International Conference on Security Studies

University for Business and Technology - UBT

Follow this and additional works at: https://knowledgecenter.ubt-uni.net/conference

Recommended Citation
University for Business and Technology - UBT, "International Conference on Security Studies" (2020). UBT International Conference. 16.
https://knowledgecenter.ubt-uni.net/conference/2020/2020booksofproceedings/16

This Event is brought to you for free and open access by the Publication and Journals at UBT Knowledge Center. It has been accepted for inclusion in UBT International Conference by an authorized administrator of UBT Knowledge Center. For more information, please contact knowledge.center@ubt-uni.net.
Proceedings
9th UBT Annual International Conference
International Conference on Security Studies
30 - 31 October
UBT Innovation Campus
Proceedings of the
9th Annual International Conference

International Conference Security Studies

Edited by
Edmond Hajrizi

October, 2020
Editor Speech of IC - BTI 2020

International Conference is the 9th international interdisciplinary peer reviewed conference which publishes works of the scientists as well as practitioners in the area where UBT is active in Education, Research and Development. The UBT aims to implement an integrated strategy to establish itself as an internationally competitive, research-intensive institution, committed to the transfer of knowledge and the provision of a world-class education to the most talented students from all backgrounds. It is delivering different courses in science, management and technology. This year we celebrate the 19th Years Anniversary. The main perspective of the conference is to connect scientists and practitioners from different disciplines in the same place and make them be aware of the recent advancements in different research fields, and provide them with a unique forum to share their experiences. It is also the place to support the new academic staff for doing research and publish their work in international standard level. This conference consists of sub conferences in different fields: - Management, Business and Economics - Humanities and Social Sciences (Law, Political Sciences, Media and Communications) - Computer Science and Information Systems - Mechatronics, Robotics, Energy and Systems Engineering - Architecture, Integrated Design, Spatial Planning, Civil Engineering and Infrastructure - Life Sciences and Technologies (Medicine, Nursing, Pharmaceutical Sciences, Psychology, Dentistry, and Food Science),- Art Disciplines (Integrated Design, Music, Fashion, and Art).

This conference is the major scientific event of the UBT. It is organizing annually and always in cooperation with the partner universities from the region and Europe. In this case as partner universities are: University of Tirana – Faculty of Economics, University of Korca. As professional partners in this conference are: Kosova Association for Control, Automation and Systems Engineering (KA – CASE), Kosova Association for Modeling and Simulation (KA – SIM), Quality Kosova, Kosova Association for Management. This conference is sponsored by EUROSIM - The European Association of Simulation. We have to thank all Authors, partners, sponsors and also the conference organizing team making this event a real international scientific event. This year we have more application, participants and publication than last year.

Congratulations!

Edmond Hajrizi,

Rector of UBT and Chair of IC - BTI 2020
## CONTENTS

- **Russian Disinformation in the Balkans**
  - Selim Ibрайми, Рузги Matoshi
  - 5

- **Security of Information Systems - Legal and Ethical Rules, Challenges of Applying in Kosovo**
  - Рузghi Jashари, Мухамет Avдлы
  - 9

- **Application of Contemporary Methods in Fighting Organized Crime in the Republic of Kosovo**
  - Sheqir Kutловci
  - 18

- **Kosovo’s Exposition to Hybrid Threats**
  - Фатош Рушити, Шпендим Охха
  - 27

- **Information Security and Feeling of Public Insecurity in COVID-19 Pandemic Circumstances**
  - Ахмет Нуредини
  - 31
RUSSIAN DISINFORMATION IN THE BALKANS

Selim Ibraimi ¹, Ruzhdi Matoshi ²

¹* South East European University in Tetovo, N. Macedonia. PhD Candidate, Political Science : e-mail: ² Faculty of Political Sciences, UBT College, Republic of Kosovo, ruzhdi.matoshi@ubt-uni.net, matoshi.r@gmail.com, selim@journalist.com

Abstract: The purpose of this paper is to identify the sources of Russian influence in the Western Balkans. The most influential tool of the Russian Federation is the information warfare, composed with hybrid tactics, attempting to set a foot in the Western Balkans. Qualitative methods were used for analysis and the findings. The main results indicate that Russia has divers’ methods to impact political developments in the Balkans. Russia has been interested in this part of Europe, and it engages with all interested sides in the region.

With its state propaganda, Russia at least has the ability to divert the policies of the Western Balkan states towards the EU. Moscow prefers the status of neutrality of the countries that emerged from the Yugoslav Federation. In other words, Kremlin challenges the U.S. on some levels and the sources of Russian influence primarily are stemming from information warfare strategies integrated in different platforms. Recently the EU and the U.S. have expressed their concerns on several occasions over the direction of democracy in the Balkans. Indeed, Bosnia and Herzegovina, Kosovo, Montenegro, and North Macedonia remain on the edge of Russia’s ‘sharp knife’ which has the purpose of reversing the reforms and imposing the set of regulations which favors Kremlin in the Balkans. As the paper indicates, Russia uses domestic and international news outlets as propaganda to reach the nations in the region to win hearts and minds of the people against the Western approach to some extent. Therefore, the tendency of Russian propaganda remains a threat for the Western Balkans fragile societies. Russian strategic investments are primarily in the energy infrastructure, the oil market and the news outlet organizations around the region.

However, Russia keeps her hands open and engages with Serbia via the news organizations such as ‘Sputink Serbija’ and it utilizes Belgrade as a geopolitical tool to stir the unrest in Northern Kosovo. Russia and Serbia have good strategic relations which makes Russia a great power in the Balkans and as a key player. We conclude that the Balkans remain a flashpoint for regional actors and non-state actors. The Balkan states must continue the path of reforms as the only way to achieve peace and prosperity. But as paper emphasizes, Russia will continue to play crucial role in all events of the Balkan politics due to the power of Russian Federation in international politics.

Keywords: Russia, Western Balkans, hybrid warfare, disinformation, covert operations

INTRODUCTION

Russia has been a global power in international relations since the 17th century when Peter the Great and later Catherine the Great raised Russia's geopolitical status internationally. At the present time, especially after 2000, with the coming to power of President Vladimir Putin, Russia has become more aggressive and antagonistic on a regional scale, including in the Western Balkans. Russia uses all means and resources to meet the national objectives related to the strategy for influence in the former spheres of influence. Therefore, Russia's silent return to the region is not accidental and is aimed at upsetting the political, economic, ethnic and cultural balances in the Balkans in the long run. Since 2008 the Russian Federation at some point achieved several objectives to push back the Balkan democracies towards reforms and European integration (Dursun, 2019: 124). While the Federation of Bosnia and Herzegovina demands a comprehensive reform of its functioning or ethnic division, Kosovo urges Washington and Brussels not to make territory and sovereignty part of the new Serbia-Kosovo agreement. The "Balkan Initiative" is going together with the other “Three Seas Initiative” (3SI) to prevent Russian-Chinese influence in Central and Southeast Europe, while Russia with hybrid methods has freely created a significant advantage in the Balkans (Bardos, 2017: 9). The strongest Russian tool is disinformation and intelligence services in the Balkans. The reforms of transition to democracy and market economy initiated by the Washington Consensus after the fall of communism have lagged behind in the Western Balkans and they have yet to undergo transformation towards the EU (Matoshi & Mulaj, 2019: 180). Moreover, transition and privatization in Kosovo began with a one decade delay than in the rest of Central and Eastern Europe and went ahead at slower pace, in part due to disagreements by the international community and Russia’s veto in the UN Security Council. After three
proposals for ownership transformation and privatization, the process finally got underway in 2002 (Mulaj, 2005: 146-149)

Russia’s influence to her neighboring states where Russians make a sizeable minority suits well the idea of nationalism and nation-states in the Balkans, primarily the Serbs who may emerge victorious along these lines. This is what the EU and the US have been concerned as it may become a precedent for other European countries consisting of multi-ethnic societies.

METHODS

The aim for this study stems from the practical and theoretical reasons for Russian influence in the Western Balkans and the US response during this period of Russian covert operations in the region. The study was based on published materials about the Russian strategy in the Balkans and uses qualitative methods, e.g. interviews with experts to determine the Russian role in the region. This study has an empirical theoretical approach and the collected material shows that a new era is beginning among the Great Powers in the Balkans (Metodieva, 2019: 14).

The US Ambassador to Berlin Richard Grenell’s new initiative was a step forward from the failed European diplomacy launched by the EU in 2010-11, led by the former EU diplomat Frederica Mogherini, where more than 30 agreements were signed between Pristina and Belgrade, and none was implemented. But this moment is a good case of Russia’s return to the Balkans through frozen conflicts such as Kosovo and Bosnia Herzegovina. Russia has a strong diplomacy, managing to turn unresolved disputes into an instrument of the Russian game in the Balkans (Jonsson, et al, 2018: 87).

A rivalry of external actors is likely to exacerbate the difficult state of regional trade and the loss of fragile ethnic balance in the hottest interethnic parts of the region. Russian diplomatic intervention for a new century-old agreement between Kosovo and Serbia, is the new Russian leap in the phase of resumption of Euro-American dialogue (Samorukov, 2019: 11). According to the material and findings, one of the main strategies of Russia in the Balkans remains that hybrid strategy a mix of classical and intelligent Russian methods inherited from the time of communism and perfected over the last two decades.

ANALYSIS

From the obtained analysis, we can argue that the Russian action has been present in the Balkans and in Northern Macedonia. The main research question is as follows: Has there been political and diplomatic intervention by Russia in the Western Balkans? The analysis of 20 interviews showed that the Russian hybrid strategy includes a series of actions in several key and very sensitive areas where Moscow manages to meet Russian strategic objectives in the Balkan region (Secrieru, 2019: 13). Figure below shows how this strategy operates.
DISCUSSION

Moscow's tremendous influence on local and national politics, media and business circles backed by the Russian Orthodox Church, poses a permanent threat to the region, and Moscow is now able to provoke ethnic and religious tensions, block reforms by supporting radical nationalist forces (Cohen 1994: 822). All these are driven by political, ethnic disputes and economic rivalry, which Russia makes it with the strategy of "divide and rule" (Stronski & Himes, 2019: 4).

