RABEK

GLOBAL SECURITY

5th INTERNATIONAL SCIENTIFIC - PROFESSIONAL CONFERENCE

Proceedings SeCMan - 2019

SECURITY AND CRISIS MANAGEMENT -THEORY AND PRACTICE

SeCMan 2019

PROCEEDINGS

BELGRADE 2019

FOREWORD

*A forum **Safety for the Future** arose out from the idea and the need to see security problems as a whole, and yet separately, through a prism of scientists and experts in order to bring science, company practice and economy together. This year, we are conducting the forum for the fifth time, with new elements of security phenomena researches in the area of management, engineering and ecology. A spectrum of phenomena which have an influence on a particular subject becomes wider and wider. Namely, it is a fact that environment, in which individuals and legal entities exist, becomes more complex. It is consist of familiar and unfamiliar circumstances. Managing those circumstances is possible to a certain extent, if there is an optimal and necessary quantum of knowledge. Hence, the knowledge is foundation on which is necessary to build capabilities of individuals and legal entities in order to be able to recognize, prevent and react on threats.*

Crisis management has become everyday need, essential for survival of an individual, companies or society as a whole. It is more and more difficult to assess the risk of events with negative effects at the very beginning of their occurrence, and coping with negative consequences leaves harder effects on society. Scientific research of security phenomena has become priority of society sustainable development.

Scientific findings do not always come to those who perform security tasks, such as individuals or legal entities. Therefore, there is a need for scientists and experts to meet and exchange ideas, opinions and knowledge. Materialization of knowledge is carried out daily in the process of modern business. Exposed to the impacts of a turbulent environment, and focused on sustainability, modern business requires permanent monitoring of changes and adaptation to these changes.

Comprehension of the environment in which the modern society exist, is possible if there is the necessary knowledge of the phenomena that characterize it. Only knowledge provides an opportunity of preventive action through an efficient risk assessment system. Only knowledge, formed as a symbiosis of science and profession, has quality and strength, which guarantees the possibility of preventive action and an optimal level of readiness to react to negative events. The resistance of contemporary society to negative events depends on the degree of knowledge development.

Proceedings from the 5th International Conference - Security and Crisis Management - Theory and Practice, presents a new value in the observation of a portfolio of security phenomena at the strategic, company, and individual level. The papers published in the proceedings are new findings and views of the author. A wide range of issues, confirms the assumption of the necessity of such a conference. The papers presented at the last four conferences have unambiguously demonstrated the need for regional cooperation and the harmonization of joint capacities.

The papers within Management-Engineering-Ecology conference give the proceedings particular quality. These papers are, in the proceedings, given through special section. The complexity of working and any other environment inevitably links management and engineering elements. The need of application of engineering methods in management processes arises.

The exhibition part of the event and practical demonstration exercises aim to ensure that consumers of implemented safety show new achievements and opportunities in solving various security problems. The intention of the organizer is, by carefully selecting the theme for demonstration exercises, to trace the way of applying the principles of practicality and the

obviousness in the process of education and training the individuals to respond in different situations.

The proceedings represent a review of existing knowledge, source of a new one, assistance in solving security problems, a support for practitioners dealing with security and a source of initiative to advance existing knowledge in the field of security and crisis management. By this way, we invite all stakeholders to improve the quality of the future editions with their work.

