{g}_i = \frac{\bar{q}_i - \bar{p}}{\|\bar{q}_i - \bar{p}\|}$

where:

J ... is the Fischer information matrix (FIM), (its presence ensure the existence of linear independence of vectors),
$\bar{g}_i$ ... is the vector heading from the target p to sensor i,
$\bar{g}_{ij}$ ... is difference between two direction vectors,
σ^2 ... expresses an error variance caused by Gauss noise. Set I consists of each individual sensor pair (i,j). Matrix G contains all vectors $\bar{g}_{ij}$, where (i,j)∈ I.

Many principles could be used to reach the minimum variance between the real and predicted positions.

The most widespread strategy is to find the minimal trace of CRB [6]:

$$min\, f_{CRB} = tr[J^{-1}] = (v\sigma)^2 tr[(GG^T)^{-1}] \qquad (2)$$

or we can calculate the maximum of trace of FIM [6]:

$$max\, f_{FIM} = tr[J] = \frac{1}{(v\sigma)^2} tr[GG^T]. \qquad (3)$$

Required conditions for calculation min f_{CRB} are:

1. $\sum_{i=1}^{M} \bar{g_i} = \bar{0}$
2. For matrix $D\,x\,M$ $g = [g_1 \dots g_M]$ must be $gg^T = \frac{M}{D} I$

where:

$\bar{g}_i$ ... is a vector heading from target p to sensor i,

M ... the number of sensors,

D ... area dimension,

I ... expresses matrix, where elements on the main diagonal of the matrix are equal to 1.

When sensors are located in 2D space, the solution is the matrix, where there is the same angle between each neighbor sensors. We can formulate it as following [7]:

$$\alpha_i = \alpha_0 + \frac{2\pi}{M}(i-1)(i = 1,2 \ldots, M) \qquad (4)$$

where:

α_i ... is an angle of "i" sensor,
α_0 ... is difference between first sensor and zero angle,
M ... is the number of sensors.

For another arrays, where formula (4) is not applicable but arrays are capable to fulfill conditions of minimization of trace of CRB, the following formula can be applicable [9]:

$$\sum_{i=1}^{M} \cos(\alpha_i) = 0 \quad \sum_{i=1}^{M} \sin(\alpha_i) = 0$$

$$\sum_{i=1}^{M} \cos(2\alpha_i) = 0 \quad \sum_{i=1}^{M} \sin(2\alpha_i) = 0 \qquad (5)$$

3 SENSOR DISLOCATION OPTIMIZATION IN 3D AREA

When sensors are dislocated in 3D area, we can focus our interest on solution, in which all sensors are in symmetrical dislocation and all of them have the same distance from the target.

We assume that all sensors are placed on the surface of the sphere and the target is positioned right in the middle. It is well known from geometry that exist only five relative dislocations of points in the space, which satisfied the condition of symmetry.

All faces of those solids are made by regular polygons – so called Platonic solids [6].

All vectors $\bar{g}_i$ are heading from the middle of geometric solids into their nodes. The number of nodes is equal to the number of sensors used in sensors network. Last written conditions (5) are valid for all of those Platonic solids.

Exactly as in case of dislocation in 2D area, Platonic solids, which are turned around the center, also meet conditions (5).

Superpositions of each individual platonic solid also meet conditions (5). In this case, the count of nodes (sensors) are summed.

Tab. 1 Solids and their nodes

Name	Shape	Nodes M=v
Tetrahedron		4
Octahedron		6
Cube		8
Icosahedron		12
Dodecahedron		20

A new matrix is made of multiple D x M matrices. If for each D x M $g = [g_1 \ldots g_M]$ conditions (5) are valid, then for resultant matrix $M = \sum_{k=1}^{K} M_k$ with sensors $g = [g_1 \ldots g_K]$ conditions (5) are valid either.

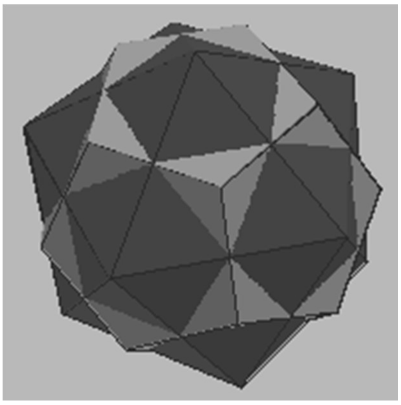


Fig. 1 Superposition of icosahedron and dodecahedron

Theory of spherical codes is suitable to used in case we need to dislocate different number of sensors which represent the nodes of Platonic solids or their superpositions.

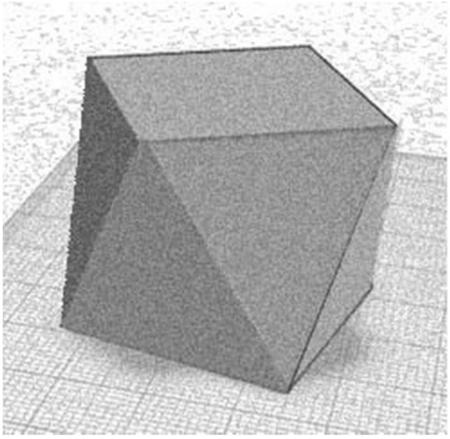


Fig. 2 Square antiprism as an example of spherical code

Each individual solids, up to M=130 nodes, are mentioned in [10].

It is well known, that most of the spherical codes are not CRB optimal, but they are very close to $f_{CRB,\ min}$. Hence, for any practical number of sensors, spherical codes can be used to design very good sensor array geometries.

4 SIMULATIONS IN 3D AREA

We assume that our sensors are carried by UAV, they are able to communicate within the network and are capable of moving in the trajectory represented by perimeter of the sphere. Second, we assume that all sensors have the same error deflection and are able to move in the same speed. The target followed by sensors is situated in the middle of the sphere.

If we assume that sensors are deployed equally around the sphere perimeter, then the formula (2) can be replaced as follows [7]:

$$\sum_{i=1}^{M} c_i^2 g_i\, g_i^T = \frac{1}{D}\sum_{i=1}^{M} c_i^2\, I_D \qquad (6)$$

where:

c_i ... is error variance of the sensor *i,*
g_i ... is vector pointing from the target to the sensor *i,*
M ... is the number of sensors,
D ... is dimension,
I_D ... is matrix of which diagonal values are equal to 1.

If previous equality is valid, then we can assume that the sensors are dislocated optimally and the minimum value can be expressed as following: $\sum_{i=1}^{M} c_i^2 g_i\, g_i^T$.

In the beginning of the simulation, each individual unit was dislocated around the perimeter of the sphere.

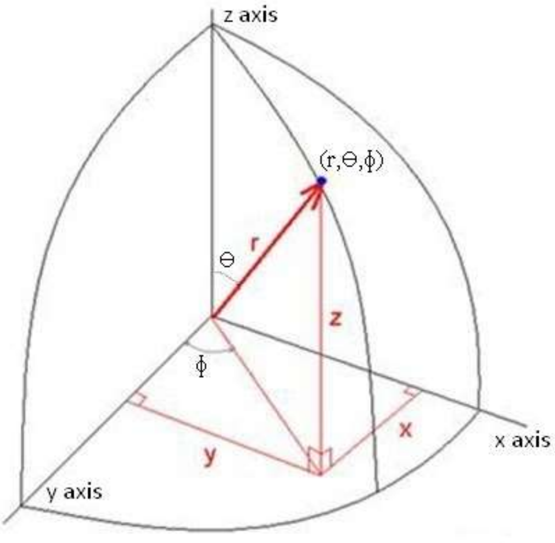


Fig. 3 Converts from Spherical to Cartesian coordinates in 3-dimensions

The coordinates of each individual sensor g_i are expressed by $[x, y, z]^{\mathrm{T}}$, where:

$x = r.\cos\phi.\sin\theta$
$y = r.\sin\phi.\sin\theta$
$z = r.\cos\theta$

In the first step, the uniform array of optimal sensor dislocations was rotated around the center in order to identify the minimum time value necessary for sensors re-dislocation from initial location to the optimal.

In the second step, based on the formula (6) and considering criteria reflecting the minimum necessary time for initial configuration changes to the optimal setting, the sensors were re-dislocated to the optimal locations.

Δ is the variance between current value $\sum_{i=1}^{M} c_i^2 g_i\, g_i^T$ and its minimum $\frac{1}{D}\sum_{i=1}^{M} c_i^2\, I_D$. If the dislocation is optimal, the Δ is equal to 0.