Russia stepped up its active measures in the region, applying more informal factors to its current policy and use of intelligence. Russia has consistently used cyber tools to punish, hack and misinform. Large-scale cyber-attacks have been carried out discreetly or as part of complex hybrid operations in combination with other coercive means (Prier, 2017: 68).

With cyberattacks, Russia has been particularly effective in the arena of psychological information, where Russian narratives have received considerable reinforcement through social media. The field of psychological information is essential for reducing support for the European Union and NATO in the region and understands the growing polarization between pro-EU and pro-Russian factions (Vejvoda, 2017: 40).

PROJECTIONS AND CONCLUSIONS

Russian hybrid strategy, cyber- attacks and espionage remain the main Russian tools in the region. However, in the Western Balkans, disinformation has been Russia's most obvious target. Strategic disinformation and communication have another impact that Russia uses for political purposes. Disinformation and propaganda are carried out through a number of actors, including Russian embassies, state, private media and hackers. U.S. has reacted very little with direct means, even only through public diplomacy, funding of non-governmental organizations to counter Russian propaganda in the Balkans. U.S.
in the Balkans can’t so easily oppose the Russian presence or Kremlin propaganda. The Russian battle is difficult. Therefore, it requires strong players to face Russia in the Balkans.

**BIBLIOGRAPHY**

Abstract Being aware of the epochal developments of Information Technology and Communication, as well as the irreplaceable role in all areas of life and the new challenges that digitalization has brought during its use, our project will clarify the legal rules, ethical and challenges during application use in Kosovo.

While we are having our time off, lunchtime, sleep time or we disconnect from information network for some moments, we see that with the clicks we are making in our computer machine, we stumble in a lot of new information. But in the ICT field, we are full of information about hundreds of new software programs and applications... which make work easier for us in these services e.g. banking, health care system, education, administration, production, etc. All these goods come as a result of the epochal development of digitalization. Large data collection; "BIG DATA", "ARTIFICIAL INTELLIGENCE", "COMMUNICATION NETWORKS", "e-GOVERNANCE" and "INTERNET", is a necessity, almost insurmountable in support of our work be they services; operational, educational, administrative... or scientific research. Whereas, the coherence of the implementation of international, constitutional, and ethical rules regarding the dignity of the individual, fundamental rights, privacy and security of personal data, leave much to be desired because their violation is the concern of the new democratic society.

Understanding of Information Security, Information systems, Big Data, Legal-Ethical Rules, and Violation of the individual’s data, are the focus of the following topic.

Keywords: Information Systems Security, Legal-Ethical Rules and Challenges of Violation of the personal data.

INTRODUCTION

Developments in digital technology, major developments in the field of programming and applications, together with the advanced development of the Internet, have brought humanity to new challenges. The 21st century belongs to the new era, of a revolutionary turn, in terms of the aspect of fundamental human freedoms, in relation to the era of digitalization. These developments have attacked, as never before, individual human rights.

If we ask, is there a sphere of human life where digital technology and information technology are not applied? Each of us would respond with: No!

In order to clarify these developments, especially the interconnection between Information Systems, Information Systems Security, Information Security, Security and Cyberspace. Personal data Protection and their Security, in continuation of this paper we will try to give a modest contribution in this field, highlighting the necessary need for the priority of INDIVIDUAL FREEDOMS.

Artificial intelligence, big data, otherwise known as analytical data, Internet of Things (Io), major developments around programming and applications, social networks of communication and information, specialized technologies of observation (interception), during operations, in the world of the Internet, before humanity, have brought and are bringing new tasks that require urgent action, the issuance of legal-ethical rules, to create staff with comprehensive knowledge of use gave the practical application of knowledge that, to the human beam of this era to bring security in privacy, security in the right to information, security in cyberspace ....

The global pandemic COVID-19, with its brutal spread, gave the lesson to all citizens of all walks of life, all professions without distinction. To keep the economy in continuity (out of collapse) and services as well as governance with them, we were forced to use online platforms to execute our jobs and services. A quality e-government, for all these sections, would definitely be a support product and service for these economies.
With the Security of the individual, of course also the economic, commercial, educational, scientific, health, administrative, political, technological developments..... etc. the following term would be completed and justified; "Knowledge society" where often as a term, has begun to be used in this century, by all societies that have touched the peaks of digital developments.

Also, to illustrate our actions in this regard, it is worth mentioning the statement of Kevin Ashdon, digitalization expert, who says for the Internet of Things: "we are able to collect everything that is possible, around you, to research everything, to increase our revenues ... ". Therefore, it is seen that profiling for the individual has not stopped and neither methods nor means have been chosen to reach the goal.

**DHE BASIC MEANING FOR SECURITY INFORMATION AND INFORMATION SYSTEMS**

By English "InfoSec" means information security (SI). While information systems are the product of a lot of work, of managed information, from the aspect of IT functioning and organization, to reporting and information through paperwork! In English we see the expression "Information System’s" - information systems (SI). Today, the efforts and promotions in terms of personnel, are oriented in the direction that through knowledge institutions, to acquire and advance knowledge in this specific field. In addition to knowledge of the functioning, role and interest of the market economy for the scientific-theoretical-practical application of information systems, knowledge of Information Systems Security (SSI) is essential.

Naturally the question arises, where to get this knowledge?

In the region, especially in Kosovo, there are very few academic institutions, colleges and faculties, in the public and private sector that deal with these studies, although worldwide, there are many specific departments and studies in this field.

But, in our country (Kosovo), we enjoy the fact that, UBT, in view of a perspective towards the future, for the needs of the country, for more than a decade, has set up a specific faculty of Information Security Systems, in it two levels, Bsc and Msc, where successfully, is giving valuable contribution, not only in Kosovo but also in the Region.

Closely related, security and information systems give every economy, whatever it is, security, reliability, sustainability, and increased profitability during its development.

**What do we mean by Information Security?**

Security in the cyber "universe" has a very wide dimension, and can be related to: Computer security, IT security, information security, information systems security, Internet security, general security in cyberspace, individual security, etc. For us this means that we are dealing with general security in society.

However, information security today, is looked at - studied through three main components; Confidentiality, Integrity and Availability, otherwise in the language of the profession is called the triangle - CIA. While, the application of the other two components continues; authenticity and non-rejection.

What do we mean by Confidentiality of information; Information security mean where confidentiality "is the characteristic that information is not made available or disclosed by unauthorized persons, entities, or processes" (ISO 27000 and 27001).

What do we mean by Integrity? In information security, data integrity means; that the data is stored and protected, and that it is accurate, complete and up-to-date at all times.

What do we mean by availability? We mean that: information should be available for any information system, when it is necessary to serve a certain purpose. So, it means: to those to whom the information is dedicated to, it should be available at the time when it is needed.

What do we mean by authenticity? We mean, originality and accuracy of information. The information is lawful and legitimate to be used by, persons or systems which are authorized and to which the information is dedicated to for use.
What do we mean by non-rejection (aspect of legality)? By law, non-refusal implies the intention of someone to fulfill their obligations in a contract. It also means that one party of a transaction cannot deny that it received a transaction, nor can the other party deny that it sent a transaction. (Note: This is also considered part of integrity). Thus, in this context, even diplomatic relations are valued through the signing of legal acts (contractual relations), Protocols, Conventions, Covenants, Decisions… etc. which have an impact on peaceful cohesion in human society, and are binding in practice, by the signatory parties.

What are Information Systems?

By an information system we mean the organized combination between: Human, hardware, software, communication networks, data resources, mode of operation and procedures.

An Information System (IS) supplies, receives, transfers and distributes information, within the organization, and, if necessary, exchanges it with the environment (outside the organization).

The tasks of an information system are: to describe correctly and accurately the information / to those who need it /, in a timely manner, in the required volume (quantity) and in the most appropriate format. The Information System (IS) performs the following tasks:
- Collects data,
- Processes data,
- Provides with data and information,
- Distributes data and information to users.

Information systems also perform other operations such as research or data tracking, where at the time of big data (BIG DATA), otherwise called analysis data, are extremely important for the development of enterprises, whether in the public or private sector, without excluding political and civil society organizations. A wide use of information systems, today, is encountered in various sectors, in research and studies in contemporary sciences, in particular, in the analysis, collection, systematization and operation of information and data, which are of interest to achieve to scientific explanations of various social and natural phenomena of interest to mankind, see (Methodology of Scientific Research in Social Sciences, (Matewsk and Rose: 2013).

From the above emphasis on information security and information systems, it is understandable that individual security precedes everyone, the term of the CIA triangle, and all the work done is in the service of individual security. So, if the individual (citizen), in the grip of the working organization or civil society, in the public or private sector, as a consumer of services will be safe and comfortable in the vortex of digitalization and ICT, then we say that information security it is satisfying.

With the individual security provided, Information Systems, public and private sectors, together with citizens, will have an advanced general security Thus the security of the individual, goes in the function of advancing the Fundamental Human Rights and Freedoms, in accordance with the UDHR of 1948 of the UN (DHRCL, 1948: UN), privacy laws (EC and EU General Regulation: 679 / 2016) and (Constitution of Kosovo, Pristina, 2008, amended 2013: Articles 21, 23, 26, 27, 36; p.14, f15, f16, f21)).

In fact, an Information Management System is a work of the whole organization to provide information for the decision-making process, Information Systems in the Insurance Sector, Tirana (Sherifi, I. 2016: 140). Based on the work they perform; Information systems are diverse, such as: Operating Systems, Decision Making Systems, Knowledge Support Systems, Human Resource Systems, Financial Accounting Systems, Data Analysis Systems, and Executive Information Support Systems, Executive Information Systems, and Information Management Systems etc. But, to ensure quality and reliability to the customer, many companies make certifications in the field of Information Security (ISMS), in the family of Security Standards, ISO 27001.
DATA AND INFORMATION (the main pillars of information systems)

How important is the security of information and privacy in social life?, the facts speak for themselves that, individual security nurtures general security and peace! So if we go back to social psychologists they have studied four strategies to turn enemies into friends: "These can be remembered as the four peacekeepers C’s: Contact, Cooperation, Communication, Community (pacification)" (David, G. Myers, EUGEN, 2003: 485). What does this have to do with Information Security and Information Systems Security? So, through communication, cooperation and reflection in the community, no matter which community it is, the threads of information security start. Therefore, the data during their processing, through information systems, up to the execution and finalization to information, to be used by the "community" to which the information is dedicated, is required to meet the requirements of the CIA triangle, plus two components, such as part of the debate not to reject and authenticity, which is required to be added to this triangle

What do we mean by data? To get a broader understanding of the data, if we click online, immediately in our search, we have some answers and some meanings, such as: from the link: (Https://www.bing.com/search?q=Cka+jan+te+dhenat+me+te+dhena&qs=n&form=Q BRE&sp=-J&pq=cka+jan+te+dhenat+me+te+dhena&sc=0-29&sk=&cvid=12694EB54BC44B08 : 3.10.2020, time 20.00h), we are provided with information for personal data, for the meaning of data, for databases, statistical data..... etc:

"Data are a set of values of qualitative or quantitative variables; that is, pieces of data are individual pieces of information. Data is measured, collected and reported, and analyzed, after which they can be visualized using graphs or images.