Program Committee

PROGRAM COMMITTEE

PhD Branko Babić, *The Higher Education Technical School of Professional Studies, Novi Sad – Chairman*
PhD Darko Božanić, *Military Academy, University of Defense in Belgrade, Serbia*
PhD Marijan Brozović, *Karlovac University of Applied Sciences, Croatia*
PhD Gian Luigi Cecchini, *Full Professor of European Union Law, University of Trieste, Italy*
PhD Aleksandra Dimitrovska, *Expert on the psychology of national security, North Macedonia*
Phd Sinisa Domazet, *Faculty of Security Studies EDUCONS, Educons University in Novi Sad, Serbia*
PhD Bojan Đorđević, *Faculty of Management in Zajecar, Megatrend University, Belgrade, Serbia*
PhD Tatjana Gerginova, *Faculty of security Skopje, North Macedonia*
PhD Ljubomir Gigović, *Military Academy, University of Defense in Belgrade, Serbia*
PhD Emina Hadžić Drežnjak, *Faculty of Civil Engineering, University of Sarajevo, Bosnia and Herzegovina*
PhD Predrag Ilić, *Institute for Protection, Ecology and Informatics, Banja Luka, Republic of Srpska, Bosnia and Herzegovina*
PhD Željko Ilić, *Republican administration of civil protection Republic of Srpska, Bosnia and Herzegovina*
PhD Vladimir Jakovljević, *Faculty of Security Studies, Belgrade, Serbia*
PhD Aco Janićijević, *Accreditation Body of Serbia, Belgrade, Serbia*
PhD Samed Karović, *Faculty of Security Studies EDUCONS, Educons University in Novi Sad, Serbia*
PhD Dalibor Kekić, *University of Criminal investigation and Police studies, Belgrade, Serbia*
PhD Savo Kentera, *Atlantic Council of Montenegro, Podgorica, Montenegro*
PhD Nenad Komazec, *Military Academy, University of Defense in Belgrade, Serbia*
PhD Tomaž Kramberger, *Faculty of Logistics Celje, University of Maribor, Slovenia*
PhD Mirjana Laban, *Faculty of Technical Sciences, University of Novi Sad, Serbia*
PhD Goran Maksimović, *Security research center, Banja Luka, Republic of Srpska, Bosnia and Herzegovina*
PhD Marina Mihajlović, *Innovation center of The Faculty of Technology and Metallurgy, University of Belgrade, Serbia*
PhD Marina Mitrevska, *Faculty of Philosophy, Institute for Security, Defense and Peace, Skopje, North Macedonia*
PhD Dragan Mlađan, *University of Criminal investigation and Police studies, Belgrade, Serbia*
PhD Nenad Mustapić, *Karlovac University of Applied Sciences, Croatia*
PhD Vesna Nikolić, *Faculty of Occupational Safety, University of Niš, Serbia*
PhD Dragan Pamučar, *Military Academy, University of Defense in Belgrade, Serbia*
PhD Ruggiero Cafari Panico, *Full Professor of European Union Law, University of Milan, Italy*

PhD Slobodan Radojevic, *Military Academy, University of Defense in Belgrade, Serbia*
PhD Tomislav Radović, *Faculty of Management in Zajecar, Megatrend University, Belgrade, Serbia*
PhD Aca Ranđelović, *Military Academy, University of Defense in Belgrade, Serbia*
PhD Aleksandar Milić, *Military Academy, University of Defense in Belgrade, Serbia*
PhD Momčilo Sakan, *Independent University of Banja Luka, Republic of Srpska, Bosnia and Herzegovina*
PhD Slobodan Simić, *Security research center, Banja Luka, Republic of Srpska, Bosnia and Herzegovina*
PhD Augusto Sinagra, *European Union Law, University of Rome „La Sapienza", Italy*
PhD Miomir Stanković, *Research and Development center „Alfatec" Niš, Serbia*
PhD Katarina Štrbac, *Director of the Directorate for European Integration and Project Management at the Ministry of Defense of Republic of Serbia, Belgrade, Serbia*
PhD Jovan Vučinić, *Karlovac University of Applied Sciences, Croatia*
PhD Marija Vukić, *Research and Development center „Alfatec" Niš, Serbia*
Msc Nada Marstijepović, *Maritime faculty Kotor, Montenegro*
Tatjana Bojanić, *Institute for Standardization of Serbia, Belgrade, Serbia*
Velizar Čađenović, *Firefighting Association of Montenegro, Montenegro*

ORGANIZING COMMITTEE

MSc Milica Mladenović, S4 GLOSEC, Global Security, Belgrade, Serbia, Chairman
MSc Aleksandra Ilić, S4 GLOSEC, Global Security, Belgrade, Serbia
Mr Branislav Milosavljević, Institute for Strategic Research, University of Defense in Belgrade, Serbia
MSc Aleksandar Petrović, Military Academy, University of Defense in Belgrade, Serbia
Mirko Ilić, Fire Brigade of Vojvodina, Serbia
Ana Kostadinović, RASEC, Belgrade, Serbia

IMPRESSUM

Editorial
Komazec Nenad, PhD, Military Academy, Belgrade, Serbia
Babic Branko, PhD, VTS Novi Sad, Serbia

Publisher
Regional Association for Security and Crisis Management
S4 GLOSEC Global security doo