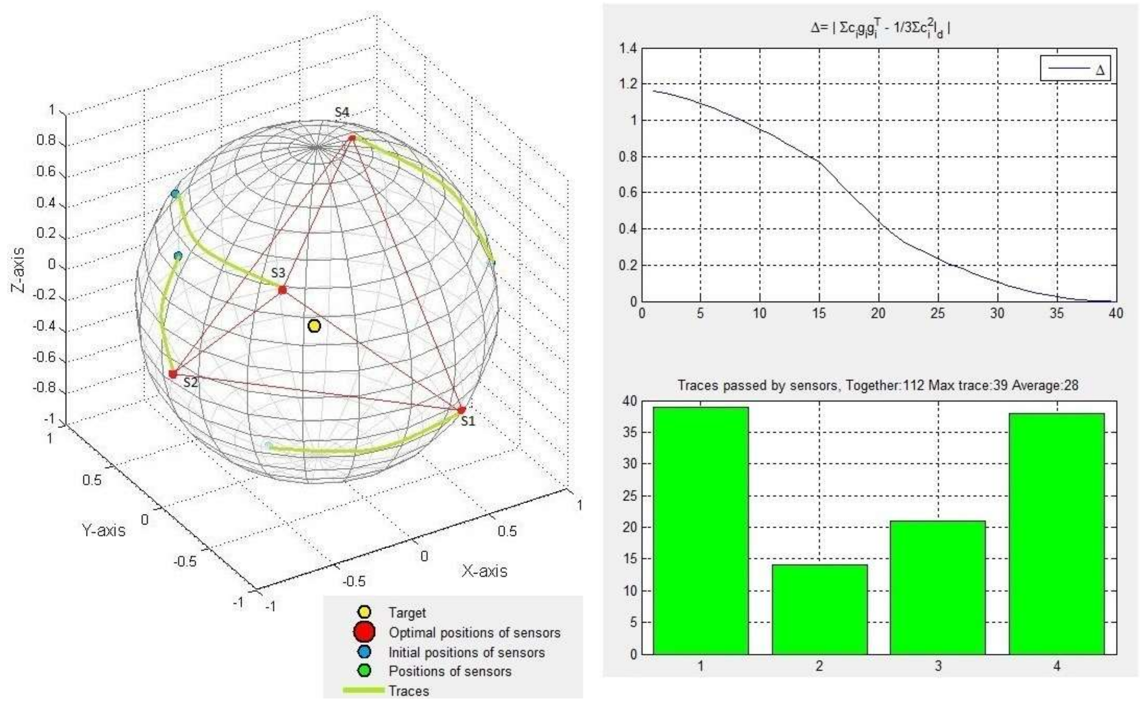


Fig. 4 The simulation of optimal dislocation of 4 sensors

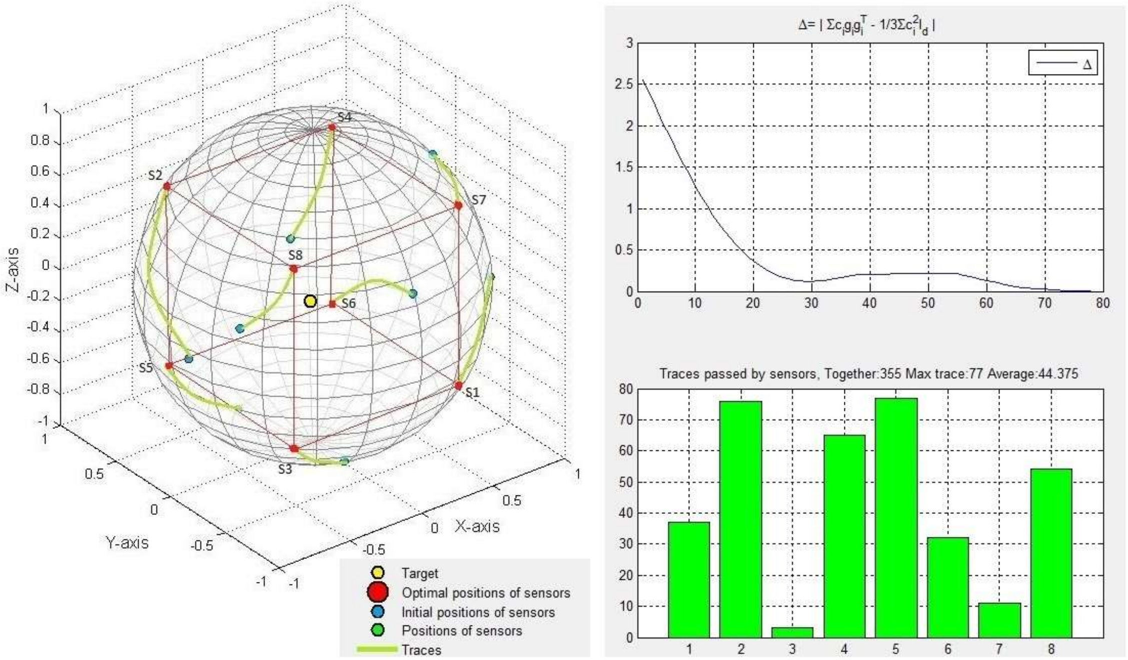


Fig. 5 The simulation of optimal dislocation of 8 sensors

5 PROBABILITY OF TARGET DETECTION

A lot of time was invested in order to find the solution for this task. In [18] authors mathematically describe the theory of communication. Secondly, the authors in [19] focused their exploration on mathematical techniques and information theory with application to radar environment. Next in [20] the authors try to mathematically describe the probability of interception of radar systems. Lastly, in [21] the author focused on an analysis of detection of signals in noise and to show how exact mathematical formulations of radar problems can be simply derived from probability theory.

The main task of the radio-location system is to recognize echoed signal in the reflected waves. Signal recognition is an statistical issue of the random event and parameters of the received signal are considered to be as random values.

Received signal $u_1(t)$ is the input signal, which is the compound of frequencies of echoed signal $s_1(t)$ and the noise $n_1(t)$ or just the noise $n_1(t)$ alone. The formula for echoed signal can be written as following [11]:

$$u_1(t) = As_1(t) + n_1(t) \tag{7}$$

where A is considered as the coefficient of signal detection.

If received signal $u_1(t)$ does not contain signal $s_1(t)$, but noise $n_1(t)$, detection coefficient has value of A = 0. The previous event is considered as A0. If received signal $u_1(t)$ contains both signal $s_1(t)$ and noise $n_1(t)$, than A=1 and the event is considered as A1. The noise at the input of the sensor affects the decision if the echoed signal from the object is present: B0 - signal $s_1(t)$is not present in received signal $u_1(t)$, B1 - received signal $u_1(t)$ contains signal $s_1(t)$.

where B is considered as the coefficient of decision.

Based on the previous, decision process can results in the following four situations:

A0B0 – true negative,
A0B1 – false positive,
A1B0 – false negative (signal is lost),
A1B1 – true positive (signal is detected).

In general, probability of the true positive detection is expressed by the following:

$$P_D = \frac{target\ detection}{the\ sum\ of\ all\ states} \tag{8}$$

Formula (8) is valid in case, when the object is detected by one sensor. Our case considers one composite probability of detection from several sensors. We can assume, that we have *i* sensors in operation area and A_1, A_2,...,A_n are independent events, which are considered as a target detections from each sensor and also that all sensors would follow just one target. For the final probability of the target detection stands:

$$P(\bigcup_{n=1}^{n} A_i) = 1 - P\left(\overline{\bigcup_{n=1}^{n} A_i}\right) = 1 - P\left(\overline{A_1}\right).P\left(\overline{A_2}\right)...P\left(\overline{A_n}\right) \tag{9}$$

where:

P... is Probability of detection.

Optimization criteria which ensure that the requirement of maximizing the probability of detection may have different bases. There are several detection rules designed of in theory of radio-location:

- Minimum Average Error Probability Detection rule,
- Neyman-Pearson detection rule,
- Maximum `a Posteriori Detection Rule,
- The Maximum Likelihood Detection Rule.

The detection rules selection is based on particular issue and input parameters. The main task of the correct selection of the rule is to maximize the probability of target detection.

Optimal decision-making algorithm

Based on maximum `a Posteriori Detection Rule, optimal decision-making algorithm can be express as [11]:

$$\Lambda(u_1) = \frac{p_{sn}(u_1)}{p_n(u_1)} \geq \Lambda_0 \tag{10}$$

then u1(t) contains s1(t),

$$\Lambda(u_1) = \frac{p_{sn}(u_1)}{p_n(u_1)} < \Lambda_0 \tag{11}$$

then u1(t) doesn't contain s1(t)

where:

$\Lambda(u_1)$ …. is the probability factor,
Λ_0 …. is the threshold value of the probability factor,
$p_{sn}(u_1)$ …. is the probability density distribution of signal with noise,
$p_n(u_1)$ …. is the probability density distribution of noise signal.

We assume that probability density distribution of noise signal has normal curve and because we exactly know echoed signal $s_1(t)$, then optimal algorithm is:

$$\Lambda(u_1) = R_v(0) = \int_0^T u_1(t)s_1(t)dt \geq \left(\frac{N_0}{2}\right) ln\,\Lambda_0 - \frac{E_1}{2} = U_0 \tag{12}$$

where:
$R_v(0) = \int_0^T u_1(t)s_1(t)dt$ … is correlation function
N_0 ... is density distribution of noise signal,
E_1 … is energy of echoed signal,
T … is integration time,
U_0 … is threshold voltage value.

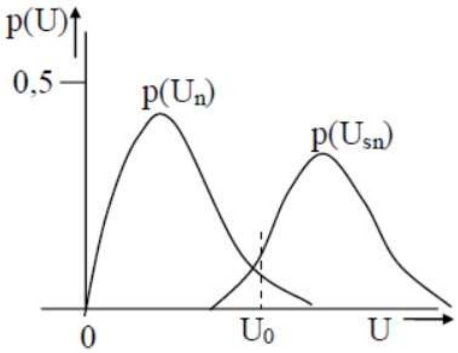


Fig. 6 The probability density distribution of signal with noise p(U_{sn}) and only noise p(U_n)

6 CONCLUSION

An estimate of the target position is difficult process, which is influenced by several input values, e.g. distance between sensor and the target and the distance between each pair of sensors in case of sensor network installed.

In this paper we were dealing with the optimization strategy of sensors and the target dislocation. Both sensors and target were dislocated in 3D area on the sphere surface and target was situated right in the middle.

The previous simulation validates our mathematical assumptions regarding the optimal sensor network dislocation in 3D while achieving the most accurate estimation of the target. The minimum time requirement condition for initial UAV configuration change to the optimal was also met.

The main goal of the previous mathematical study is to determine the appropriate mathematical model, based on which we will be able to define the dependency of the final information entropy from the current sensor's matrix dislocation.

To determine the final value of the information entropy, it is necessary to express the information about the probability of the detection in each individual time slot for current sensors matrix.

The overall probability expressing the state of predicted position will rely on declination between recent and optimal dislocation of the sensors. The value of the probability will be influenced by the probability of the reliability (the factor of reliability), expressed by the formula (5), and the probability of the detection capability, which is the parameter usually defined by the constructor and listed in the data sheet of the localization device. The resultant probability will be the primary input parameter to determine the information entropy. The reason to implement the information entropy is to determine the limited - threshold value in situation when the commander's knowledge exceeds the capability to act.

The previous approach allows to define both positive and negative effects of the network complexity and cooperation based on Shannon's entropy used as the knowledge measure. The model can be applied also during quantification of the cooperation benefits in the whole information network NEC.

References

[1] RINDZÁK, P.: Optimal sensor dislocation for target localization in 2D and 3D area. In *Science & Military 1/2017.* Liptovský Mikuláš : Armed Forces Academy.

[2] CARTER, G. C. Ed.: Special issue on time delay estimation. In *IEEE Trans*. Acoust, Speech, Signal Processing, vol. 29, June 1981.

[3] CARTER, G. C. Ed. *Coherence and Time Delay Estimation*, IEEE Press, 1993.

[4] TORRIERI, D. J. Statistical theory of passive location systems. In *IEEE Trans*. Aerosp. Electron. Syst.., vol. 20, p.183-197, 1984

[5] SPIRITO, M. A. On the accuracy of cellular mobile station location estimation. In *IEEE Trans. Veh. Technol*., vol.50, p. 674-685, 2001.

[6] YANG, B., SCHEUING, J. Cramer-Rao bound and optimum sensor array for source localization from TDOA. *In IEEE ICASSP*, 2005, vol.4, p. 961-964.

[7] YANG, B. Different sensor placement strategies for TDOA based localization. In *Proceedings of the 2007 IEEE International Conference on Acoustics*, *Speech, and Signal Processing,* vol. 2, pp. II–1093–II–1096, Apr. 2007.

[8] BISHOP, A. N. Optimality analysis of sensor-target geometries in passive localization. In *Conference of Intelligent sensors*, Melbourne, Australia, 2007.

[9] ISAACS, J. T., KLEIN, D. J., HESPANHA, J. P. Optimal sensor placement for time difference of arrival localization. In *Proceedings of the 48th Conference on Decision and Control* (pp. 7878–7884). Shanghai, China.

[10] SLOANE, N. J. A., HARDIN, R. H., SMITH, W. D. *Spherical codes.* Available at: http://www.research.att.com/njas/packings/.

[11] OCHODNICKÝ, J.: *Rádiolokácia a navigácia.* Súbor prednášok z predmetu. Liptovský Mikuláš : Akadémia ozbrojených síl, 2017.