What do we mean by open data? According to the same link “Open data are those data which are created by organizations and public sector institutions for the realization of their competencies, which are published in order to enables their use by legal or natural persons for the creation of new information, contents, applications or services”. This data is open for use by the public, otherwise it is information!

Enormous amounts of different data, quantities, names, various publications, regardless of type and kind, whether physical or not, such as: Name, telephone number, address, square kilometers of a land area, number of inhabitants, product prices, number of members of a party, sickness ratio, number of passengers on the plane, bank deposits, amount of daily output in a factory, number of students in a school, building material of an apartment, daily output of bread, employees of a ministry, ... etc. Constitute different factual values of data within different organizations. This data, after being processed, is placed in databases, where after their finalization, they are dedicated, or are open to different users.

Today, due to the constant demands of civil society, a lot of finalized data is required to be made public, and open to the public, in order, as structured on their sites, for easy access by the public, to help and advanced employment, studies, research, analysis and broad interest, with the motto: transparency, accountability economic development.. (Open DATA Kosovo) https://opendatakosovo.org/ ,03.10.2020. Time 22.30h.

In today's technological developments, in the field of digitalization and the Internet, the possibility of compromising data and information is quite high. Therefore, personal data, which even as relevant data of the individual, which linked to the individual (person), being outside the public interest, today are excluded from such publications, with the very fact that they endanger the privacy of the individual.

What do we mean by information's? They are data processed or converted, that have content that is understandable and usable for the user. All the data, when they go out of the enterprise, to be used by the customers, then we say that we are dealing with information. Next, through the diagram diagram we see the data processing, input-output, through an information system.
Information systems (IS) are used in all areas and human activities. The expression IS does not make sense without the use of computers. Computer-aided information systems (ISs) are called: Information Systems Computer Database (ISCD). In Information Systems, IT represents the Information Systems infrastructure.

ETHICAL AND LEGAL ASPECTS

The rapid development of digitalization has posed risks to privacy and individual security. Personal data and information security are seriously endangered. While enormous amounts of data, minute by minute, are generated on various Internet networks and give rise to new applications and programs for economic advancement, including the invention of digital devices, then it is understandable that there is a possibility that malware is a steps before the rule of law regulators, while a lot of time is spent until the issuance of legal acts and their implementation in practice.

This "yellow" time space can serve as fertile time for cybercrimes, organized cybercrime terrorism, up to the international level.

In order to avoid these problems of human society, so that we do not have the collapse of the systems of life and work, it is necessary to issue laws and rules for the use, practical implementation and institutional supervision of the use of IT. Shared unified society platforms, for security would greatly advance the security and privacy aspect.

Knowing that the use of Internet "is a system of interconnected computer networks that use the Internet Protocol suite (TCP/IP) to connect billions of devices worldwide. It is a network of networks consisting of millions of private, public, academic, business, and government networks, with local to global scope, connected by a wide electronic collection ... 
(https://www.bing.com/search?q=qfar+kuptojme+me+te+dhena&form=EDGHPT&qs=PF&cvid=4fcf940ce88b455780d3118dc0bc2f00&cc=AL&setlang=en-U, 3.10, 22.00h).

Then, seeing this possibility of such rapid developments, of global communication, rapid actions are required, until the issuance of sanctioning codes and laws for the supervision of this field, in the "gray" period not covered by laws, an important effect for data security would be provided by CODES OF ETHICS, issued at national and international levels, which are issued more quickly, and can become binding on all public and private bodies.

Codes of Ethics
By ethical issues we mean standards, which define what is right and what is wrong; based on the obligations to avoid actions such as: rape, murder, robbery, abuse, human rights violations, etc. Codes of Ethics, then, are rules of individual behavior or morality of people in society. Ethics as a science-branch of philosophy has its roots in antiquity, but today, professional codes of ethics can be drafted (written), in the form of instructions or in the form of normative acts (laws, regulations ...). To increase accountability at work, and to gain public trust, professional codes of conduct are issued and published by professional associations, various companies, corporations and institutions, without distinction, in the public and private sectors. This is a self-regulatory obligation of organizations of different professions, to regulate themselves, in the general interest of society. In the regulatory institutions of human rights, information security, right to information, etc are the mandatory codes of ethics, which are found on the official websites of these institutions. Ethical codes are issued, even at the European level, where we can find them on their official website, such as the European Commissioner for Information Security, the European Commissioner for the Right to Information, the European Commissioner for Personal Data Protection, etc. In Directive 95/46 it was the obligation of all institutions of the EU and EC MPP, that before the final approval, the codes of ethics of these institutions to obtain the approval of the Consultative Committee 108/81, of the MDP of Directive 95/46 46, Working Group 29. This Directive has already been revised and transposed into the General Regulation of Personal Data Protection 679/2016, of the EU and the EC.

The introduction of new information technologies has shocking effects on society, so new ethical, social and political issues have been raised that need to be addressed at the individual, social and political levels and in the relationship between ethical, social and political issues in an information society, International Summer Academy of Science, (Jashari.R.: UBT, 2020), Pristina.

The universal principles of ethics are: Personal, Professional and Global.


In this regard, to strengthen ethical control and accountability, the EUROSAI Steering Board has established the EUROSAI Audit and Ethics Task Force (TFA & E) as an instrument to support European SAIs in promoting the importance of ethical conduct, http://www.klsh.org.al/web/mbeshtetje_sai_ve_per_permiresimin_e_infrastruktures_etike_1083.pdf, 06.10.2020, time 21.00h, in various life campaigns.

Laws and Legal Rules

The search power of Internet search engines has changed the form of communication, and with dizzying speed has connected humanity, regardless of its location, anywhere in the Globe. This communicative power has transformed the way of behaving and living, generating new inventions with the help of Artificial Intelligence, transforming administrative affairs through e-Government. The publication of numerous data on the Internet, called "BIG DATA", has caused humanity to spend billions of dollars, for programs and data analysis experts, to enter the function and service of the economy.

Numerous data on the Internet bring not only profits and industrial-economic development, but often times, cyber threats endanger entire systems, where they go out of order, and cause billions of dollars in damage. The information downloaded on the Internet is stored for years, where; "Information which is published on the Internet, through search engines such as google, bingo, yahoo, etc. may reappearance even after many years; If you want to hide your identity, photos that enable your identification should not be used. Name and profile picture (fit-ks.org/wp-content/uploads/2016/03/5.-RJETET-SOCIALE.pdf · https://www.bing.com/search?q=qka+jane+informatat&qs=PF&cvid=fa2538494a74495dbf5013b6c57ab29f&ccc=AI&setlang=en-US&first=1&FORM=PORE1, (time 22.00h, 04.10.2020)

Today, the personal data of the individual are endangered. We often encounter intrusions into our profiles, data theft, account hacking, cloning of bank cards, etc. Therefore, in order to provide solutions to these problems and protect personal data, the EU and the EC, in 2016, issued the General Regulation of Personal Data Protection, 679/2016, which entered into force on, 25, May 2018.
The regulation is mandatory for all states, members of the EC, and signatory to Convention 108/1981, which strengthens sanctions against abusers and violators of data, increases the powers of regulatory authorities of the MDP, takes into account the right to was forgotten, provides obligations for certification and training in the field of MDP, as well as made mandatory the work of data protection officers in all public and private bodies.

The Law on PPS in Kosovo has been harmonized with the General Regulation (GDPR), during 2019. Kosovo has also issued the Law on Protection against Cybercrime, in accordance with the requirements of the Convention against Cybercrime, approved in 2001 and entered in force in v.2004. The Convention has also formed the European Committee on Cybercrime (GDPC).

Kosovo has also issued a cyber-security strategy 2016-2019, which should reflect the issuance of new laws, Cyber Security, Information Systems Security, Trust and Electronic Certifications and, should advance in a new strategy cyber security and protection of personal data at national level.

As for the constitutional aspect, the Constitution of Kosovo, 17 February 2008, and (amand.2013) has a sufficient legal basis regarding the protection and security of personal data, where Article 36, with four paragraphs, guarantees protection of personal data, and article 21 the dignity of the individual. The Constitution with 36 provisions in Chapter II, guarantees the Fundamental Human Rights and Freedoms (Constitution: 2008). While, great work remains, in issuing regulations, codes of ethics, administrative instructions and education of citizens, in ensuring individual security, as a threat to data and information security (Collins, A: 2012), "Bash time studies of Security in Social Sciences" Oxford press University, Tirana.

EXAMPLES ABOUT SECURITY AND PPD

Example 1.

CIA Director Georg Tenet, in his Book in the Eye of the Cyclone, on the occasion of the AlkaIde’s terrorist attacks on the World Trade Center in the Twin Towers in New York, on the occasion of receiving passenger lists from the Airport, had waited 15 minutes, due to privacy laws, when American national security was put at risk.. ?? So legal proportionality is imperative.

Example 2.

Known as "Dehari case", 2016, when the data of the camera recordings are published, during the investigation process, on TV Klan Kosovo…? This action, contrary to the Law on Criminal Procedure. So this publication constituted a criminal offense.

Example 3.

"The case of Memet Haqif", Intrusion into privacy, when the cameras were monitoring the school toilets, the intrusion was made in the privacy of students, prohibited by applicable laws. This was a punishable act in accordance with the LMDHP.

What do Information Systems students say?