Reviewers
Vucinic Jovan, PhD - Croatia
Mustapic Nenad, PhD- Croatia
Kramberger Tomaz, PhD- Slovenia
Karovic Samed, PhD -Serbia
Strbac Katarina, PhD – Serbia
Pamucar Dragan, PhD-Serbia
Stankovic Miomir, PhD- Serbia
Babic Branko, PhD-Serbia
Mladjan Dragan, PhD- Serbia
Randjelovic Aca, PhD – Serbia
Simic Slobodan, PhD - Bosnia and Herzegovina
Jurisic Dragisa, PhD- Bosnia and Herzegovina
Bozanic Darko, PhD – Serbia
Komazec Nenad, PhD – Serbia
Maksimovic Goran, PhD - Bosnia and Herzegovina
Tatjana Gerginova, PhD - North Macedonia
Aleksandra Dimitrovska, PhD - North Macedonia

Design
Mladenovic Milica, MSc
Komazec Nenad, PhD

Edition
60 copies

The press:
Štamparija Donat Graf, Grocka, Belgrade

ISBN
978-86-80692-04-3

Note:
The authors opinions expressed in this book do not necessary reflect the views of the institution in which they are employed

CONTENT

V INTERNATIONAL SCIENTIFIC CONFERENCE
SAFETY AND CRISIS MANAGEMENT – THEORY AND PRACTISE
SAFETY FOR THE FUTURE – SecMan 2019.

GEOGRAPHY IN GEOSPATIAL INTELLIGENCE - C4IRS AND CYBER SECURITY

PhD Aleksandar Petrovski[1], PhD Nenad Taneski[2], PhD Dimitar Bogatinov[3]
[1] University "Goce Delchev" Shtip, Military academy "General Mihailo Apostolski" associated member, Skopje, Northern MACEDONIA
[1] University "Goce Delchev" Shtip, Military academy "General Mihailo Apostolski" associated member, Skopje, Northern MACEDONIA
[1] University "Goce Delchev" Shtip, Military academy "General Mihailo Apostolski" associated member, Skopje, Northern MACEDONIA

Abstract: *Information in 21st century represents power, and with that, safest and most legitimate "machine for dominating". Since ancient times, people have used maps to represent information about real places. This allowed them to visualize and think about these places while not actually being physically present. Information becomes displayed at a reduced scale organized by a cartographer. It expresses a view of extensive regions impossible to see from a single vantage point and communicates information about the represented space. Consequences from the rapid growth of information technologies and their usage for army purposes make information one of the key concepts of the unconventional warfare. Application of Geography in the Army for getting information is wide used all over the world, but this paper gives an overview and make particular ideas for further development in usage of GIS for geospatial intelligence - C4IRS and Cyber security. Today, in western societies, more people are employed collecting, handling, and distributing information than in any other occupation. Computers, optical fiber, copper wire, and electromagnetic waves link people to the vast array of information handling devices. Our society is truly an Information Society. Our time is the Information Age.*

The main aim is getting specific information about objects, buildings and devices on the ground through geo-location and plots field data (various digital, video images), further management and planning strategies for ensuring proper cyber security, and also in other way, getting information from the intelligence services based on the information from the C4IRS. In this paper, despite the overview of usage geography for geo-reconnaissance in army, is presented an application for the soldiers on the battlefield for live streaming (drones and video camera) and live processing of the decisions from their commands, getting real time track log with moving map (through a GPS signal), which displays their current coordinate location, and their protection in cyber space of heading directions given by their commanders. The development of this kind of application based on GIS will make a breakthrough in geospatial intelligence, helping in the everyday life.

Keywords: *Geography, cyber, geospatial, security, GIS.*

1. INTRODUCTION

None of the most important weapons transforming warfare in the 20th Century –the Airplane, Tank, Radar, Jet Engine, Helicopter, Electronic Computer, not even the Atomic Bomb –owed its initial development to a Doctrinal Requirement or Request of the Military." [1] Since ancient times, people have used maps to represent information about real places. This allowed

them to visualize and think about these places while not actually being physically present. Information becomes displayed at a reduced scale organized by a cartographer. It expresses a view of extensive regions impossible to see from a single vantage point and communicates information about the represented space. Today, in western societies, more people are employed collecting, handling, and distributing information than in any other occupation. Computers, optical fiber, copper wire, and electromagnetic waves link people to the vast array of information handling devices. Our society is truly an Information Society. Our time is the Information Age. One interpretation, made by Thomas M. Barnett's that "connected" societies require less need for US military interventions (figure 1). [2] Barnett draws on a fascinating combination of economic, political, and cultural factors to predict and explain the nature of modern warfare**.**