[12] ZHAO, S., CHEN, B. M., LEE, T. H. Optimal deployment of mobile sensors for target tracking in 2D and 3D spaces. In *Acta Automatica Sinica,* 2014, 1(1): 50−56.

[13] IEEE Trans. Aerospace and Electron. Systems, „Statistical theory of passive location systems“, vol. 20, p.183-198.

[14] FARINA, A., STUDER, F. A. *Radar data processing*. Hertfordshire, UK, 1985.

[15] REN, W., CAO, Y. C. *Distributed Coordination of Multi-agent Networks*. New York : Springer, 2011.

[16] OUSINGSAWAT, J., CAMPBELL, M. E. Optimal Cooperative reconnaissance using multiple vehicles. In *Journal of Guidance*, Control and Dynamics, 2007 p.122-132

[17] HU, J. W., XU, J., XIE, L. H. *Cooperative search and exploration in robotic networks.* "Unmanned systems", 2013 p. 121-142.

[18] SHANNON, C. E., WEAVER W. *The mathematical theory of communication.* University of Illinois Press, 1949.

[19] WOODWARD, P. M. *Probability and information theory with applications to radar.* Pitman press, London, 1957.

[20] PACE, P. E. *Detecting and Classifying Low Probability of Intercept Radar*. London : Artech house, 2009.

[21] WOODWARD, P. Information and Probability Theory, with Applications to Radar. Artech house, London, 1980

Eng. Peter RINDZÁK
Ministry of Defence of the Slovak Republic
Kutuzovova 8
832 47 Bratislava
Slovak Republic
E-mail: peter.rindzak@gmail.com

Eng. Peter Rindzák - was born in Humenné, Slovakia in 1983. He received his M.Sc. (Ing.) at the Academy of the Armed Forces of general Milan Rastislav Štefánik in Liptovský Mikuláš. His is research interests are modeling, simulation, measurement, optimal deployment of sensor arrays and information entropy.

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.

1 INTRODUCTION

Automatic event log collection and analysis allows SIEM - Security information and event management to detect security threats in corporate networks. The choice of generated event logs significantly affects the quality of security threat detection and therefore requires detailed knowledge of the monitored system and its configuration. In this article, we focused on Windows 10 workstations and Windows 2016 server that are used in the computer lab to teach programming and operating systems. We analyzed system default settings, applied the recommended security settings and we have modified them. Based on the experimentally obtained data from individual stages of measurement, we designed filters to reduce unnecessary data and reduce the SIEM load.

The experiment took place in several phases. In the first phase, event logs were obtained from one workstation in the initial security configuration. A standard event viewer was used to analyze the count and types of event logs. In the second phase, security settings recommended by the manufacturer were used [1]. Microsoft Security Compliance Manager (SCM) tool contains security templates for current versions of operating systems and selected program packages. For the purpose of the experiment, we used the Windows 10-1607 Computer Security Compliance 1.0 template that contains 765 unique settings and WS2016 Domain Controller Security Compliance 1.0 that contains 1013 unique settings. A significant increase in quantity and variety of events has been recorded and therefore we have used the Event Log Explorer for analysis [2]. This tool enables efficient consolidation, analysis and filtering of event logs. Captured event logs were analyzed and followed by a final adjustment of security settings. The security parameters were set based on our own experience, taken into account published recommendations [3-5]. The content of logs has been analyzed and we have proposed rules for later filtering. In the third phase, the security settings were used on computers in the computer lab and event logs collected on the log server. The log server was configured on Windows 2012 R2 using the published procedure - [6]. The log server filtered the collected data and prepared them for processing in SIEM – Fig.1.

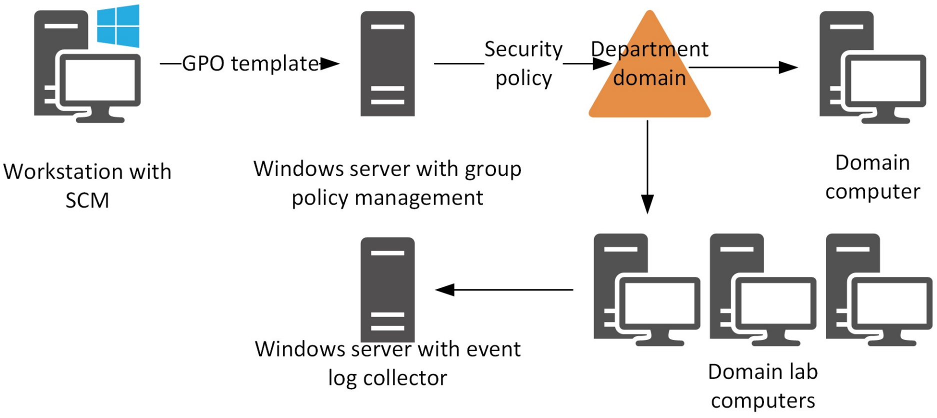


Fig. 1 Topology of experiment

2 TOOLS USED

An important role in the experiment was to work with the security settings of the operating system. The Windows Defender Security Center introduced in Windows 10 creators update includes five pillars:

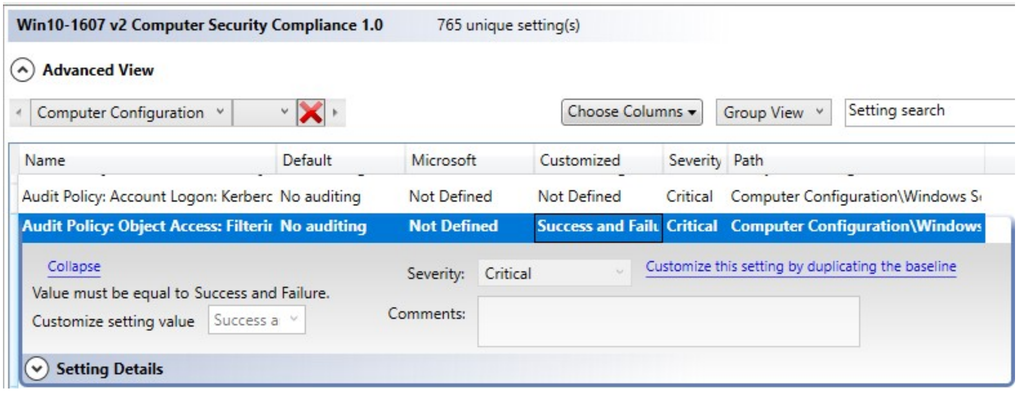
- virus & threat protection,
- device performance & health,
- firewall & network protection,
- app & browser control,
- family options.

That gives user control and visibility of the device security, health and online safety experiences [7]. However, it is not clear how the message generation is set for logging. For sophisticated Windows 10 EDU settings, the Local Security Policy Editor is available. This editor allows you to change the security settings of your local computer in detail, but it is not possible to track the changes you make, and the changes can be overridden by the group policies. The solution was to use Microsoft SCM [1] to create and manage security templates. Template settings – Tab. 1 can be exported and used in a global security policy applied to the domain members.

Tab. 1 List of baselines applicable to windows 10

Baseline name	Unique settings
BitLocker Security	40
Computer Security Compliance	765
Credential Guard Security	2
Domain Security Compliance	9
User Security Compliance	198
IE10 Computer Security Compliance	147
IE10 User Security Compliance	5
Office2013 Computer Security	27
Office2013 User Security	720

In the experiment, we focused on the Computer Security Compliance template, which contains 21 settings groups. An example of a modification of the parameter in the security policy is in Fig. 2.



Win10-1607 v2 Computer Security Compliance 1.0 765 unique setting(s)

Advanced View

Name	Default	Microsoft	Customized	Severity	Path
Audit Policy: Account Logon: Kerberc	No auditing	Not Defined	Not Defined	Critical	Computer Configuration\Windows S
Audit Policy: Object Access: Filterii	No auditing	Not Defined	Success and Failu	Critical	Computer Configuration\Windows

Collapse

Value must be equal to Success and Failure.

Customize setting value: Success a

Severity: Critical

Customize this setting by duplicating the baseline

Comments:

Setting Details

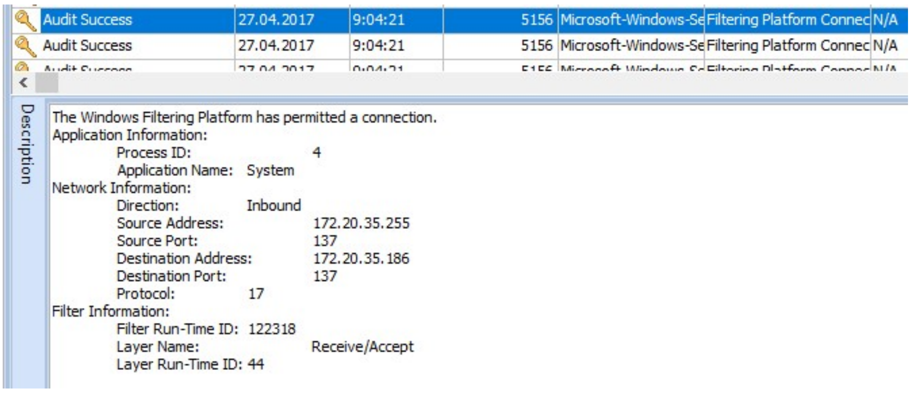
Fig. 2 Modification of the parameter in the security policy

An event log explorer was used to analyze obtained logs. Event Log Explorer is an effective software solution for viewing, analyzing and monitoring events recorded in Microsoft Windows event logs. Event Log Explorer greatly simplifies and speeds up the analysis of event logs (security, application, system, setup, directory service, DNS and others). Event Log Explorer extends the standard Windows Event Viewer functionality and brings many new features. Users, who tried Event Log Explorer, see it as a superior solution to Windows Event Viewer helping to boost their productivity twice [2]. The selected benefits of event log explorer include:

- instant access to event logs,
- efficient filtering,
- event log consolidation,
- export events and report generator,
- advanced filtering by any criteria including event description text,
- analytical reports - summary tables and pivot charts,
- servers import etc.

Example of event viewing in event log explorer is in Fig. 3.