In the questionnaire for evaluation of the academic staff (R. Jashari), the second year students, level Bsc. (UBT: 2020), among the 14 questions for evaluation, in the subject Ethical and Legal Issues in IS, had this question: "II SUBJECT AND RESOURCES-Evaluate the course materials and evaluation (the course is of interest for professional development)"? The answers were as follows: Out of 32 students included in the assessment: 18 st. said, that, 60% is of interest, 9 st. 40% said that it is of interest, while 6 st.80% assessed that it is of professional interest to be taught.

So, the assessment comes out, somewhere over 60% who say that this knowledge is necessary for the profession and for society. But, the courses of IT Law and Society, Security and Privacy of Information Systems, are exactly the same forms of Legal, Ethical, Security and Privacy knowledge, at IT and IS in the faculties of CSI and IS. Raise awareness, education and professional responsibilities in the respective professions and are much needed in the age of digitalization. For the generation of advanced knowledge,
this knowledge is a necessity to be taught in the faculties with study programs, as well as in Social Sciences and Contemporary Security Studies.

CONCLUSIONS

At the national level, the following actions are given priority:

- Issuance of the National Strategy for Cyber Security and Security Systems
- Issuance of the National Strategy in the field of Personal Data Protection,
- Staffing and Institutional Strengthening of the Supervisory Authorities of IS and MDHP. The 5-year period without the head of the Authority Authority, is a poor performance of the State of Kosovo, in the field of Security and Individual Freedoms.
- Strengthening knowledge at academic levels in the following areas: IT Law and Society, Information Security and Privacy, Ethical and Legal Issues in IS, and Protection against Cybercrime.
- Capacity building of CERTs and CSIRTs.
- Code of Ethics in all public and private sectors.

REFERENCES

● Authorized lectures, in the subject, Privacy and Information Security, UBT, 2018-2020,
● European Convention on Human Rights and Freedoms, 1953,
● Convent 108/1981, Strasbourg, 1981,
● General Regulation GDPRR, 679/2016 of the EU,
● EC Directive, 46/95 of the Commission, of the Parliament and of the EC, on MDHP, Luxembourg 1995,
● Law on Personal Data Protection, 03 / L-086, 2019,
● R. Jashari, Personal Data Protection, UBT, 2018,
● Questionnaire for the evaluation of academic staff, in SI, UBT, 2020,
● Matewsk and Rose, Scientific Research Methods in the Social Sciences, 2013,
● G.Tenet, In the Eyes of the Cyclone, 2001.,
Application of Contemporary Methods in Fighting Organized Crime in the Republic of Kosovo

Sheqir Kutllovci
Abstract. In this paper 1 we will explain the causes that lead to problems in the application of modern methods and tools of combating organized crime in the Republic of Kosovo. Based on the analysis of cause and effect, efforts are being made to overcome them. The paper is based on comparative analysis and presentation of local and international forensic practices that ensure quality. The paper focuses on the following issues: analysis of the strategy against organized crime; the incompetence of the human factor in the police, prosecution and judiciary; insufficient motivation in the application of forensic methods; better coordination with contemporary methods aimed at combating organized crime is needed. Special attention is paid to standardization and international police cooperation in the fight against organized crime.

2. Modern terrorism a threat to human security In the scientific and professional literature, politics and the media have been occupied over the last few decades by the problem of terrorism and the consequences of its manifestations on the security of states. Developing the concept of focusing human security towards the consequences that this modern security is in threatening man and his values. The paper will emphasize that the state is threatened by terrorism through threats and the consequences of terrorism. For this reason, the fight against modern terrorism must be in the service of the protection and security of human beings. In this paper will be considered how the human component is positioned in the National Security Strategy, as it is the most strategic document of our country. It will be considered how terrorism is a greater threat to the traditional values of the state such as territorial integrity and its human component. Finally, we will show how the fight against terrorism contributes to the protection of human security, i.e. in its segment that endangers itself through terrorist activity.

Keywords: professionalism in policing; problems in applying modern methods and lack of forensic knowledge in the police, prosecution and judiciary; work at the scene; police motivation problems; standardization in forensic services.

Introductory part

When we talk about special measures against organized crime, we mean the reaction of the competent bodies of pre-trial and criminal proceedings to this phenomenon, namely the ways in which the legal system reacts to the need for more efficient detection and verification of crimes belonging to this form of crime.

Today, criminal procedure legislation in most countries, almost without exception, provides, to a greater or lesser extent, some special rules when it comes to criminal proceedings related to organized crime. The connection of these special rules with the general ones, which are contained in the sources of criminal procedural law, is reduced to the known relation between the norms of lex specialis and lex generalis. With the adoption of the new Code of Criminal Procedure, for the first time, some special rules regarding organized crime have been included in our criminal procedure legislation. Although these solutions were a big step, there was no major deviation from the traditional concept of our criminal procedure legislation. However, very soon these new solutions proved insufficient and this resulted in the adoption of a number of other rules through the amendment of the CPC included in the new Chapter XXIX of the Code of Criminal Procedure. This innovation introduced a completely new criminal procedure, hurting all the evidence mechanisms that mainly or even exclusively refer to the procedures for organized crime, which significantly modified all our criminal procedure legislation and these changes represent the most significant innovation in the procedure.

With this innovation, special rules have also been adopted in the Law on Organization and Competencies of State Bodies in the Fight against Organized Crime. This law introduced a number of new rules and mechanisms of criminal procedure in criminal proceedings, and also introduced new rules on the organization and competencies of state bodies of pre-trial and criminal proceedings in relation to criminal actions with an element of organized crime.
In this way, a very broad legislation of secondary criminal procedure was created, instead of some rules being included in the Code of Criminal Procedure, where they belong, as it is the basic and most important source of our criminal procedural law.

The conceptual characteristics and factual specifics of organized crime and its actors result in great probative difficulties when criminal actions with an element of organized crime are the object of criminal proceedings.

The need to establish adequate mechanisms of criminal procedure to overcome, or at least minimize these factual difficulties, is the legal report on the establishment of the basic rules of criminal procedure in relation to organized crime, which essentially ends in the creation of an environment of proper normative Within which organized crime crimes can be more easily and simply explain and certify. Criminal proceedings Organized crime actions have a number of specific - specific procedural solutions that are primarily related to the detection and investigation of these crimes. These specifics classify criminal proceedings into a set of special criminal proceedings in which the procedural model has been adapted to the specific requirements of the criminal case. In the context of the differentiation of procedural forms, the question arises whether criminal proceedings for organized crime in Kosovo are a separate procedural form or a procedural variability. While the general form sub means the form intended for adjudication in all matters not excluded from it and placed under special rules, the special form means a form that deviates from the general, and which is based on specific grounds and motivated by intentions. specific. The differential moment is present in the basis and structure of the process form. The basis of the process is the crucial reason for creating a particular form of process and we can find it in the characteristics of the process object and / or the subject.

The specific basis also includes the specificity of the process structure, which may be reflected in the removal or addition of certain stages of the process or stages of the procedure, or a significant modification of existing ones.

M. Škulić, Krimii Organizuar, Beograd 2003, fq.197.

As for the procedural basis, it is obviously in the features of the procedural object when it comes to organized crime offenses (gravity of the offense and social risk).

However, differentiated regulation does not change the structure of the process, but only changes certain provisions for the subjects of the process and the actions of the process, which will be discussed separately, so it is not a separate form of the process, but a variability of the process. that characterizes a specific basis resulting in a specific process structure.

**Special measures for the detection and verification of criminal offenses against organized crime**

Based on extensive forensic, criminological and criminal research, as well as several decades of experience in police practice in the fight against organized crime in the United States and Italy, based on numerous analyzes, it has been concluded that it is necessary to use special measures, secretly: e.g. Covert surveillance with collection and technical registration of data from various technical devices, electronic surveillance of communications, use of undercover investigators, controlled transport and distribution of criminal offenses, etc. As a rule, these measures are taken before the initiation of criminal proceedings, in order to reveal the structure, form, scope and methods of criminal organizations in order to initiate criminal proceedings against members of these organizations, and the results of these special measures can be used in proceedings. criminal as evidence certain facts only if:

- are expressly provided by legal provisions (principle of legality);
- there are no softer measures to achieve the same goal (principle of subsidiarity);
- these are very serious criminal offenses (principle of proportionality);
• the consent of the judge has been obtained in advance or the measures are carried out under his supervision (principle of judicial supervision).


Regarding the achievement of the same goal, the possibility of using witness protection measures, the testimony of the so-called repentant witness, who, with the effective implementation of legal mechanisms for confiscation of proceeds of crime and prevention of money laundering, must enable the successful fight against organized crime within generally accepted legal standards of restrictions on human rights and freedoms.

Obtaining information on organized crime should be based on the collection of criminal intelligence data on its bearers, structure, logistics, communication and financial base. Therefore, criminal investigations related to organized crime should be proactive (action instead of reaction), which means that the mentioned new investigative techniques should be applied, which cancel the concealment as a characteristic of organized crime. Also, the investigative activity should not only focus on the investigation of an individual criminal event, but in that case the necessary criminal intelligence data should be collected and the full criminal structure, all criminal chains and the complete criminal network should be investigated at the stage early preparation of crime in the national territory and the territory of other states. This approach to the fight against organized crime has resulted in the adoption of new laws or changes in existing procedural and police legislation, which significantly expands the repertoire of measures to combat organized crime by expanding opportunities for international police and judicial cooperation.

To effectively combat organized crime, as already mentioned, many legislations have introduced the possibility of implementing special measures to reveal the structure, form, scope and mode of operation of criminal organizations, in order to gather sufficient evidence to initiate criminal proceedings against members of these organizations. These measures are used when classic criminal measures and investigative actions do not yield greater results. The main difference between these special measures and the classic general criminal measures is in the probative value, with their help, of the data and knowledge gathered. Namely, while the results of the application of classical policy measures can not be used in judicial evidence, except exceptionally, and have only informal cognitive value for the purpose of coordinating and planning further investigative actions in criminal proceedings, the data and knowledge obtained from special measures have evidence of force before the court.

Jović, V., Organized Crime and Combat, Institute for Comparative Law, Belgrade, 2013, 64.

Po aty, p. 65.

These measures are mentioned differently in the legal literature. For example, in the German legal literature we come across the following names of these measures: special investigative measures, special police investigation methods, covert investigations.