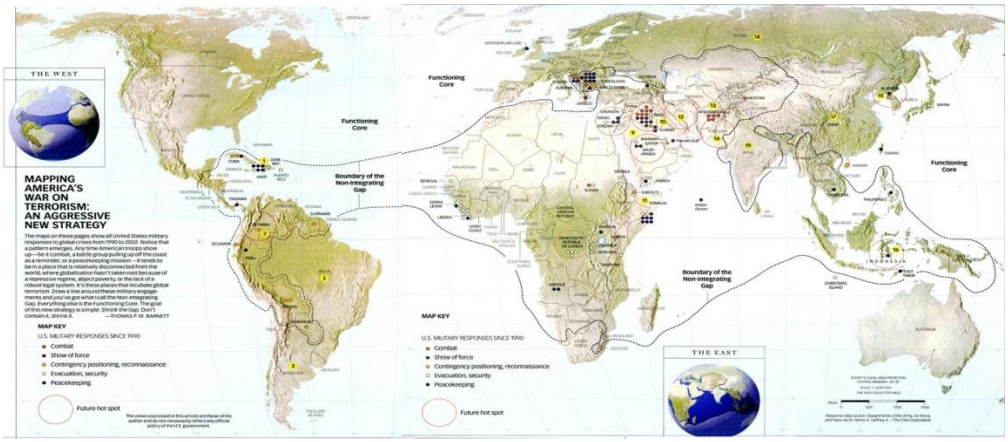

Figure 1. Thomas P.M. Barnett's original characterization of "The Pentagon's New Atlas."

This division between the connected and non-connected areas of the globe drew the association between the lack of the free flow of information and the areas where US military forces were most likely to be engaged. The author's premise is that the more "connected" the less likelihood of a need for military intervention by the US military.

In book of global theorist Parag Khanna, **Connectography: Mapping the Future of Global Civilization**, he redraws the way humanity is organized according to lines of infrastructure and connectivity rather than our antiquated political borders. This emerging global network civilization holds the promise of reducing pollution and inequality - and possibly even overcoming geopolitical rivalries, and he asks us to embrace a new maxim for the future: **"Connectivity is destiny."**

2. GEOSPATIAL INTELLIGENCE - C4IRS and CYBER SECURITY

Armies in the 21st century have to manage with difficult operations in the field of unconventional warfare. Today, battles are won in the middle of the big cities and on the computers in the operational center where the information is the most powerful tool. Buildings and streets are the new battlefield, in which every corner hides different type of danger. Soldiers have very difficult task, to observe and save themselves from the various attacks. To eliminate these dangers and transform them in favorable role, armies must change "old" topographic maps with new modern maps which allow to the armies in the world to be one step ahead of the enemy. The term "modern" map, covers, of course, not only the up-to-datedness, transparency (that is, being able to be used simply, from the user's point of view) and increasing precision, but also a higher-than- average information content that supports

military use to the greatest extent possible, considering special military aspects. [3] This is what GIS is about: to display special kind of information about specific area with unlimited amount of essential mapping information (layers), used to display the knowledge base of that area.

The term "geospatial intelligence" means- " the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth". GEOINT consists of imagery, imagery intelligence, and geospatial information." [4] Our main idea in this scientific paper is to discover, describe, explain, and interpret geographic and cyber information in order to anticipate a subject's use of geography. A outcome to this can be stated as: *Cyber information is an artifact of a subject's use of geography.* Advanced technology now provides the capability to use and combine geospatial data in different ways to create interactive/dynamic, customized visual products. It allows the analyst too quickly make more complex connections between different types of data and information than previously possible. Geospatial products can now leverage a wider variety of data, including from other INTs (such as SIGINT, HUMINT, and MASINT), through collaborative processes, to provide more accurate, comprehensive, and relevant products. GEOINT can also be combined with other INTs, such as SIGINT, to develop custom products. The result of these advances is a transformation in the analytic and technical processes used to create geospatial products. It is the cumulative effect of all these changes that propelled the evolution of the GEOINT discipline. GEOINT professionals represent and are drawn from a Aeronautical Analysis, Cartography, Geodetic Sciences, Geospatial Analysis, Imagery Analysis, Imagery Sciences, Marine Analysis, Regional Analysis, Source Analysis, The richness of available open source information, generated either by social media or other sources, is too complex to accumulate and analyze using current approaches. Analysts often use multiple sources of information to create actionable intelligence. The datasets are large in volume, and are typically stored across multiple databases in several locations. This requires queries to be pre-specified – filtering significant amounts of data before an analyst has an opportunity to decide if it's important. This query-retrieve procedure effectively removes the possibility of the "lucky find," because the analyst has to know what they want to query. The datasets are becoming more complex while the transaction costs are decreasing.