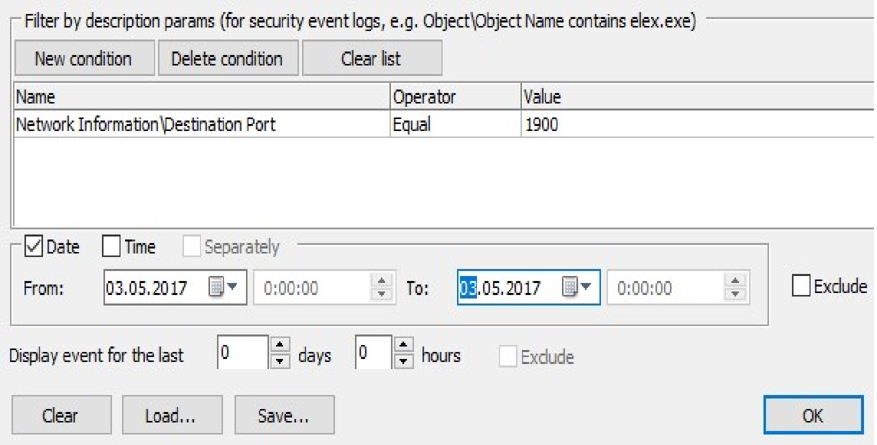
Since the analysis of the logs structure plays an important role in the experiments, we used the log file filtering option as shown in Fig. 4.



```
Audit Success   27.04.2017   9:04:21   5156 Microsoft-Windows-Se Filtering Platform Connec N/A
Audit Success   27.04.2017   9:04:21   5156 Microsoft-Windows-Se Filtering Platform Connec N/A
Audit Success   27.04.2017   9:04:21   5156 Microsoft-Windows-Se Filtering Platform Connec N/A
```

```
The Windows Filtering Platform has permitted a connection.
Application Information:
        Process ID:             4
        Application Name:   System
Network Information:
        Direction:          Inbound
        Source Address:         172.20.35.255
        Source Port:            137
        Destination Address:    172.20.35.186
        Destination Port:       137
        Protocol:           17
Filter Information:
        Filter Run-Time ID:  122318
        Layer Name:             Receive/Accept
        Layer Run-Time ID: 44
```

Fig. 3 Event detail view



Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

Name	Operator	Value
Network Information\Destination Port	Equal	1900

☑ Date ☐ Time ☐ Separately

From: 03.05.2017 0:00:00 To: 03.05.2017 0:00:00 ☐ Exclude

Display event for the last 0 days 0 hours ☐ Exclude

Fig. 4 Manual log file filtering

3 WORKSTATION EXPERIMENTAL RESULTS

The aim of the first phase of the experiment was to determine the starting point, the second phase reflects the manufacturer's recommendations and the continuation of the second phase reflects the results of our optimization. The measured values show the number of event types and the number of evets recorded per computer and 8 working hours – Tab. 2.

Tab. 2 Types and number of events in Phases 1 and 2

	Phase 1	Phase 2	Optimized phase 2
Event types	14	73	40
Event count	4839	230046	188531

Audit settings in the default operating system setup has proven to be inadequate for our needs and generated Event IDs were not enough to detect current security threats. In phase 2, we changed audit parameters using Windows 10-1607 Computer Security Compliance 1.0 template that contained 765 parameters, one parameter influencing the generation of one or more Event IDs. Audit parameters were of defined importance, with 202 being critical, 97 important, 39 optional, and others undefined. The types and quantity of generated events increased significantly – Tab. 1. Based on an in-depth analysis of the settings, taken into account the latest published recommendations in Windows security, we have defined and applied new settings in optimized phase 2. The number of audit settings changes for each phase of the experiment is listed in Tab. 3. The total number of event types and event counts decreased, which was an expected and positive result.

Tab. 3 Number of changes to the audit settings

	Phase 2 vs Phase 1	Optimized phase 2 vs Phase 2
Number of changes	140	29

Optimized Phase 2 contained 40 event types, with 85 percent events being Event ID: 5154, 5156, and 5158 – Fig. 5.

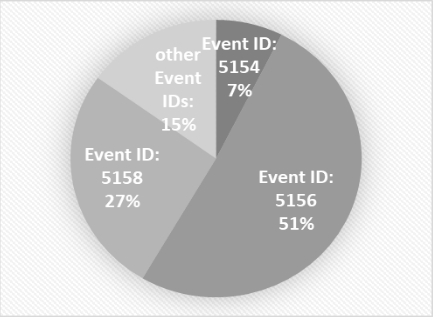


Fig. 5 Optimized Phase 2 Event ID types

For a further reduction of processed events, we analyzed the content of the most abundant Event IDs. Event ID 5156 generates a record whenever the Windows Filtering Platform (WFP) allows a program to connect to another process locally or remotely. Event ID 5158 generates a record whenever a client or server application binds to a port. Event ID 5154 generates and records whenever WFP allows an application or service to listen on a port for incoming connections. The event IDs mentioned above indicate the network communication of the operating system and running applications and can greatly improve detection of security threats. The next task was to filter unnecessary records. We analyzed the content of the most numerous Event IDs for filtering purposes. The Event ID 5156 record structure is shown in Fig. 6.

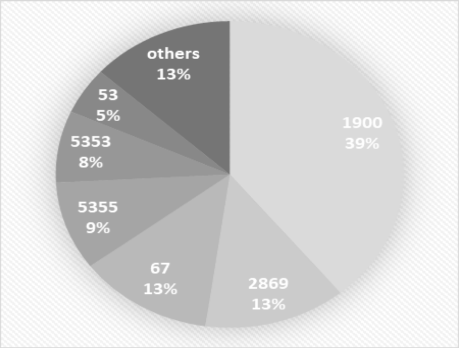


Fig. 6 Event ID 5156 record structure by transport layer address

Simple Service Discovery Protocol (SSDP) discovery of UPnP devices represented by ports 1900 and 2869 generates 52 percent of messages, followed by DHCP protocol - port 67 with 13 percent of messages. SSDP Discovery service is required for UPnP and Media Center Extender, and if we do not use UPnP, the service can be disabled and messages can be filtered. DHCP messages are unusable for analysis because they do not contain link layer address information, and these messages can also be filtered. Filtering the mentioned messages reduces the number of Event ID 5156 records by 65 percent. Similarly, the structure of the Event ID 5158 records was analyzed, where 24 percent of the records could be filtered. Event ID 5154 was left unchanged after the analysis, and we did not perform filtering. In Phase 3 we applied settings from optimized Phase 2 without filtering. In the lab, 15 computers were used for teaching 4 lessons (from 08:00 AM to 11:15 AM). For more than 3 hours, 3.1 million records were recorded, with 59 percent being Event ID 5156 and 12 percent Event ID 5158.

The log file size in just over 3 hours has grown to 10GiB. After applying the filtering to input data, there was a reduction of 41 percent of the total number of records to the final 1.8 million.

4 SERVER EXPERIMENTAL RESULTS

The same methodology was used for windows 2016 server testing as for the windows 10 workstation. The Windows 2016 server served as a domain controller, DNS, and DHCP server. The aim of the first phase (Phase 1) of the experiment was to determine the starting point – default settings, the second phase (Phase 2) reflects the manufacturer's recommendations and the continuation of the second phase (Phase 3) reflects the results of our optimization. Since the domain controller security requirements are different from the workstation, the final step (Phase 4) was to align WFP settings to compare the results. The measured values show the number of event types and the number of evets recorded from the server for 8 working hours – Tab. 4.

Tab. 4 Types and number of events in Phases 1 to 4

	Phase 1	Phase 2	Phase 3	Phase 4
Event types	20	13	16	29
Event count	8893	9035	11857	100710

Audit settings in the default operating system setup has proven to be inadequate for our needs and generated Event IDs were not enough to detect current security threats. In phase 2, we changed audit parameters using WS2016 Domain Controller Security Compliance 1.0 template that contained 1013 parameters, one parameter influencing the generation of one or more Event IDs.

The number of audit settings changes for each phase of the experiment is listed in Tab. 5. The total number of event types and event counts increased, which was an expected and positive result.

Tab. 5 Number of changes to the audit settings

	Phase 2 vs Phase 1	Phase 3 vs Phase 2	Phase 4 vs Phase 3
Number of changes	923	11	24

Phase 4 contained 29 event types, with 80 percent events being Event ID: 5156 – Fig. 7.

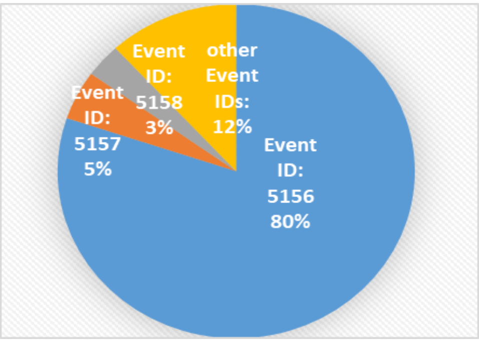


Fig. 7 Optimized Phase 2 Event ID types

As in the case of the workstation, a large number of events number 5156 were generated. Their composition is different, as 82 % of the records belong to name resolution activities - ports 53,137 and 5355.

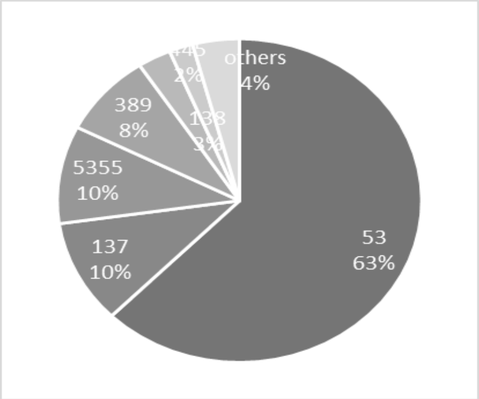


Fig. 6 Window server Event ID 5156 record structure by transport layer address

If we compare phase 4 - windows server and the optimized workstation phase 2, we find that the number of events generated by the server is reasonable. The event structure does not allow significant filtering without loss of relevant data and was therefore omitted in the experiment.

5 CONCLUSION

In the article, we focused on selecting and optimizing the Event logs of the Windows 10 and Windows 2016 server operating systems for the purpose of detecting security threats. We optimized the choice of Event ID with focus on network communication.

Windows workstation optimization has been the reduction of event types from 73 to 40 in phase 2. Then we analyzed the structure of the most massive Event IDs and designed filters to remove unnecessary messages. The proposed solution was experimentally verified on the normal operation of 15 laboratory computers during the course. Using filters, we reduced the number of messages by 41 percent. Taking real-time deployment needs into more than 200 computers working 8 hours a day, this is a significant reduction in disk space and computer performance needed to analyze records.

By changing the recommended settings in phase 4 of the windows 2016 server, we have generated the required event IDs and their further filtering has not made any significant changes.

Although Windows 10 and Windows Server 2016 use the same kernel, the recommended security templates are different to take into account different usage scenarios. Therefore, an individual approach has to be used to optimize generated events.

References

[1] *Security compliance manager* 2006, Microsoft Corporation.

[2] *Event log explorer*. 2016, FSPro Labs.

[3] *Advanced security audit policy settings*. Windows IP Center 2017. Available from: https://docs.microsoft.com/sk-sk/windows/device-security/auditing/advanced-security-audit-policy-settings.

[4] *Audit policy recommendations*. 2016 [cited 2017] Available from: https://docs.microsoft.com/sk-sk/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations.

[5] *windows-itpro-docs/windows/keep-secure/*. 2016 [cited 2016] Available from: https://github.com/Microsoft/windows-itpro-docs/tree/master/windows/keep-secure.

[6] A. Costea. *How to configure Windows event log forwarding*. 2016 [cited 2017]; Available from: http://www.vkernel.ro/blog/how-to-configure-windows-event-log-forwarding.

[7] R. Lefferts. *Introducing Windows Defender Security Center*. 2017 [cited 2017]; Available from: https://blogs.windows.com/windowsexperience/2017/01/23/introducing-windows-defender-security-center/#7kDTFztBkgBvOzdU.97.