In the American legal literature, these measures are called: secret methods, operations and secret procedures. The name of the special measure seems the most appropriate, because it can already be seen from the title that they differ from the general forensic measures which aim at detecting and clarifying the general crime. All these special measures are secret operations performed without the knowledge of the persons affected by those measures, with the use of adequate optical, acoustic and other technical means, which, according to the rules of intelligence work, gather relevant knowledge and data on organized criminal (terrorist) activity.

The notion of covert operations can be defined as a procedure established by law in which a number of operational and criminal-tactical measures and actions are used to gain the trust of persons suspected of preparation or execution by law, especially certain serious criminal offenses, or in order for authorized officials of the internal affairs bodies, with the help of legally prescribed measures and actions, to gather knowledge or document certain actions of the suspects, all with the aim of gathering possible evidence and determining the scope and organization of the suspects' criminal activities.

Covert operations, depending on the duration of implementation, can be divided into: long-term, short-term and ad hoc operations. Long-term operations mean the implementation of certain measures for several
months, individually or in combination, by which potential knowledge and evidence are continuously gathered for several months. Long-term operations include: surveillance and recording of telephone conversations, covert surveillance and optical recording of photography, and the use of undercover investigators. Short-term surgeries refer to a period of one month, and sometimes they last only a few days or even hours (for example, when it is known with certainty that a certain amount of drug will be bought and sold in a certain place at a certain time, i.e. before deprivation of liberty, with covert monitoring of the collection and evidence of other possible involvement of persons who do not participate). Covert ad hoc operations are conditioned by the impossibility of delaying the conduct of an undercover operation, and therefore it is carried out as soon as possible, with the shortest possible preparation time, and therefore they should not be complex (e.g. street drug purchase and deprivation of liberty of persons immediately thereafter). Special measures are divided into: infiltration measures and surveillance measures. In our legislation, special operational measures of policy infiltration in the sense include: hiring an undercover investigator, completing simulated legal transactions and providing simulated services, while covert surveillance measures are: surveillance and recording of telephone and conversations and other communications by other technical means, optical registration of persons, control of business and personal accounts of the suspect and controlled delivery.

**Controlled transport and delivery of criminal objects**

Controlled transport and delivery of criminal objects is one of the special measures for the detection and verification of criminal offenses, and we can say this to the youngest of all the mentioned measures. It is mainly applied to the detection and verification of criminal acts of illegal drug trafficking, transportation of nuclear waste, etc. Namely, within international criminal organizations, there is a clear division of labor, and the heads of criminal organizations themselves, as well as their financiers, are very difficult to relate to a specific crime. One such example is international drug smuggling, where couriers usually have contact with drugs, while organizers and funders come into contact with or near drugs only occasionally, during final delivery. This is why, by applying special measures, they try to identify all persons involved in smuggling (drug supplier, courier, corrupt police officers, customs, etc., smugglers and organizers, drug buyers, roads of smuggling, methods of smuggling).

Shikman, M., op. cit., p. 417.

Jović, V., vep. cit., p. 80-81.

C. Joubert, National and International Aspects of Secret Police, Police Magazine 4/95, 309.

e etc.). In all countries through which drugs pass, including those countries where money is made through drug smuggling. Controlled submission of criminal cases is in fact police oversight of illegal transport with late intervention, in order to reach the organizers and financiers of the criminal enterprise. In order for such an operation to be successful, it is necessary that the participating countries have the legal capacity to implement such measures. The police authorities and the judiciary must be very well coordinated, which means a well-developed and orderly system of communication and, ultimately, the deprivation of liberty in all countries must be simultaneous.

Article 1 of the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 13 controlled distribution is defined as an investigative technique through which the illicit or suspected shipment of narcotics, psychotropic substances and substances from the tables annexed to this Convention or substances substituting them, allow them to continue their journey, cross the territory or enter the territory of the same countries, with the knowledge and supervision of their competent authorities to identify persons involved in criminal offenses established in accordance with Article 32 rr. 2 of the Convention. The same Convention called the signatory of the controlled distribution application:

1) If permitted by the fundamental principles of their national legal system, the Parties shall, within their capabilities, take the necessary measures to enable the proper use of internationally controlled distribution, in accordance with the agreements or arrangements agreed upon, for identify persons involved in criminal offenses established in accordance with Art. 3 rr. 1 of this Convention and taking legal action against them;
2) Decisions on the use of controlled shipments shall be taken on a case-by-case basis and, where necessary, may take into account financial arrangements and arrangements relating to the exercise of jurisdiction by the parties themselves;

3) Illegal deliveries for the controlled delivery of which an agreement is reached, with the consent of the interested parties, may be confiscated and may be allowed to continue.


their journey with narcotic drugs or psychotropic substances intact or withdrawn or replaced, in whole or in part.

Special measures against organized crime under the Code of Criminal Procedure

When investigating certain types and groups of criminals, some investigative actions do not lead to the direct taking of evidence. However, this does not mean their uselessness and not their effectiveness in general. Such actions often create the conditions for obtaining evidence through a series of actions, events, measures Within the framework of the operative-tactical combination.

The use of modern, scientific and technological advances in the fight against crime is very necessary in today's world. Domestic work authorities can only succeed in the fight against serious crime, especially organized crime, only by using modern means. The term special investigative techniques (special investigative actions) is emerging recently, and is being adopted by the United Nations Convention against Transnational Organized Crime.

Covert or technical surveillance and investigation measures means each of the following measures:

- Covert photographic or video surveillance;
- Covert monitoring of conversations;
- Control of postal deliveries;
- Interception of telecommunications and the Reader should be used - IMSI - International Mobile User Identification;
- Interception of communications via computer network;
- Controlled delivery of postal items;
- Use of surveillance or placement of interception devices;
- Simulated purchase of an item;

Criminal activities provided in Art. 3 rr. 1 are: production, processing, distribution, preparation, offering, offering for sale, distribution, sale, distribution or any other term involving intermediation, transmission and a whole range of other activities listed in relation to drug and substance abuse illegal psychoactive, and which are essentially provided by the relevant incriminations of our positive criminal legislation.

http://gazetashqiptari.com/kombinimet-operativo-taktike-ne-luften-kunder-krimit-te-organizuara/?fbclid=IwAR3kD_i2oBPhg0CoC5QFb9z5OpZW7-G1pxtVfifaGcpXlry4dW-KNY9AA1Y


Simulation of the crime of corruption;
Secret investigation;
- Recording of telephone calls; and
- Disclosure of financial data.

The term special investigative techniques (special investigative actions) is emerging recently, and is being adopted by the United Nations Convention against Transnational Organized Crime. The actions and measures covered by the content of this term were accepted by many countries even before the adoption of the Convention, while other countries included these methods in their national legislation under different names only after the Convention was adopted and ratified.

Covert surveillance of communications

Covert surveillance of communications can be cited as another specific method used by security agencies to combat organized crime. Namely, modern technological progress has contributed to numerous benefits for humanity, which are monitored in the form of the development of computer and other telecommunication and information technologies in all spheres of social life. While, on the one hand, technological advances have influenced the development of new criminal methods and techniques in the fight against crime, on the other hand, it has also contributed to a large number of abuses in various areas of criminal activity. New technologies have led to changes in modern methods and techniques of surveillance, which are of great importance today in the fight against organized crime.

Covert surveillance of communications is a conspiratorial surveillance of objects of criminal interest and all types of actions and communications of persons in order to obtain operational information and evidence of their criminal activities.

Po aty, p. 269.

Po aty, p. 24.


3. Search of the apartment and personal search of persons suspected of committing organized crime

Control is a technical-tactical operation, which means that tactical-psychological experiences and methods help solve the question of "where should you control". Who is looking.

However, if armed resistance, any form of violence or destruction of evidence in another apartment or room is presumed, a search may also be carried out without any prompt order. The apartment owner will first be invited to open the premises voluntarily, after which the premises will be forcibly opened. In addition to the apartment owner, or his representative, landlord or neighbor, the legislature predicts that two adult citizens will be present as witnesses. The person conducting the search and the witnesses present may be only the person of the sex as well as the person being searched. Apartment search can be recorded with a camera, or some objects can be photographed. If during the search, the police discover items related to other criminal offenses for which criminal prosecution is being undertaken ex officio, they will seize the items and describe them in the minutes and confiscate the items you will issue a certificate.

In accordance with Article 26 of the Constitution of the Republic of Macedonia, the search of the house and other premises can be carried out only if it is possible that the search will catch the perpetrator, find traces or items that may be of great importance for the course of The search of the apartment is intensively legal because the legislator knows that on the one hand this action restricts the right to private and family life in the home and the correspondence of the persons being searched, traces or items will be found that may be of great importance. for the course of the procedure.
The control starts from an alcove, exactly from a certain point and continues on both sides (left and right) and vice versa, but in a way that the walls, furniture and other items near the walls are also controlled.


https://www.academia.edu/8903590/Pretres_stana


If during the search are found items that are thought to have originated from the criminal offense, then they are taken which are thought to have originated from the criminal offense, then they are temporarily taken (seized).

The first unavoidable action is the detailed control of all the accompanying persons. It is understood that, in advance, inside the blocked building or space, they have been checked for security issues and the suspects have been checked, but a detailed search is being done at the police station.

This is done in order to find and confiscate tools and traces of criminal offenses, as well as weapons or tools suitable for attack, defense or self-harm. If, during the search, certain means or traces are found, certain weapons or means, they are confiscated in accordance with the provisions of the Criminal Procedure.

4. Sequestration of items for cases related to the commission of organized crime

Confiscation or seizure is also a very important measure through which material evidence is provided in criminal proceedings. This represents a fairly common measure in the practice of the judiciary.

The state prosecutor may request the pre-trial judge to issue an order for the temporary seizure of items, property, evidence or money. Such request shall state precisely the items, property, evidence or money and shall describe how these items of evidence of the offense may be, how these items, property or money may enable the commission of the offense, or how these items, assets or money constitutes property gain gained through a criminal offense.

The temporarily seized items are photographed and kept in appropriate containers or transparent plastic bags and the authorized police officer or state prosecutor keeps a register of photographs and minutes on the supervision of each item or set of documents.