GIS is widely used in almost all the branches of the modern armies. Capabilities that use GIS are following: Command and Control, Defense mapping organizations, Base operations and facility management, Force protection and security, Military engineering, Mine clearance and mapping, Mission planning, Terrain analysis etc.[5] C4IRS defines a Command, Control, Communication, Computer, Information system, Reconnaissance and Surveillance. Geo-reconnaissance determine specific type of information gathered from the visual observation or other detection methods, which give us information's about the terrain, geographical elements of it, objects on that specific area, that can help us to create a better picture for the enemy and the resources they are using. So, one of the ways of data gathering is by aerial photographs and space images. Advantage of these kinds of collecting data is the possibility of gaining information without getting any contact with the earth surface directly, but with contacting a mediatory unit carrying information about the surface. As that kind of mediatory unit which carry an assessing equipment to gain information are today's popular unmanned aerial vehicle (UAC) commonly known as a drone. With proper equipment they can be used to observe and make live photographs of the enemy terrain. This method will reduce the usage of people risking their life for the purpose of collecting information. [6]

From the US Army's *"Cyberspace Operations Concept Capability Plan 2016-2028"* cyberspace is one of five domains; the others are air, land, maritime, and space. These five

domains are interdependent. Cyberspace nodes physically reside in all the other domains. Activities in cyberspace can enable freedom of action for activities in the other domains, and activities in the other domains can also create effects in and through cyberspace. As Figure 2 illustrates, Cyberspace can be viewed as three layers (physical, logical, and social) made up of five components (geographic, physical network, logical network, cyber persona, and persona). While these five components describe the boundaries of cyberspace, the information that flows through these components has to be recognized as unique in its own right. [7]

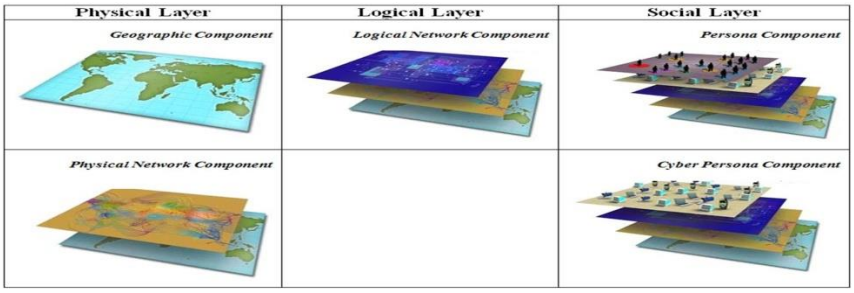

Figure 2: The Three Layers of Cyberspace (physical, logical, social) & 5 components (geographic, physical network, logical network, cyber persona, persona).

The layers of cyberspace as viewed above consist of the interdependent networks of IT infrastructures and data resident within those structures. The interdependent networks of IT infrastructures and resident data that define cyberspace exist in one or more layers of cyberspace. All the layers must be considered as they relate to the information environment, the operational environment, and the operational area. [8]

The **physical network layer** includes both geographic and physical network components. The geographic component is the physical location of elements of the network. The physical network component includes all the physical equipment associated with links (wired, wireless, and optical) and the physical connectors that support the transfer of code and data on the networks and nodes. As an example, physical networks components may include wires, cables, radio frequencies, routers, servers, computers, radars, weapons systems, telecommunications systems, personal digital assistants, and other networked devices where data is created, manipulated, processed, and stored.

The **logical network layer** consists of the components of the network that are related to one another in ways that are abstracted from the physical network. For instance, nodes in the physical layer may logically relate to one another to form entities in cyberspace that are not tied to a specific node, path, or individual. Websites hosted on servers in multiple physical locations where content can be accessed through a single uniform resource locator or web address provide another example.

The **social layer** consists of both a cyber-persona layer and a persona layer and are abstractions of the logical network, and it uses the rules of the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. This layer consists of the people who actually use the network and therefore have one or more identities that can be identified, attributed, and acted upon. These identities may include e-mail addresses, social networking identities, other web forum identities, computer Internet protocol addresses, and cell phone numbers. Cyber-personas hold important implications in terms of attributing responsibility and targeting the source of a cyberspace threat. Because cyber-personas can be complex, with elements in many virtual locations, but normally not linked to a single physical location or form, significant intelligence collection and analysis capabilities may be required.