Eng. Július BARÁTH, PhD.
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: julius.barath@aos.sk

Eng. Július Baráth, PhD. - graduated Military Technical University in 1991, received PhD in 1996 and works 19 years as a senior assistant at the Department of Informatics, Armed Forces Academy, Liptovský Mikuláš, Slovakia. His professional interests include computer networks, operating systems and computer security.

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.

1 INTRODUCTION

Last year, over 2,100 enterprises were breached as a result of poor internal security practices and latent vendor content security. The average cost of a corporate security breach is estimated at $3.5 million USD and is rising at 15 % year over year. Intrusions, malware/botnets and malicious applications collectively comprise a massive risk to your enterprise network. These attack mechanisms can give attackers access to our most sensitive files and database information.

The goal of this report was to conduct a survey in the real environment, which consist of education and executive parts. Inspected network is divided into subnets with its unique numbers. This document provides the findings of a recent analysis of company infrastructure. The document represents a summary of these findings and presents a set of proposed recommendations for addressing the detected events. The analysis is based on data collected using the characteristics below:

- network analysed: Internal LAN,
- functions enabled: Antivirus, App Control, IPS, Traffic, Web,
- test duration: 8 day(s).

The network was monitored with a device in Transparent Mode. This is a non-invasive way to intercept traffic as it moves over the network.

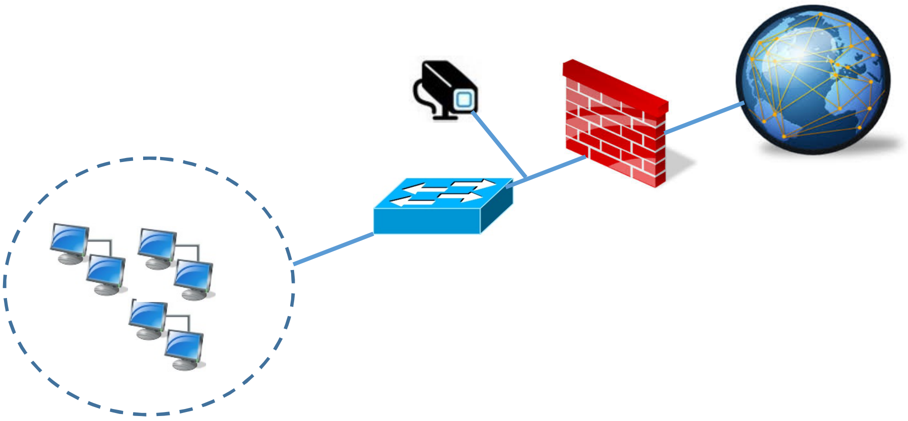


Fig. 1 Block diagram of connection in transparent mode

During the assessment, network activity was monitored as it passed through the infrastructure. While traffic logs record much of the session information flowing across the network, security device can also monitor more in-depth security logging such as IPS, anti-virus, web and application control. This assessment was created based on telemetry from all log types and provides an overview of the monitored network's activity.

User application usage and browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate a lack of proper enforcement of corporate usage policies. Most enterprises recognize that personal use of corporate resources is acceptable. But there are many grey areas that organisation must keep a close eye on including: use of proxy avoidance/peer to peer applications, inappropriate web browsing, phishing websites, and potentially illegal activity - all of which expose the company to undue liability and potential damages.

Performance effectiveness is an often undervalued aspect of security devices, but firewalls must keep up with the line speeds that today's next generation switches operate at. A recent survey by Infonetics indicates that 77 % of decision-makers at large organizations feel that they must upgrade their network security performance (100+ Gbps aggregate throughput) in the coming year.

The survey was aimed to detection of:

- IPS Attacks,
- High-Risk Applications Used,
- Malicious Websites,
- Applications,
- Top Used Application,
- Top Application Category.

2 SUMMARY OF THE ANALYSIS

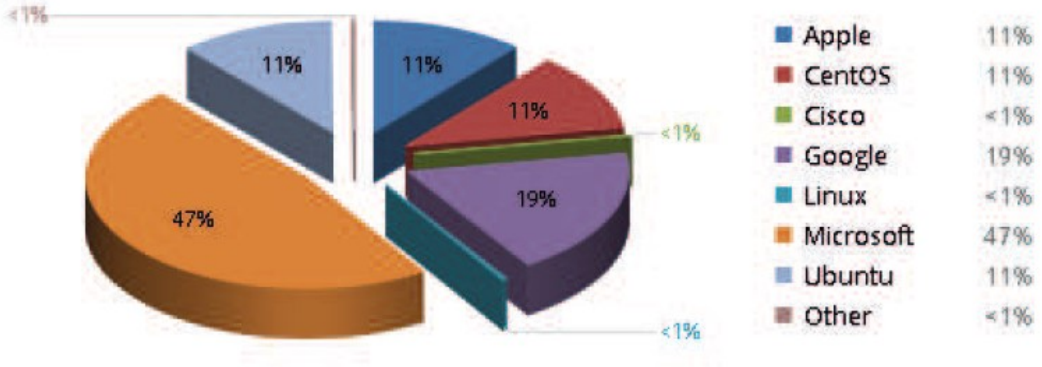


Fig. 2 The operating systems on analysed network

Amount of monitored total bandwidth was 1.50 TB.

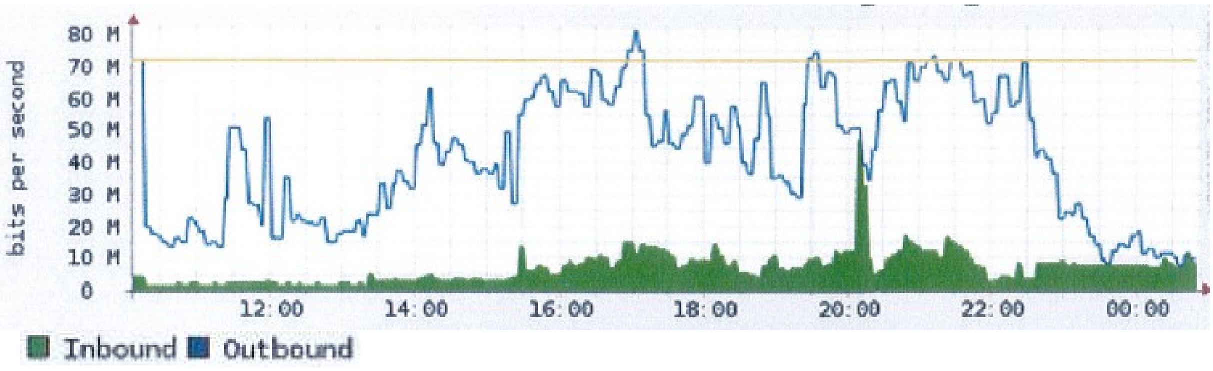


Fig. 3 Example of monitored bandwidth for 12 hours

Malware types

Malware exposes different types of risk to the organisation that encounters it. Malware is commonly categorized into different types. Below are different types of malware.

Tab. 1 Types of malware

Malware type	Description
Botnet client	A botnet is a collection of computers controlled by a third party. Hosts controlled by a botnet may steal information from an organisation or be used to launch denial-of-service attacks, send spam or conduct other undesirable activity.
Trojan / Backdoor	A Trojan horse is a program that appears to be benign to an end user but in fact is malicious. It can be used to steal information or introduce control.
Spyware	Spyware is a software installed on machines that collects information without user´s knowledge and forwards it to others.

Files moving around the network

The following files types have been seen moving around the monitored network.

Downloads

File Category	File type	Protocol	Count
Multimedia	M3U	HTTP	83,709
Archive	MSCAB	HTTP	82,028
Archive	RAR	HTTP	9,515
Archive	GZ	HTTP	7,793
Multimedia	SWF	HTTP	4,720

Uploads

File Category	File type	Protocol	Count
Archive	GZ	HTTP	729
Archive	ZIP	HTTP	82
Office Documents	MSOLE2	HTTP	34
System files	DMP	HTTP	18
PDF files	PDF	HTTP	12

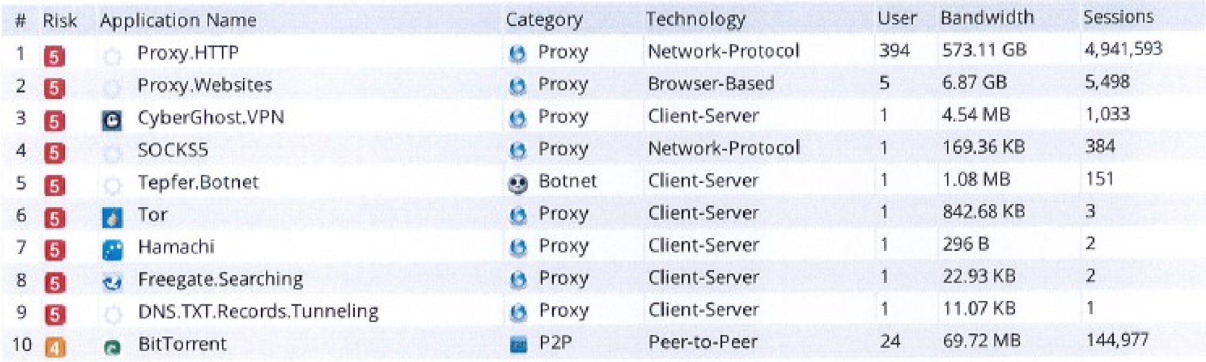
Misc

File Category	File type	Protocol	Count
PDF files	PDF	SMTP	88
Archive	ZIP	SMTP	32
Multimedia	MP4	SMTP	26
Multimedia	MOV	SMTP	24
PDF files	PDF	FTP Data	20

Fig. 4 File types moving around the network

High Risk Applications

The used technology assigns a risk rating of 1 to 5 to an application based on the application behavioral characteristics. The risk rating can help administrators to identify the high-risk applications quickly and make a better decision on the application control policy. Applications listed below were assigned a risk rating of 4 or higher.