Petryo, p. 15.
Hajdari. A.op. cit., p. 280.
Sahiti E. Murati R. ElshaniXh.op. cit., p. 320.
Petyo, p. 320.

Weapons, vehicles, planes or other large items that have been temporarily confiscated are photographed and kept in the relevant safe areas and the authorized police officer or state prosecutor keeps a record of photographs and minutes of surveillance for each item or set of documents. When items are confiscated, it should be indicated where they were found and those items should be described. If necessary, proof of their identity must be provided in some other way. The seizure certificate must be issued for the seized items. During 2014 there was an increase in terms of temporary sequestration of property. According to the register of criminal reports on confiscated items temporarily approved by the Court at the request of the State Prosecutor, 5002 weapons, 63 vehicles, 4 houses, cash 117 491.60 euros, 61.58 kg of drugs, drugs 20 449 items were temporarily confiscated, other items worth 98 153.00 euros which in total amounts to 756105.19 euros. Meanwhile, according to the register of criminal reports for which the prosecutor with the indictment has requested permanent confiscation of items temporarily confiscated were confiscated: 24
Statistical data received during the period January - March 2015, speak as follows: - Only 1 order was issued under Article 264 of the CPC, or orders for temporary freezing of assets, this order was also issued by the SPRK; - Only 1 request for temporary issuance of an order was issued according to Article 265 of the CPC, or detention orders, and this request was issued by the BP in Pristina; - 32 requests for temporary confiscation were issued according to Article 267 of the CPC, including 22 such requests from the SPRK, 3 from the BP in Gjilan, 1 from the BP in Prizren, 2 from the BP in Prishtina, 4 from BPs in Ferizaj, 0 from BPs in Gjakova and Mitrovica. Out of 32 such requests, the courts have so far approved 17 such requests. EULEX prosecutors have reported 0 such requests. NO
TE: The database records that only one order was issued under Article 264 and again only another order under Article 265 of the CPC, but what is indicative is the fact that these requests were issued in one case from SPRK and in the other case from BP in Pristina. In all likelihood it is a matter of not keeping records properly because when a freezing order is issued under Article 264 then it is very likely, though not entirely necessary, to issue another request under Article 265 as long as if the request is issued according to article 265 then it must have been preceded by the order according to article 264 and this speaks about how unstable such a database is because the records are not being entered properly. The database continued to show that there was not a single claim related to the confiscated property, i.e. requests for the transfer of assets to government use, claims for compensation of the injured party, claims for the sale of confiscated items or destruction of items. confiscated and such a thing should be returned to the point of discussion for KPC members to see why such columns continue to be at zero figures and where are the reasons for such inaction. Further in the column of requests of the prosecutor for permanent confiscation of items obtained with criminal offenses, filed according to the indictment for all prosecution offices, it turns out that we are dealing with a total of 35 such requests. Leads BP in Ferizaj with 20 such requests, followed by BP in Gjilan with 6 such requests, BP in Prizren also with 6 such requests, BP in Peja with 3 requests and BPs in Prishtina, Gjakova and Mitrovicë / Mitrovica reported zero such requests. It is about small amounts because in one case in the BP of Gjilan was requested the confiscation of € 900 cash and in another case in the BP of Ferizaj were requested to be confiscated € 634. Taken as a whole, this section states that for this period of time € 210,000 were requested to be confiscated with an indictment, as cash, vehicles, medicines, etc.

Conclusion

Successful fight against organized crime implies the existence and implementation of a coherent and coordinated system of preventive measures and criminal law enforcement measures.

However, when taking these measures, some important facts of these forms of crime must be taken into account, such as the tendency to constantly change and adapt to current social conditions, the use of scientific and technical achievements in the methods of criminal activity, its state and proper protection. And a high degree of social risk.

Consequently, there is a need for continuous improvement of methods of combating these forms of crime, as well as the expertise and personnel of all entities involved in this fight. Accordingly, it is concluded that the existence of specialized bodies for the fight against organized crime and their continuous education is necessary.

Well-organized, planned and implemented activities, preventive and combative, prevent the emergence of new forms of organized crime, terrorism and corruption.
It is much more difficult, for example, to detect and prove the criminal acts of organized crime when it becomes known about their existence at the stage when it manifests itself in such forms that it has already taken certain positions in the government structure and certain bodies relevant.

Depending on the form, frequency and type of activity of organized criminal groups, states apply different methods in the fight against them, engaging mainly professional bodies but also all other social forces whose activities can contribute to successful repression of these forms of crime.

Countering organized crime requires overcoming the previous way of planning and the necessity of accepting strategic planning of all criminal activity, respectively operational, which is much wider and more dubious than traditional planning, which was undertaken exclusively after the execution of crime. Therefore, it is necessary to monitor the development of this crime, to investigate its etiology and phenomenology, to use the achievements of other sciences and to constantly adapt the methods of dealing with forms of certain of this criminal activity. Also, the essence of organized crime must be respected, i.e. financial power, money laundering, tackling corruption and social status, and in that sense adopting appropriate regulations that must be consistently implemented in practice.

**Bibliography**

5. Vessel Latifi, AgronBeka: Criminal Tactics, Pristina, 2017
6. Vlado Vodineliq: Criminology, Belgrade, 1996
7. V. Zafirovski; G. Kalajdzhiev; Z. Jankuloski; T. Stojanovski - Police and Human Rights, Police Training Manual; Skopje 2002
8. Petrovi B. B. Introduction to Forensics, Pristina, 2006

**Electronic sources:**

http://www.kosovopolic.com/
http://levizjafol.org/ anti-mafia law assists justice system in fighting and prosecuting organized crime and corruption /
https://www.academia.edu/8903590/Pretres_stana
http://gazetashqiptari.com/ operational tactical combinations in the fight against organized crime /? fbclid = IwAR3kD_12oBPZh0CoC50Fb9z5OpZW7-G1pxTViqaGepXlry4dW-KNY9AA1Y

**KOSOVO’s EXPOSITION TO HYBRID THREATS**

Fatos Rushiti, Shpendim Oxha
College UBT, R.Kosovo,
fatos.rushiti@ubt-uni.net, shpendim.oxha@ubt-uni.net
Abstract: The state of Kosovo is located in a geo-strategic position of the Western Balkans, and continuously is exposed to threats of interference by Serbia, whether directly or in other forms, like the hybrid threats. Kosovo is lagging behind in receiving more recognitions of the states in the world, and Serbia’s mature engagement in order to make obstacles in its membership in international organizations, in one hand, and the political crises accompanied by frequent early parliamentary elections, on the other hand, are sufficient political and theoretical circumstances in taking our decision for the analysis of the hybrid threats in Kosovo. Since the trends and the international developments in Western Balkans exclude the classical war as a mean for reaching goals, now the war is being developed in other forms, like diplomatic, economic, and technological ones. In referring to the theoretical definitions, the hybrid threats dedicate to the use of methods and means by a state or non-state actor, which decides to influence practically or strengthen its influence, in order to increase its interests, strategies, and evil-minded goals. These definitions mostly fit to the special war of Serbia against Kosovo. The fact that Kosovo does not have a special platform for reading the potential hybrid services, gives bigger interest to our scientific analysis. The legal, political and economic aspect, the media aspect, as well, without excluding the classical spying, that Serbia can still use in Kosovo, will be part of our scientific analysis. I must emphasize the measures to be proposed in a manner that Kosovo will be able to identify easier the destructive and destabilizing elements within its territory that contribute to Serbia’s interest, and damaging Kosovo.

1. Hybrid threats as a new phenomenon in the world

1.1 Hybrid threats definition

When there is a case of appearance of the term which in organized manner and with a plan, and at the same time in a symmetric and asymmetric way, this combinations imposes the need for a new definition: "hybrid war". The expression “hybrid war” began to form about the expression “hybrid threat”, which in November 2008 the American general George Kaysy in an informal manner defined it as “Changeable and dynamic combination of conventional, irregular, terrorist and criminal Possibilities”.

As defined by “European Energy – Information Sharing & Analysis Centre (EE-ISAC)”, the hybrid threats can be defined as a combination of violent and subversive activities, conventional and nonconventional methods (like the diplomatic, economic, and technologic methods), which are used in a coordinated manner by state and non-state actors to achieve a specific goal, event that they remain in the officially declared war.

1.2 International institutional respond against hybrid threats

Parliamentary assembly of NATO, respectively the Commission for Civil security dimension in March 2018, among other things in the Draft Report on this field, says that the use of hybrid techniques by Moscow is not accidental and it is not spontaneous. This presents, according to this report, a well planned strategy, financed and coordinated, as well.

Otherwise, NATO has established the Excellency Centres to resist the hybrid threats. So, it has built important intergovernmental mechanisms to enable states and societies (NATO non-member, as well) to fight in the non-declared war. The authors Eugenio Cusumano and Marian Corbe, consider the civil-military respond against these threats, by increasing the Excellency Centres, and decreasing the formal structures in the NATO headquarters.

---

1 Gjorgji Velovski, Revista Globi, see http://www.mod.gov.mk/?shtit=%D1%85%D0%B8%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0-%D0%B2%D0%BE%D1%98%D0%BD%D0%B0&lang=sq, publikuar më datë 23.06, 2014.
2 Burim Ramadani, ekspert i sigurisë, see https://lajmi.net/cka-jane-kercenimet-hibride/
The NATO and the most powerful states’ reaction, with USA came as a result of the war in terrain in Afghanistan between the American forces and the Taliban forces or the Israeli army with the forces of “Hezbollah”. The reforms of transition to democracy and market economy initiated by the Washington Consensus after the fall of communism have lagged behind in the Western Balkans and they have yet to undergo transformation towards the EU (Matoshi & Mulaj, 2019: 180).

2. Kosova is permanently being under the threat of Serbia

2.1 Kosova is not excluded by the hybrid threats

The security of one country is a systematic action. In order the security to work as a principle structural element of the society it is necessary that each state to determine its security politics, which is derived by the security condition. The security in the case of Kosova, which is still in an open conflict with Serbia, and the latter is not excluded of developing hybrid threats. në rastin e Kosovës e cila ende ka konlikt të hapur me Serbinë, nga kjo e fundit nuk this is as a result of the new geostrategic circumstances in Western Balkans, Serbia cannot imagine of turning back to war in relation to Kosova.