In summary, information is the only benefit that is stolen by replication. As such, securing it is problematic because, for it to be of any use, it needs to be available for access. In USA DOD is written *"The Department and the nation have vulnerabilities in cyberspace. Our reliance on cyberspace stands in stark contrast to the inadequacy of our cyber security – the security of the technologies that we use each day."*

3. GEOGRAPHY OF GEOSPATIAL INTELLIGENCE AND CYBERSPACE

"I invoke the first law of geography: everything is related to everything else, but near things are more related than distant things'' (Tobler 1970) Tobler's statement is high-level, domain-neutral, and problem independent in scope and is problematic to evaluate empirically as a result. Keep in mind there are potential downsides (or dark sides) to use of data. Open data is not immune to exploitation. In 2016, N.A. Raymond poses a potential scenario where an NGO managing displaced persons (IDPs) allows a UN agency to publish a map showing the camps with the largest numbers of IDPs, while at the same time another NGO working to assist demobilized child soldiers allows another UN agency to provide their data in the open as well. Combined, these two sources of GeoInt enable a local armed force looking to reclaim their liberated child soldiers from the locations where their efforts will give up the greatest payback. They attack a camp and re-abduct the children based on the UN-NGO provided GeoInt. Most of the time, we concern ourselves with unlikely situation, but there are obviously other considerations.

We should recognize the tremendous power of information technology and vigorously promote its development. The melding of the traditional economy and information technology will provide the engine for the development of the economy and society in the 21st century." [9] Internet communication technologies (ICTs) play an increasingly important role in terms of how individuals express themselves and communicate with each other. Public office holders, as well those who speak to power, recognize the increasing importance of ICTs and related technologies, which combined make up the domain of cyberspace. Within the Department of Defense, it is now considered a domain equal in importance to land, air, sea, and space and is the medium through which e-commerce, e-education, e-hobbies, e-politics, and e-conflict all take place. To no one's surprise, cyberspace has become an increasingly contested space - an area of strategic geopolitical competition. Contests are frequent and occur on a daily basis, from the formation of military cyber commands (the US is not the only one to stand one up), to the filtering of social media tools by repressive regimes, to the creation of new tools and methods designed to circumvent them. The contests over and within cyberspace are the result of an increasing entanglement of competing geostrategic interests mutually dependent on and targeting a common information space. We are constantly reminded that the environment we are talking about is only several decades old, and in a short period of time it has gone through exponential growth and evolution that continues unabated.

Flouting geography challenges the idea of the sovereign nation state, and it is this challenge of the state's independence that is at the heart of many of the issues surrounding the current governance of cyberspace. It was designed as a solution to a military problem of message exchange between soldiers without letting their enemies know where they were. The resulting architecture is evolving and decentralized, and the routing of the messages has nothing to do physical locations. The shape of the network was and is in constant flux. When the Web started expanding rapidly, the growing value it provides to countries forced most governments to either accept the status quo of Web governance or form their own policies at the domestic level, risking pushback from the international community. Maintaining a network separate from the rest of the Web is a common practice where security concerns in lower-level network operations exists. From the user perspective, the abstract online world defies ties to either

geographic or political boundaries, but it does depend on physical infrastructure that has a geographic location. Every country adapts domestic and foreign policies that impact the Web, some of which can affect the activities of the user community. Strategic geopolitics is therefore interwoven into the development of these policies.

Geo-location technology is not currently 100% accurate in providing the location of an IP address. When the user's IP address is a loaded on a proxy server that doesn't expose the user's IP address, it is practically impossible to locate the physical location of the user. Some estimates place the country accuracy at about 99%. For IP addresses in the US, it is 90% accurate on the state level, and estimated at 81% accurate within a 40 km radius. Many world-wide users indicate as little as 55% accuracy within 25km.