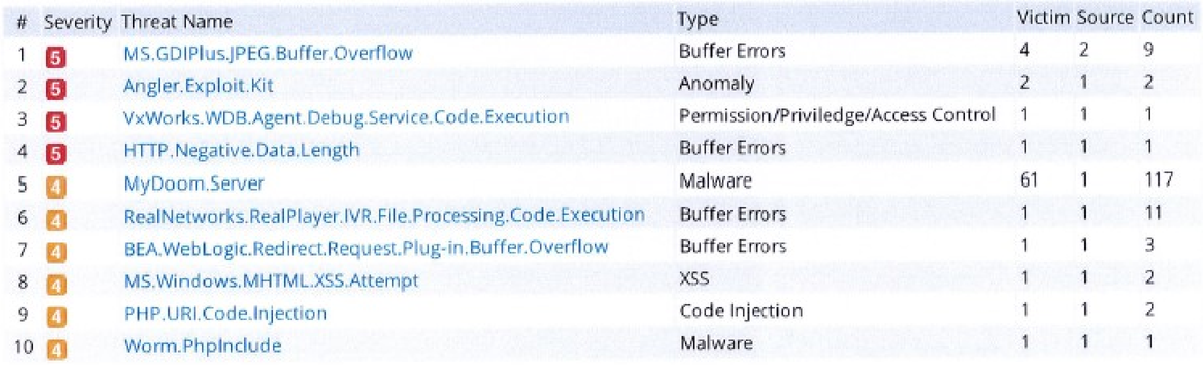


#	Risk	Application Name	Category	Technology	User	Bandwidth	Sessions
1	5	Proxy.HTTP	Proxy	Network-Protocol	394	573.11 GB	4,941,593
2	5	Proxy.Websites	Proxy	Browser-Based	5	6.87 GB	5,498
3	5	CyberGhost.VPN	Proxy	Client-Server	1	4.54 MB	1,033
4	5	SOCKS5	Proxy	Network-Protocol	1	169.36 KB	384
5	5	Tepfer.Botnet	Botnet	Client-Server	1	1.08 MB	151
6	5	Tor	Proxy	Client-Server	1	842.68 KB	3
7	5	Hamachi	Proxy	Client-Server	1	296 B	2
8	5	Freegate.Searching	Proxy	Client-Server	1	22.93 KB	2
9	5	DNS.TXT.Records.Tunneling	Proxy	Client-Server	1	11.07 KB	1
10	4	BitTorrent	P2P	Peer-to-Peer	24	69.72 MB	144,977

Fig. 5 Highest risk applications sorted by the risk and sessions

Application Vulnerability Exploits

The application vulnerabilities can be exploited to compromise the security of your network and evade traditional firewall systems.

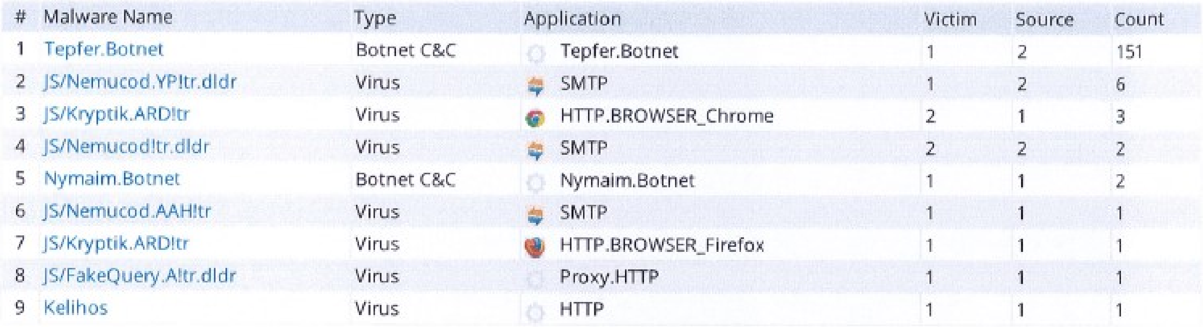


#	Severity	Threat Name	Type	Victim	Source	Count
1	5	MS.GDIPlus.JPEG.Buffer.Overflow	Buffer Errors	4	2	9
2	5	Angler.Exploit.Kit	Anomaly	2	1	2
3	5	VxWorks.WDB.Agent.Debug.Service.Code.Execution	Permission/Priviledge/Access Control	1	1	1
4	5	HTTP.Negative.Data.Length	Buffer Errors	1	1	1
5	4	MyDoom.Server	Malware	61	1	117
6	4	RealNetworks.RealPlayer.IVR.File.Processing.Code.Execution	Buffer Errors	1	1	11
7	4	BEA.WebLogic.Redirect.Request.Plug-in.Buffer.Overflow	Buffer Errors	1	1	3
8	4	MS.Windows.MHTML.XSS.Attempt	XSS	1	1	2
9	4	PHP.URI.Code.Injection	Code Injection	1	1	2
10	4	Worm.PhpInclude	Malware	1	1	1

Fig. 6 Top vulnerabilities identified, sorted by severity and count

Malware, Botnets and Spyware/Adware

There are numerous channels that cybercriminals use to distribute malware. Most common methods motivate users to open an infected file in an email attachment, download an infected file, or click on a link leading to a malicious site. During the security assessment, it was identified a number of malware and botnet-related events which indicate malicious file downloads or connections to botnet command and control sites.

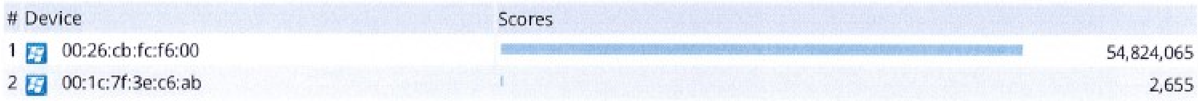


#	Malware Name	Type	Application	Victim	Source	Count
1	Tepfer.Botnet	Botnet C&C	Tepfer.Botnet	1	2	151
2	JS/Nemucod.YP!tr.dldr	Virus	SMTP	1	2	6
3	JS/Kryptik.ARD!tr	Virus	HTTP.BROWSER_Chrome	2	1	3
4	JS/Nemucod!tr.dldr	Virus	SMTP	2	2	2
5	Nymaim.Botnet	Botnet C&C	Nymaim.Botnet	1	1	2
6	JS/Nemucod.AAH!tr	Virus	SMTP	1	1	1
7	JS/Kryptik.ARD!tr	Virus	HTTP.BROWSER_Firefox	1	1	1
8	JS/FakeQuery.A!tr.dldr	Virus	Proxy.HTTP	1	1	1
9	Kelihos	Virus	HTTP	1	1	1

Fig. 7 Common Malware, Botnets, Spyware and Adware detected

At-risk devices and hosts

Based on the types of activity exhibited by an individual host, we can approximate the trustworthiness of each individual client. This client reputation is based on key factors such as websites browsed, applications used and inbound/outbound destinations utilized. Ultimately, we can create an overall threat score by looking at the aggregated activity used by each individual host. These devices should be audited for malware and intrusion susceptibility.



#	Device	Scores
1	00:26:cb:fc:f6:00	54,824,065
2	00:1c:7f:3e:c6:ab	2,655

Fig. 8 Most at-risk devices and hosts

Encrypted web traffic

From a security perspective, it's important to visualize how much of the web-based traffic is encrypted. Encrypted traffic poses very real challenges for enterprises who want to ensure that those same applications are not being used for malicious purposes, including data exfiltration. Ideally, the firewall can inspect encrypted traffic at high speeds - this is why performance and hardware offloading are key when evaluating a firewall.

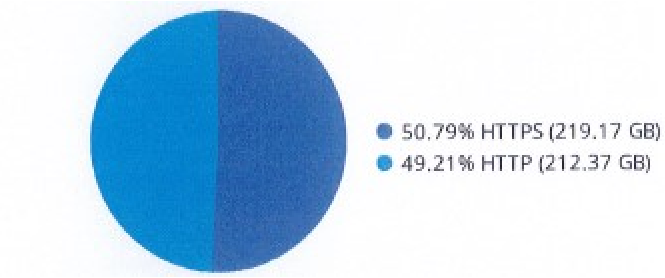
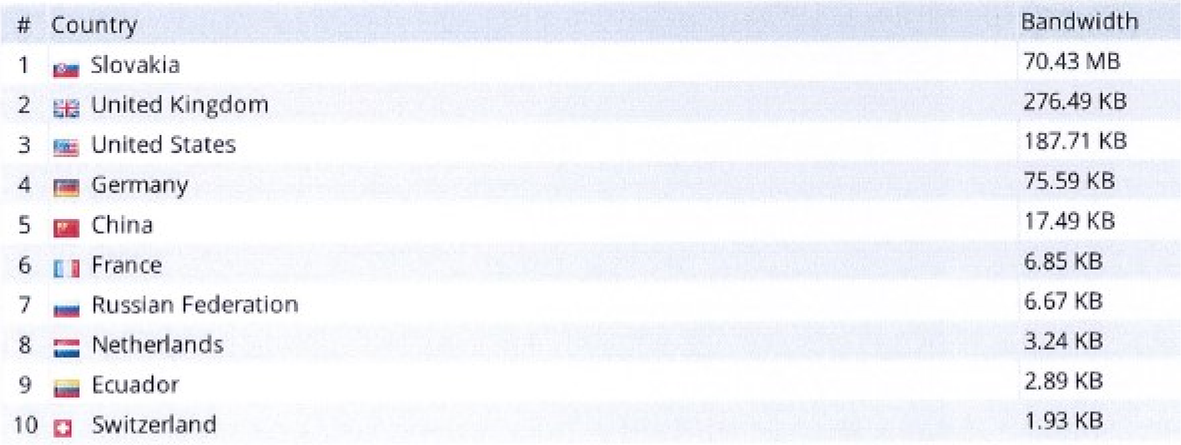


Fig. 9 HTTPS vs. HTTP traffic ratio

Top source countries

By looking at IP source traffic, we can determine the originating country of any particular request. Certain botnets, command and control functions, and even remote access can be session heavy and indicative of targeted attacks or persistent threats from nation-states. This chart is representative of country-based traffic - activity from specific originating nations may be anomalous and warrant further investigation. Activity originating from these countries should be audited for expected traffic sources.



#	Country	Bandwidth
1	Slovakia	70.43 MB
2	United Kingdom	276.49 KB
3	United States	187.71 KB
4	Germany	75.59 KB
5	China	17.49 KB
6	France	6.85 KB
7	Russian Federation	6.67 KB
8	Netherlands	3.24 KB
9	Ecuador	2.89 KB
10	Switzerland	1.93 KB

Fig. 10 Top source countries

User productivity application usage

The applications were categorizes into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow better application control [2].

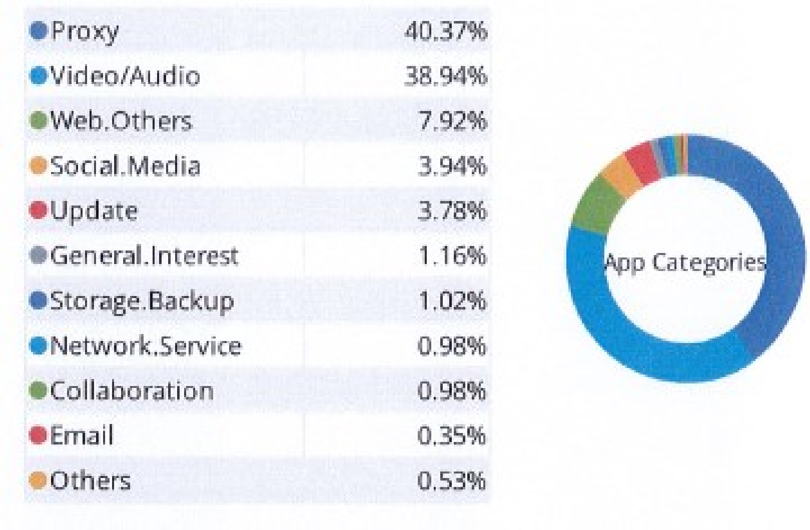


Fig. 11 The application usage

Cloud Usage

With the proliferation of cloud-based computing, enterprises are increasingly reliant on third parties for infrastructure plumbing. This means that their information is only as secure as the cloud provider's security. In addition, it can often introduce redundancy (if services are already available internally) and increase costs (if not monitored properly).