Kosova is being exposed more than the other countries of the regionto hybrid threats because of the crisis and the political polarization, the absense of he sovereign authorities for security inpolitics, its fragile economic conditions, rule of law, public security. In international plan, being not recoginzed as an independent country, and being out of the international organizations for security, present some pre-conditions that threat the securiyt of Kosova.

2.2 Are there any Serbian spies in Kosova?

There is no doubt that the nationalistic political Serbian essence, comes from the century tradition of using violence in systematic manner against Albanian elemtn all over Balkans, and wider. During the international administration Serbia wa very active in Kosova. The increasement of the Serbian service in Kaosovo has a purpose of introducing distrust to KFOR, UNMIK, international police, Police of Kosova, and other local bodies and institutions.

Former Serbian exponents have openly said with numbers during the statements given in the trial of the former prime minister Ramush Haradinaj a the Hague Trial, that they had spies in the UCK, too, which were about 200. The former chief of the analytics of the Serbian secret service, Zoran Stioviq, said this when witnessed against Ramush Haradinaj in Hague. The spy action, like in every other country in Kosova, as well, are considered illegal. Article 124, who ever that communicates the state secret, hands or makes approachable to a foreign country, foreign organization os to a person that serves the others, is sentenced to prison from five (5) to twelve (12) years in prison.

3. The lack of a platform for reading hybrid threats

3.1 Insufficient legal infrastructure

---

3 Gjorgji Velovski, “Kombinimiimundësivekonvencionale, tëparregullta, terroritedhekriminale”, RevistaGlobi, publikuar n faqeelektrinike me 23.06.2014.
5 Fisnik Sadiku, “Të kuptuarit e sistemeve të inteligjencës”, Mitrovicë, 2015, faqe 197.
8 Ramadan Qehaja, “Çështjet e Sigurisë Nacionale të Kosovës”, Prishtin;, 2004, faqe 75.
9 Po aty faqe166.
10 Shih më gjerësisht Kodin Penaë të Republikës së Kosovës.
The security condition is formed by many factors and indicators. They show the security condition, the issues related to order in public, crime dynamic, and which has an impact on personal security, the security on property belonging to citizens and those as a property belonging to the society, the impact of the foreign element on the internal security, threats coming from extremist organizations, development of the self-security in the region and the world, international relations of the country, etc.\(^\text{11}\) In the intelligence and counterintelligence field in Kosova is acting the Kosova Intelligence Agency (AKI). AKI collects information on threats against the security in Kosova.\(^\text{12}\)

In relation to possible activities of the AKI employees against the interests of Kosova, and in the interest of other neighbour countries, is working the General Inspector of AKI. According to the law for AKI, article 10 line 1, the General Inspector inspects AKI’s activities. The General Inspector is responsible for offering a function to internal control in AKI while reviewing AKI’s activities, initiating inspections, audits and investigations, reviewing complaints in relation to AKI’s activities, or filed by persons in Kosova.\(^\text{13}\)

Another institution that does not have executive competencies, but rather an informing and counseling role, is the Secretariat of the Security Council of Kosova. The Secretariat of the Security Council prepares reports on relation to security condition for the Government and the Security Council. As in the old strategy, in the new strategy, as well, there is nothing specifically for reading hybrid threats. On the other hand, the other institutions of Kosova until now did not prepare any special platform for reading hybrid threats. By the Security Secretariat of Kosova there were only some attempts like meetings and conversations that the employees had with the high representatives of the Government, but there was no initiative or a specific proposal.

4. **Conclusion**

Even that Kosova has political crises very often, crises related to the Government and constitutional ones, as well, until now has been no action by security and intelligence institutions to present evidence that eventually a relevant politician of Kosova, or another person that has influence in public is cooperating with Serbia, nad that had a main and secondary access in causing these crises or these various problems.

Kosova’s institutions have achieved to adopt the new Strategy for the Security, but on it the hybrid threats are not mentioned that much.

Kosova does not have a special platform about reading hybrid threats, and this is why the government institutions should initiate as soon as possible the creation of the special platform through which the intelligence institutions will easily note, read, identify the actions or accesses of the specific persons, including the specific politicians.

Kosova does not have a special institution to work only on revealing espionage that goes in the interest of Serbia, something that North Macedonia with the Agency for security and intelligence, which works on identification of the espionage element. This is why it is necessary to create a special Agency for external espionage only.

5. **Literature**


\(^{13}\)Same, article 10, line 7.
Information security and feeling of public insecurity in covid-19 pandemic circumstances

Ahmet Nuredini

1 AKSP, Vushtrri

{ahmetnuredini1@gmail.com}
Abstract. This paper aims to present a model of information security in the context of the global pandemic "COVID-19". The world today is facing the "COVID-19" virus that made life difficult for citizens and created the sense of insecurity for the public around the world. The global pandemic "COVID-19" created a challenging situation in all areas, especially in the field of public safety. This situation challenged the work of educational, economic and in particular the work of health and security institutions. Criminals of various profiles are exploiting the fear and insecurity from the pandemic, especially those dealing with cybercrime such as hackers and cyber criminals who are taking advantage of the situation to attack computer networks, information systems, businesses and even global organizations. With the spread of the coronavirus, the security of information in Kosovo and the world has been endangered, because many profiles that spread false news have been created and are mainly related to the new virus, or even individual cyber-attacks and attacks on various companies have been activated. The transfer of work from home to the office on one hand has created facilities and security for employees because the fact that they work from home offers greater security and prevents their infection with the virus "COVID 19" but on the other hand it was followed by the risk of information security. Initially hackers attempted to access various organizations through workers who work from home, because at home the infrastructure for work is weaker. Keywords: security, information, crime, cyber, covid-19.

Introduction

The information dates back from the development of human society. The need for information was present in all periods during development of the society.

It is well known that today, information with the information of society is passing at a later stage, even, it may be said that we now live in the society of As Rifkin points out, “We are not entering the era of access to service and a network and selection in a series of transfer activity takes place in space cybernetics and computer networking ”14.

The information and information security presents the most important asset of all organizations and security agencies in general and national security in particular.

However, there is a need for an increased security of systems, due to various attacks on computer systems and networks, this as a result of identified weaknesses on current information technologies by the perpetrators. The criminal offences related to the security of the information, represent the most serious challenges not only for the national security and its institutions and agencies, but also for international security agencies and global security.

The issue of existing problems related to information and criminal offences related to information security, represent the most serious challenges not only for the security agencies and national security of a country, but also for the international security agencies and global security.

More specifically, the information security is exposed towards threats by criminal offences related to information security, committed by various subjects in different forms, among others by unlawfully using the technology and communication network.

While the criminal offences against the information security are not categorised as traditional criminal offences, they are present in our society. It is a disturbing fact that the criminal offences related to information security are more distinct and in conjunction with other criminal offences such as: cybercrimes, terrorism, organized crime, fraud, threats and other criminal offences that are punishable in Kosovo.

Based on the higher risk that the criminal offences present against information security, all state mechanisms in general and security agencies in particular, need to develop their information defence architecture and its security. In this aspect, the purpose of securing the information is to ensure the availability of data system and confidentiality, so to disable unauthorised access to information and to preserve the confidentiality of information during its transmission through data verification and integrity.

The definition and relevance of information

Information is a notification that we receive for something; for data of the work status in a specific field; for someone’s activity or for an event.15 The term information derives from Latin (information), meaning to give form, notification, explanation, education. In general, information is any sort of notice or

---

14 Rifkin, 2001: 221
15 Glossary of today's Albanian language 1980:721
description, written or verbal communication. The availability of information, familiarizing with the
information, and its efficient use, would serve in reaching objective and efficient decisions in the field that
each institution, organization or individual covers.

Information security

The value of information derives from its owned characteristics. When a characteristic of an
information changes, it increases or decreases the value of information. The characteristics qualified as
critical are the availability, the accuracy and the authenticity of information.

Information security can be defined as defending information from unauthorised access, transfer,
modification and destruction by accident or intent of information that one organization or institution
possesses. The aim of information security is to ensure the availability of systems and data; to ensure the
confidentiality of information in order to disable unauthorised persons in accessing; to ensure
confidentiality of information during its transmission; and to ensure data authenticity and integrity.

Lastly, information security consists in defending from a wide range of threats towards
information and its critical elements of confidentiality, integrity and availability as previously noted.

Threats towards information security

In the aspect of security information, the threat is described as an object, person or other subject
outside institution that presents a continuous risk for a specified asset of information. The information
security may by threatened severely also within the institution, through inappropriate politics applied in
processing and storing information, from negligence in maintaining electronic equipment, also from human
error at work.

Threats facing information security may be considered as threats coming from outside and inside sources.
The latest digital technology inventions enabled use information technology to commit criminal offences
related to information security. The growth of electronic industry, expansion of computer production and
purchase by consumers increased the probability of new forms of these criminal offences, while cybercrime
reached a global character. Some of the criminal offences are known as cybercrimes such as: hacking,
development and distribution of viruses, software privacy, illegal downloading, identity theft etc.

Criminal justice aspect of criminal offences related to information security

Comparative aspects of criminal offences related to information security with special emphasis on
the analysis of criminal offence elements

The Criminal Code provides fifteen criminal offences related to information security. It is
distinctive that some of the criminal offences are directly related with the information security, while other
criminal offences are indirectly related to the information security. The criminal offences related to
information security foreseen in the Kosovo Criminal Code are as follows:

Espionage

The criminal offence is carried out when; whoever communicates, hands over a State secret or
makes a State secret accessible to a foreign country, foreign organization or to the person serving them;
whoever creates or directs an intelligence service, collects classified data and supports such service that
works for a foreign country or organization operating in Republic of Kosovo.  

Disclosure of classified information and failure to protect classified information

According to article 132 of Kosovo Criminal Code, the offence is described as an illegal action
consisting of disclosing or failing to protect classified information. The definition provides that the offence
is committed in two instances. In the first instance, the offence is performed when the person discloses the
classified information, while in the second instance the offence is committed when the classified
information is not protected by the person and the failure to protect enables unauthorised persons to be
informed or have access to the information. 