When you use other parameters, it can get more accurate. For example, Digital Element utilizes as much information as possible from a list of available information for this uses audience segmentation capabilities and targeting based on parameters such as:

- Country
- Region/State
- City
- Zip/Postal Codes
- Custom Regions*
- Connection Type
- Mobile/ WiFi
- Longitude/Latitude
- Phone Area Code
- Time Zone/ Language
- Proxies
- ISP
- Domain
- ASN
- Confidence Factors
- Home/Business
- Industry Codes
- Company Name
- Org Name
- Demographics

Figure 3. Audience segmentation capabilities and targeting based on parameters.[10]

In line with Cyber Intelligence and Security of geo-information it might be helpful to review some of the salient points presented so far.
- Attempts to map both the Internet and where explicit knowledge is located has been frustrated by a lack of understanding of the synergies between such diverse fields as communication theory, geography, economics, GIS, and strategic studies – among others.
- Information is physical. Geospatial information references a physical location. Explicit information cannot exist without a physical infrastructure to support it. Cyberspace is created as a domain by this infrastructure and has a geospatial component as well than can be expressed as a set of septuple coordinates associated (connected) through the ICT infrastructure.
- The ICT infrastructure provides the possibility of a transaction based relationship between distant points that extends the application of Tobler's 1st Law of Geography.
- As ICT infrastructure increases, access to information increases. Social change is more likely in areas where this increase is occurring.
- There is an intelligence value to the phenomena of the messages sent over such ICTs as social media. These messages have a geospatial component.
- The intelligence value is recognized in the IC, and studies at leading universities are being funded by the IC to further the Body of Knowledge (BOK) in using new HUMINT sources found in the Open Sources.
- The current understanding and practice of Cyber Intelligence is limited to attacks and defense on the infrastructure.
- Bodies attempting to censor the flow of information tend to provide blocks on the infrastructure and ignore or are incapable of monitoring and exploiting the sources of the

communications. Needing the connectivity to function, the blocks are soon lifted when the impression of "control" seems established.

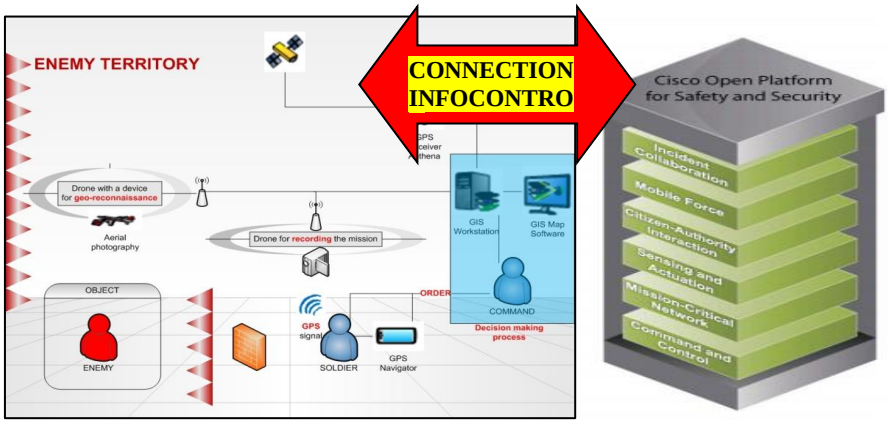

Figure 4: Model of C4IRS and CISCO Open Platform for Cyber Safety and Security Information Centar (3C2SI)

CISCO Cyber Safety and Security Information Centar (3C2SI) will give control for sensitive information in Incident Collaboration, Mobile Force, Citizen- Authority Interaction, Sensing and Actuation, Mission Critical Network, Command and Control. An application for the soldiers on the battlefield for live streaming (drones and video camera) and live processing of the decisions from their commands, getting real time track log with moving map (through a GPS signal), which displays their current coordinate location, and their protection in cyber space of heading directions given by their commanders through 3CSI.

TABLE 1: CISCO Solutions in Geospatial Network Intelligence & Cyber Space

TABLE 1: CISCO Solutions in Geospatial Network Intelligence & Cyber Space	Resiliency	Network Virtualization	Traffic Optimization	Mobility and Location	Network Management and Monitoring	Storage	Identity	Unified Communications	Compute	Application Networking	Security
Cisco IOS Software	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Cisco Wireless and Mobility Solutions				✓	✓						✓
CiscoWorks Network Management Solutions					✓		✓	✓			✓
Multilayer Data Center Solution	✓	✓			✓	✓			✓	✓	✓
Cisco Trust and Identity Management					✓		✓				✓
Cisco ISR Multiservice Routers, Catalyst Switches	✓		✓	✓	✓			✓		✓	✓
Cisco Unified Computing		✓			✓	✓			✓	✓	
Cisco Wide Area Application Services, Cisco ACE Application Control Engine, Cisco AVS Application Velocity System, Cisco Application Content Networking Solution	✓		✓		✓	✓				✓	
Cisco Self-Defending Network Solution					✓		✓				✓