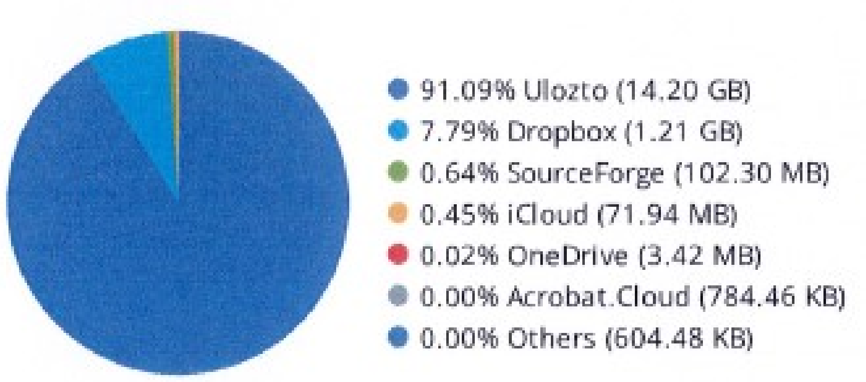


Fig. 12 The Cloud usage

Application category breakdowns

Understanding application subcategories can give invaluable insights into how efficiently corporate network is operating. Certain application types (such as P2P or gaming applications) are not necessarily conducive to corporate environments and can be blocked or limited in their scope. Other applications may have dual purpose uses (such as video/audio streaming or social media apps) and can be managed accordingly.

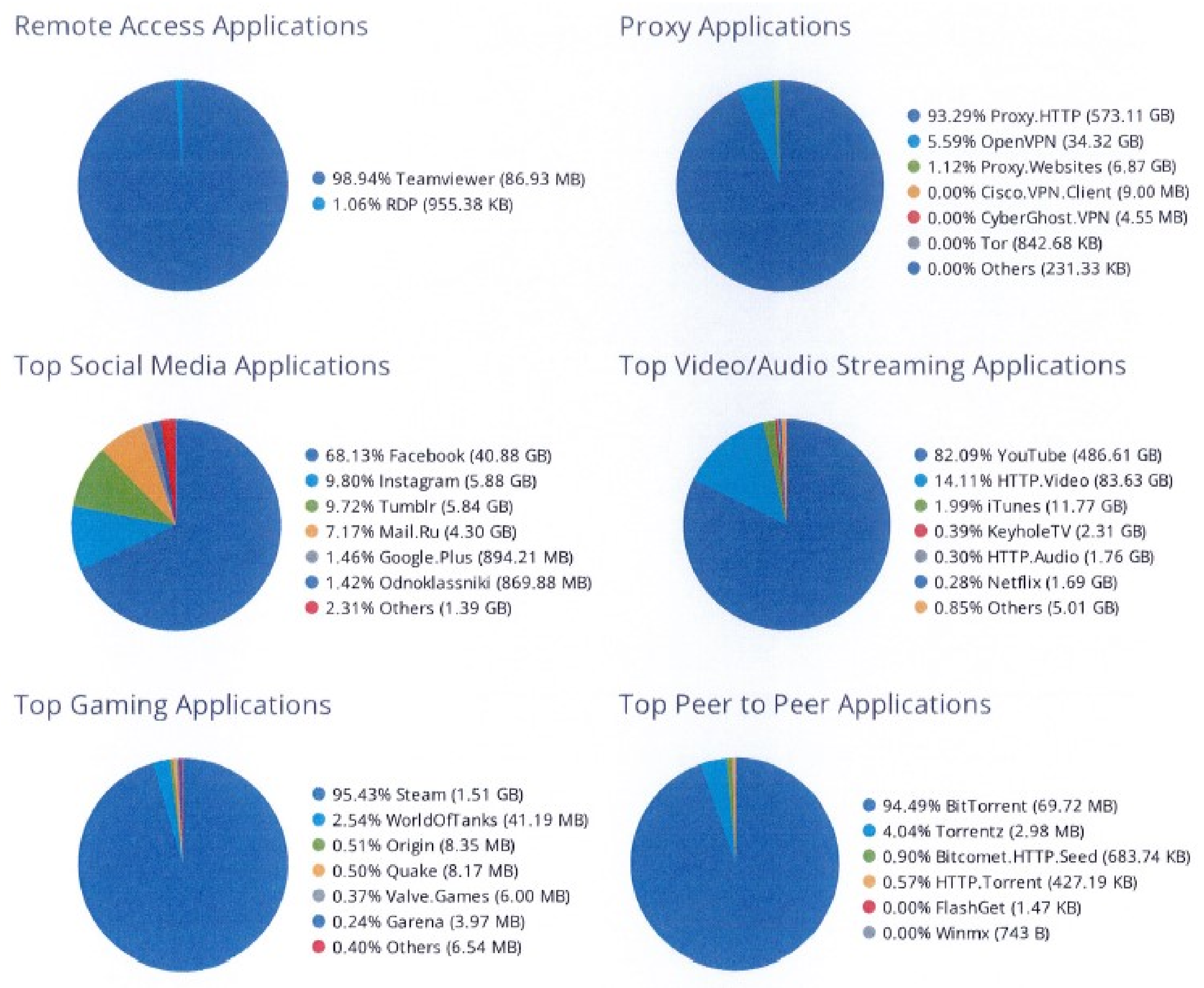
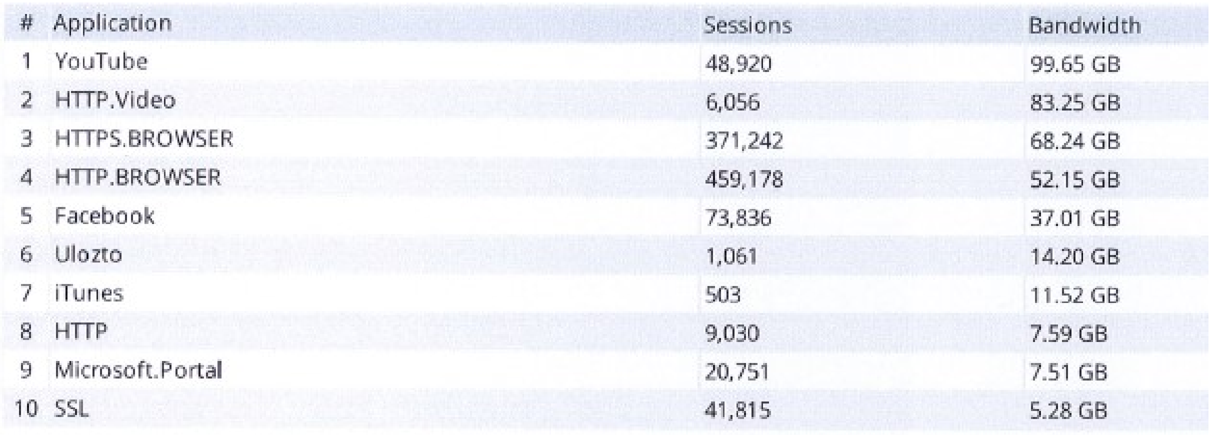


Fig. 13 Application categories sorted by the amount of bandwidth they used during the discovery period

Web Usage

In today's network environments, many applications leverage HTTP for communications. The primary benefit of HTTP is that communication is ubiquitous, universally accepted and (generally) open on most firewalls. For most business-related and whitelisted applications this typically augments communication, but some non-business applications also use HTTP in either unproductive or potentially nefarious ways.

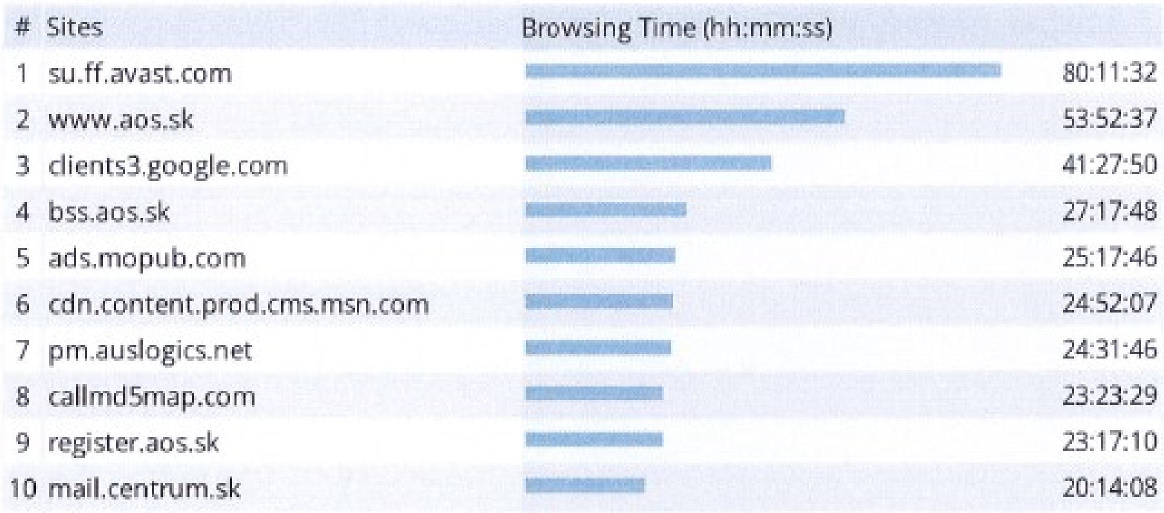


#	Application	Sessions	Bandwidth
1	YouTube	48,920	99.65 GB
2	HTTP.Video	6,056	83.25 GB
3	HTTPS.BROWSER	371,242	68.24 GB
4	HTTP.BROWSER	459,178	52.15 GB
5	Facebook	73,836	37.01 GB
6	Ulozto	1,061	14.20 GB
7	iTunes	503	11.52 GB
8	HTTP	9,030	7.59 GB
9	Microsoft.Portal	20,751	7.51 GB
10	SSL	41,815	5.28 GB