---

16 Kosovo Criminal Code, article 131.
17 Kosovo Criminal Code, article 132.
Infringing privacy in correspondence and computer databases

Based on article 202 of Kosovo Criminal Code, the offence is described as an illegal action consisting of opening a letter, telegram, facsimile or some other sealed document, package or electronic communication of another person or in any other way that violates the privacy of such materials or, without authorization, withholds, conceals, destroys or delivers to another person a letter, telegram, facsimile, or package of another person.\textsuperscript{18}

Unauthorized disclosure of confidential information

According to article 203 of Criminal Code, the offence is described as illegal action consisting of unauthorised disclosure of confidential information by the attorney, a defence counsel, physician or any other person that became aware of while exercising his or her profession and that he or she is under legal duty to maintain as confidential.

Intrusion into computer systems

Intrusion into computer systems it is considered the illegal action that comprises a criminal offence when, whoever, without authorization and with the intent to obtain an unlawful material benefit for himself, herself or another person or to cause damage to another person, alters, publishes, deletes, suppresses or destroys computer data or programs or in any other way intrudes into a computer system.\textsuperscript{19}

Misusing official information

According to article 423 of Kosovo Criminal Code, it is considered the illegal action that comprises a criminal offence when an official person misuses official information with the intent to acquire any undue gain or advantage for himself or herself or another person.

Disclosing official secrets

According to article 423 of Kosovo Criminal Code, it is considered the illegal action that comprises a criminal offence when an official person who, without authorization, communicates, sends, or in some other way makes available to another person the information which constitutes an official secret or obtains such information with the intent to convey it to an unauthorized person.

Criminal offences related to information security committed by use of information of technology

The latest digital technology inventions enabled use information technology to commit criminal offences related to information security. The growth of electronic industry, expansion of computer production and purchase by consumers increased the probability of new forms of these criminal offences, while cybercrime reached a global character. Some of the criminal offences are known as cybercrimes such as: hacking, development and distribution of viruses, software privacy, illegal downloading, identity theft etc.

Cybercrimes

Cybercrimes are one of the main threats for global and national security in general, and for the information security in particular.

The cybercrime is described as use of the computer, computer system or its applications in committing an illegal activity. The computer equipment may be used to commit crimes in three ways: as a tool, target of a crime and as a tool and a target of a crime.

Criminal offences related to security of information, foreseen in the law on prevention and fight of the cyber crimes

The criminal offences related to cybercrimes in Kosovo are sanctioned under specific law- Law on Prevention and Fight of the Cyber Crimes that foresees fifteen criminal offences.

\textsuperscript{18} Kosovo Criminal Code, article 202.
\textsuperscript{19} Kosovo Criminal Code, article 339.
Feeling of public insecurity in covid-19 pandemic circumstances

The Covid-19 coronavirus outbreak has now become a global pandemic. Although it now appears to be slowing in China, the spread of the disease is accelerating elsewhere, with the World Health Organization recently describing Europe as its current ‘epicentre’. Governments are reacting in ever more dramatic ways, closing borders, imposing lockdowns and travel restrictions, shutting schools and colleges, and banning mass gatherings such as sporting events.

Stay-at-home orders (lockdowns) have been deployed globally to control COVID-19 transmission, and might impair economic conditions and mental health, and exacerbate risk of food insecurity and intimate partner violence. The effect of lockdowns in low-income and middle-income countries must be understood to ensure safe deployment of these interventions in less affluent settings.  

The way the crisis will run from here cannot be known. But alongside the tragic human toll, it is already having considerable economic impacts, posing major challenges to the global supply chain and certain business sectors such as airlines, travel and leisure, and causing significant stock market volatility and some precipitous falls.

Speaking of technology, the crisis could also be the spur to look at moving more systems and applications to the cloud - an area that insurers have lagged other sectors in. With more people working remotely, having systems in the cloud offers much greater bandwidth and capacity than if staff are accessing on-premise servers remotely. This is an opportunity for the insurance industry and could be the catalyst for this movement. Actuarial modelling software, for example, often sits on individuals’ computers, as there are deemed to be security issues with putting it in the cloud.

Cyber security in the time of coronavirus

Cybercrimes are one of the main threats for global and national security in general, and for the information security in particular.

The cybercrime is described as use of the computer, computer system or its applications in committing an illegal activity. The computer equipment may be used to commit crimes in three ways: as a tool, target of a crime and as a tool and a target of a crime.

As concerns regarding the COVID-19 pandemic grow, computer hackers are taking advantage of the situation to launch cyberattacks, spreading insidious viruses of a different sort.

A huge percentage of personal laptops, printers, and other devices on home networks have malware. The flight to “work from home” is opening up many doors and windows for the bad actors to gain access to corporate networks and sensitive data. My concern is that we’re potentially going to have a wave of cyber incidents coming in the wake of the coronavirus pandemic.

COVID-19 has brought to the public conscience that a workforce shift from office based to more remote work arrangements are likely more permanent than temporary. One repeated issue that’s come up is the increase in false positives in intrusion/risk alerts and complexity in filtering the false positives from actual positives. Understanding different scenarios that exist with remote working arrangements (for example, a higher number of false positives due to work systems and infrastructure access shifting from the office to home, hackers using the disruption in normal work patterns to hide intrusion activities, etc.) will help prepare in defining the right processes and picking the right systems.

COVID-19 may present a present data security crisis, but the truth is, these threats existed before the pandemic. Current circumstances only underline the importance of an organization’s BCP, incident response plan, disaster recovery plan and other security monitoring plans – and of course picking the right critical software platforms and providers that are adept at responding to a data security incident while


minimizing business interruption, including those that effect personnel. The cybersecurity rules that were applicable prior to the COVID-19 are still in effect now. Cybersecurity laws, regulations and procedures have not been lessened as a result of this, and there is no indication that enforcement will be curtailed or suspended at this time. The appropriate response to the COVID-19 from a cybersecurity perspective is to continue to enforce basic good cyber policies, procedures and auditing.  

**Coronavirus phishing.**

COVID-19 has opened a gate to hackers using the current circumstance for nefariously purposes. Creation and spread of viruses. The basic feature of this work is the creation and dissemination of these destructive programs, the possibilities of which are the promotion and transfer of forms of various lesions in the systems where those viruses are found. It is clear that phishing is any process designed to extract datapersonal by the targeted victim. This is often done by e-mail. "A scenario of may include the author of the work, who has created a fake website, designed to look like a legitimate website, and a financial institution."  

As with other major world events, the COVID-19 outbreak represents an opportunity for malicious actors, from simple scammers to government-backed hacker groups. Individuals and businesses worldwide are now being targeted by phishing campaigns designed to play on fear of the virus and of the lack of reliable information on the outbreak. Extra vigilance should be exercised by all regarding any communication, hyperlink, attachment or request for information relating to coronavirus. Warning your employees about this will reduce the threat to them and to you.

Employees are human, and the news and media are full of stories of those susceptible to targeted phishing, fraud and other cybercriminal activities solely based on trying to get information on COVID-19, or interests and concerns relating to the pandemic. While the topic of COVID-19 may be new, the techniques and messages used to entice individuals to click malicious links often remain similar to other scams that are constant and persistent on the internet. Use the interest and fervour around COVID-19 as another driver for security awareness by alerting employees or others to these risks.

**CONCLUSIONS**

Based on the complex analysis and study of the security of information in general and the criminal offences related to information security in particular we have reached several conclusions and recommendations that according to my opinion are useful and are presented as follows:

- Information and its security jointly followed the evolution of the society.
- Currently, the modern society confronts the greatest technical-technology achievements. The increased use of information technology in general and the internet in particular, including the tendency of having a networking society, raise the risks that we confront today. The development of information technology and use of internet in this modern society enabled premeditated misuse of such achievements by facilitating possibilities in committing criminal offences against the information security.
- The information and information security area, requires national and international cooperation and coordination, so to guarantee the information security. The information security is a concern for all users of information technology in the society. Specifically, the information security is a priority issue in the society.
- The information security is an obligation for the entire which can be achieved by building national and international cooperation bridges in harmonizing legislation and joint effort in ensuring global information systems, furthering developments of politics and procedures in combating cybercrimes.

---

23 https://www.episerver.com/guides/covid-19-privacy-considerations
24 Vula, 2010: 105
25 Eastom & Taylor, 2011: 6
Criminal offences against information security require a specialized approach by the criminal justice institutions, law enforcement agencies and prosecution office. Therefore, these institutions need to develop their capacities in order to effectively increase investigation in securing electronic evidences related to these criminal offences.

The Kosovo legal frame in the field of information security has essential similarity with the EU legislation in general, and the Slovenian legislation in particular.

Considering the fact that criminal offences against information security endanger all potential users of information technology equipment and users of internet, therefore wide-ranging information sources are suggested through training and education especially for the youth, families, schools, civil society, and state institutions.

The success in prevention of criminal offences related to information security depends largely in the degree of received information and knowledge of the youth in potential risks from the crimes committed through unauthorized use of technology and communication.

The most practical forms to institutionalize a competent information for the society in general and the youth in particular, is to receive information on criminal offences related to information security, organizing joint workshops with representatives of civil society, media and security agency officials, organizing of awareness campaigns on internet proper use.

The cybercrimes are mainly committed by persons having an advanced knowledge of computer systems, mainly through computer technology.

Bibliography

- Vula V., (2010), Kriminaliteti kompjuterik, Shtypshkronja "Koha" Prishtinë".
- Kosovo Criminal Code,
- Glossary of today's Albanian language 1980

Siguria Kombëtare -- Konferencat -- 2020 -- Prishtinë (Kosovë)


Aleph [000098109]
CHAPTERS:
- Computer Science and Communication Engineering
- Management, Business and Economics
- Mechatronics, System Engineering and Robotics
- Energy Efficiency Engineering
- Information Systems and Security
- Architecture - Spatial Planning
- Civil Engineering, Infrastructure and Environment
- Law
- Political Science
- Journalism, Media and Communication
- Food Science and Technology
- Pharmaceutical and Natural Sciences
- Design
- Psychology
- Education and Development
- Fashion
- Music
- Art and Digital Media
- Dentistry
- Medicine & Nursing
- Sports, Health and Society
- Security Studies
- Language and Culture


Lagija Kalabria  p.n  KS - 10000, Prishtinë
+383 38 541 400
+383 38 542 138

www.ubt-uni.net
conferences@ubt-uni.net