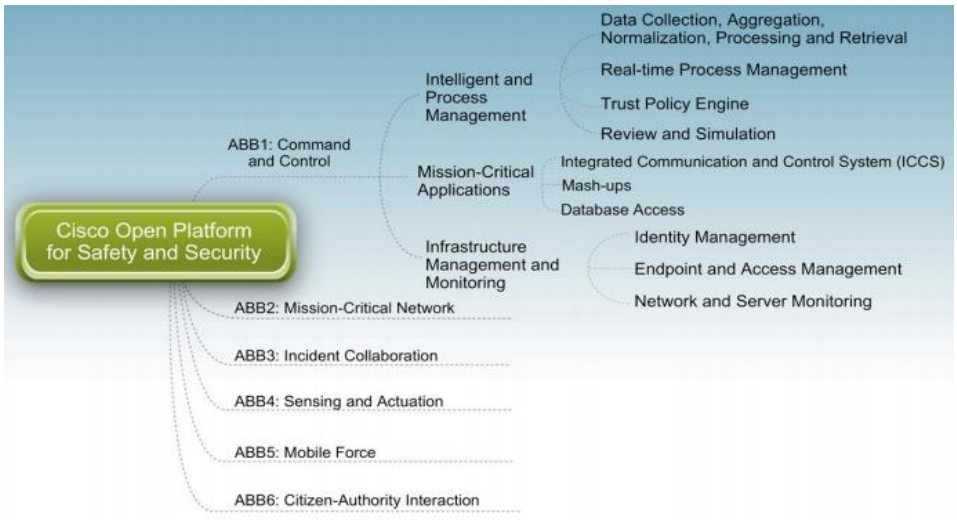

Figure 5: Processing of information in CISCO Open Platform for Cyber Safety and Security Center

5. CONCLUSION

GIS has a fast growth in today world, but his capabilities are not explored completely. The possibilities that are offered from GIS have a wide range of use, and because of it, this information system nowadays is more and more used in various fields of study. Of course that military industry discovers different ways of composing this information system in manufacturing of new devices, vehicles and weapons and also in integrating of the GIS in the existing technologies.

Some of the usage of GIS is for geo-reconnaissance and C4IRS which was previously described in this paper. These subjects are already explored and have application in armies around the world for: tracking units or soldiers, reconnaissance of the enemy's terrain, adding war-fighting symbols and tactical editing of the data from the battlefield, rapid and massive transferring of messages and orders, coordinate conversion, digital terrain elevation data information etc. A military information system based on connecting of these two powerful usages of GIS, will help the armies in the world and the decision makers for better observation on the mission or battle and giving specific orders based on the information's collected from geo-reconnaissance and live-streaming of the situation on the battlefield. . Input values for the commanders represent the data from the geo-reconnaissance i.e. the situation on the enemy's terrain and the geo-location of the own units and soldiers. The command make a decision which represents an output value of the system, and it is send to the soldiers as a voice order or as movement navigation.

REFERENCES

[1] John Chambers, ed., *The Oxford Companion to American Military History* (New York: Oxford University Press, 1999).
[2] Thomas M. Barnett in The Pentagon's New Map: War and Peace in the Twenty-first Century, Berkley Trade, 2005, ISBN 978-0425202395.
[3] Peter Nagy, "GIS in the army of 21st century", Hungary, 2004, pp587-600;
[4] http://www.fas.org/irp/agency/nga/doctrine.pdf.

[5] ESRI, "GIS for Defense and Intelligence", 2005.
[6] GIS IN ARMY: APPLICATION OF GIS IN GEO-RECONNAISSANCE AND C4IS IN ARMY PURPOSES, GEOBALCANICA 2016.
[7] The United States Army's: Cyberspace Operations Concept Capability Plan 2016-2018, TRADOC Pamphlet 525-7-8.pdf and FM 3-38.
[8] The paragraphs below are taken from FM 3-38 Cyber Electromagnetic Activities Feb 2014.
[9] (Jiang Zemin, August 2000).
[10] Based on image from USA DMA/MSA, U.K. ITV Regions, France Departments, Tim Hardie, “Distributing Authoritative Name Servers via Shared Unicast Addresses,” RFC 3258, April 2002.