Fig. 14 Top web applications

Websites frequented

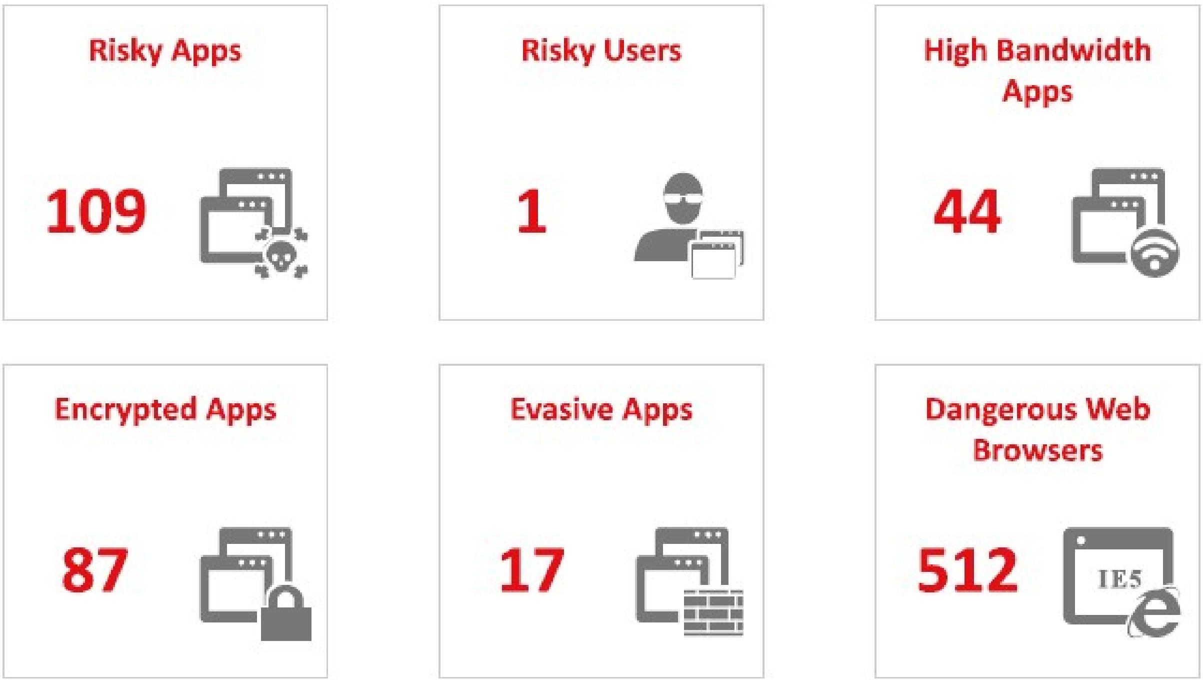
Estimated browsing times for individual websites can be useful when trying to get an accurate picture of popular websites. Typically, these represent internal web resources such as intranets, but they can occasionally be indicative of excessive behaviour. Browse times can be employed to justify the implementation of web caching technologies or help shape organizational corporate use policies.



#	Sites	Browsing Time (hh:mm:ss)
1	su.ff.avast.com	80:11:32
2	www.aos.sk	53:52:37
3	clients3.google.com	41:27:50
4	bss.aos.sk	27:17:48
5	ads.mopub.com	25:17:46
6	cdn.content.prod.cms.msn.com	24:52:07
7	pm.auslogics.net	24:31:46
8	callmd5map.com	23:23:29
9	register.aos.sk	23:17:10
10	mail.centrum.sk	20:14:08

Fig. 15 Top websites by browsing time

Executive summary



Risky Apps 109

Risky Users 1

High Bandwidth Apps 44

Encrypted Apps 87

Evasive Apps 17

Dangerous Web Browsers 512

Fig. 16 Network risk executive summary

The following attacks are very important to investigate because they directly target machines that have been identified as potentially vulnerable. The target machine's operating system version, running services, and potential vulnerabilities all match what the threat is designed to attack.

EVEN TYPE	DETAILS	POTENTIALLY VULNERABLE HOSTS
A Network Trojan was Detected	BLACKLIST DNS request for known malware domain megabrowse.biz-Win. Trojan.Mudrop (1:30833:2)	17
A Network Trojan was Detected	BLACKLIST DNS request for known malware domain counter.yadro.ru (1:29119:1)	9
A Network Trojan was Detected	APP-DETECT DNS request for potential malware SafeGuard to domain 360safe.com (1:28070:1)	7
A Network Trojan was Detected	MALWARE-CNC Win.Trojan.Necurs variant outbound connection (1:31243:1)	7
A Network Trojan was Detected	BLACKLIST DNS reverse lookup response for known malware domain spheral.ru-Win.Trojan.Glupteba (1:31600:1)	5

Fig. 17 High impact attacks

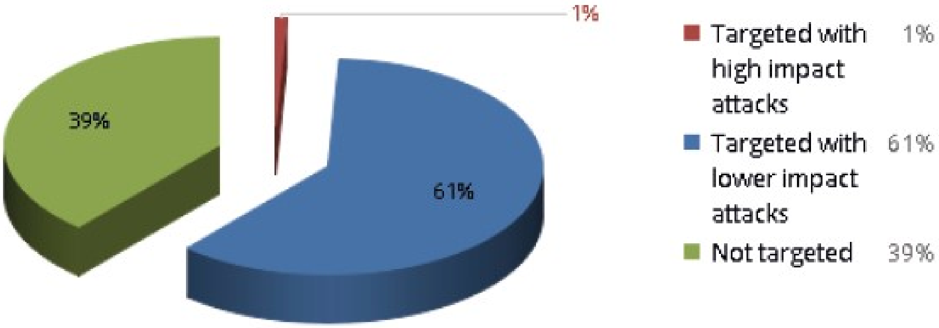


Fig. 18 Impacted hosts

The following applications (Figure 19) have been identified as associated with attacks.

APPS ASSOCIATED WITH HIGH IMPACT EVENTS	COUNT
DNS	2,111
Web browser	1,961
Internet Explorer	8
SMTP client	3
Firefox	2

APPS ASSOCIATED WITH LOWER IMPACT EVENTS	COUNT
DNS	186,565
BitTorrent client	4,215
Web browser	2,408
Chrome	1,655
SMTP client	1,633

Fig. 19 Applications associated with attacks

3 CONCLUSION

Application vulnerability attacks detection

Application vulnerabilities (also known as IPS attacks) act as entry points used to bypass security infrastructure and allow attackers a foothold into your organization. These vulnerabilities are often exploited due to an overlooked update or lack of patch management process. Identification of any unpatched hosts is the key to protecting against application vulnerability attacks [1].

Detected 51 application vulnerabilities.

Malware detection

Malware can take many forms: viruses, trojans, spyware/adware, etc. Any instances of malware detected moving laterally across the network could also indicate a threat vector originating from inside the organization, albeit unwittingly. Through a combination of signature and behavioral analysis, malware can usually be prevented from executing and exposing your network to malicious activity. Augmenting the network with APT/sandboxing technology can also prevent previously unknown malware (zero-day threats) from propagating within your network.

Detected 6 malwares.

Botnet infections

Bots can be used for launching denial-of-service (DoS) attacks, distributing spam, spyware and adware, propagating malicious code, and harvesting confidential information which can lead to serious financial and legal consequences. Botnet infections need to be taken seriously and immediate action is required, identify botnet infected computers and clean them up using antivirus software.

Detected 2 infections.

Malicious websites detection

Malicious websites are sites known to host software/malware that is designed to covertly collect information, damage the host computer or otherwise manipulate the target machine without the user's consent. Generally visiting a malicious website is a precursor to infection and represents the initial stages of the kill chain. Blocking malicious sites and/or instructing employees not to visit/install software from unknown websites is the best form of prevention here.

Detected 0 malicious websites.

Phishing websites detection

Similar to malicious websites, phishing websites emulate the webpages of legitimate websites in an effort to collect personal or private (logins, passwords, etc.) information from end users. Phishing websites are often linked to within unsolicited emails sent to your employees. A skeptical approach to emails asking for personal information and hovering over links to determine validity can prevent most phishing attacks.

Detected 0 phishing websites.

Proxy applications detection

These applications are used (usually intentionally) to bypass in-place security measures. For instance, users may circumvent the firewall by disguising or encrypting external communications. In many cases, this can be considered a willful act and a violation of corporate use policies.

Detected 11 proxy applications.

Remote access applications detection

Remote access applications are often used to access internal hosts remotely, thus bypassing NAT or providing a secondary access path (backdoor) to internal hosts. In the worst case scenario, remote access can be used to facilitate data exfiltration and corporate espionage activity. Many times, the use of remote access is unrestricted and internal corporate use changes should be put into practice.

Detected 3 remote access applications.

P2P and filesharing applications

These applications can be used to bypass existing content controls and lead to unauthorized data transfer and data policy violations. Policies on appropriate use of these applications need to be implemented.

Detected 6 P2P and filesharing applications.

Internal threats are inevitable and are growing exponentially, while cybercriminals profit from stolen consumer and business information leaked from corporate networks.

Knowledge of the threat landscape combined with the ability to respond quickly at multiple levels is the foundation for providing effective security. Application control and intrusion prevention (IPS) are foundational security technologies in a next generation firewall.

References

[1] Available at: http://www.fortiguard.com/intrusion

[2] Available at: http://www.fortiguard.com/encyclopedia/application

[3] Available at: https://www.paessler.com/network_traffic_analyzer

[4] Available at: https://www.sans.org/reading-room/whitepapers/forensics/detecting-malware-sandbox-evasion-techniques-36667

[5] Available at: http://blog.opensecurityresearch.com/2014/03/identifying-malware-traffic-with-bro.html

[6] Available at: http://la.trendmicro.com/media/wp/tms-whitepaper-en.pdf

[7] Available at: https://www.cisco.com/c/en/us/support/security/cyber-threat-defense/products-implementation-design-guides-list.html

[8] Available at: https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76

Eng. Martin DROPPA
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: martin.droppa@aos.sk

Capt. Eng. Boris MATEJ
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: boris.matej@aos.sk

Col. (ret.) Assoc. Prof. Eng. Marcel HARAKAĽ, PhD.
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: marcel.harakal@aos.sk

Eng. Martin Droppa was born in 1980. Degree in 2003 on the Military Academy in Liptovský Mikuláš. Since 2003 until now he has been working on various IT positions within Armed Forces Academy in Liptovský Mikuláš and other companies. He is a PhD. student at the Armed Forces Academy in Liptovský Mikuláš.

Eng. Boris Matej was born in 1980 in Liptovský Mikuláš, Slovak Republic. He graduated (Ing.) in 2003 on the Military Academy in Liptovský Mikuláš. He work at the Armed Forces Academy in Liptovský Mikuláš as assistant at the department of Informatics. He is a PhD. student at the Armed Forces Academy in Liptovský Mikuláš.

Col. (ret.) Assoc. Prof. Eng. Marcel Harakaľ, PhD. - He received the MSc. degree in electrical engineering from the Faculty of Electrical Engineering, Slovak Technical University in Bratislava in 1983. In 1997 he successfully finished his PhD. studies in artificial intelligence. From 1983 to 1989 he worked as a research engineer at the Military Research Institute in Liptovský Mikuláš. In 1989 he joined the Armed Forces and since then he has worked in various teaching and managerial positions at the Department of Informatics. During his university career from 2004 to 2012 he led the Department of Informatics. Currently he is in the position of Vice Rector for Science of the Armed Forces Academy of General Milan Rastislav Štefánik, Liptovský Mikuláš, Slovakia.

His research interests include computer engineering, image processing, cyber security, and network operations. He is the guarantor of the bachelor degree study program “Computer systems, networks, and services”. Since 2003 he has been a member of AFCEA and since September 2006 he has been in the position of Vice President for Membership of AFCEA Slovak Chapter. Since 2004 he has been the General Chairman of the International Scientific Conference “Communication and Information Technology - KIT” in Tatranské Zruby, High Tatras.