Branislav Todorović,[*]
Institute for National and International Security

Darko Trifunović,[**]
Institute for National and International Security

[*] E-mail: bane@intelligence-security.rs
[**] E-mail: darko@intelligence-security.rs

DOI: https://doi.org/10.37458/ssj.1.1.1
Review Paper
UDK 351.74:004.738.5
004.6.056
Received: January 29, 2020
Accepted: May 26, 2020

SECURITY SCIENCE AS A SCIENTIFIC DISCIPLINE - TECHNOLOGICAL ASPECTS -

Abstract**:** *The paper argues the facts that the growth and expansion of its domain, in combination with its own procedures and methodologies, justifies the existence of Security Science. The paper starts with the global opinion overview of security as a scientific discipline. With the focus on technological segments, a possible scientific approach to security analysis (SA) is presented in detail. Finally, examples are provided regarding the use of mathematics modelling and tools for data analysis and interpretation in security domain.*

Keywords**:** *Security Science, security analysis, cyber security, mathematical modelling.*

1. Introduction

The decisive action is required to close various discussions over the topic whether security is an independent scientific discipline or not. One serious reason for such action would be the constant rise of risks and threats, which requires an organised methodological approach to security in all spheres of the today's society. As long as security is considered and treated only as a goal to be achieved by various activities performed by defence agencies or practitioners, or as a segment of other scientific disciplines, the lack of in-depth understanding and corresponding planning will leave open vulnerabilities in important systems, operations and functions. Such vulnerabilities area constantly challenged by terrorist organisations, natural disasters and other disruptive forces.

Throughout the human history, at some point of time the aggregated knowledge had caused some segment of science to leap to a new level or form. In this paper we are arguing the necessity of declaring security as the independent scientific discipline and providing the reasoning for that by analysing the technological aspects of security science.

Another question emerges more and more often during the last decade - *Security was initially defined as a social science discipline, but is it still so?*

2. Security as a Scientific Discipline - Global Opinion Overview

Most security theorists begin their considerations in the beginning with the wrong basics. The principle of them all is a fundamental ignorance of security as a science. So today there is a very strange situation that many scientists who are not primary dealing with security are engage in theoretical definition of this science. It would be really useless to waste the time and attention of scientists by listing all those scholars in the fields of philosophy, psychology, law, and other disciplines of science who, from their positions, seek to place security in some scientific framework. This is where the problem arises because most of them do not understand what security is all about. With no intention of continuing to criticize, it is sufficient to consider the consequences that are catastrophic. Students at all levels studying security at the end of their studies simply do not know how to do what should be the basis of their studies - security assessment. Why is it so? Take a look at the curriculums of the world's leading educational institutions that claim to provide students with the level of knowledge that someone wants to become a security professional. With a simple insight you will understand that in these curricula there are no integrated units in subjects such as security analytics, intelligence with methodology of its work, counterintelligence and methodology of its work, national security, international security and other subjects necessary for someone to become a security professional. Without further due, let us explain why Security is Science and not just Studies.

The very word "security"

Whether it's about Serbian word bezbednost, the Latin securitas, English security, the ancient Greek asphalei, or the Hebrew word bitachon, the meaning is the same. It describes the condition of the state as an ordered society. It describes processes and phenomena which affect the above mentioned condition.

Definition

Security is Science about the condition of state and processes within the state, specifically, condition and processes which enable normal functioning of state and development.

That condition is depending on internal and external risk/s. Security Science is based on theories of State and Law, the theory of Conflicts, the theory of Complex Systems as well as the theories of Catastrophe. Starting from Plato Ideal Society within the Ideal States to Tomas Hobs and his description of the Natural condition of Mankind and Natural Laws and Contract.

Security Science uses all social scientific methods and besides that, a special scientific methodology that is different from all other social sciences. It is a methodology used in the collection, processing, and analysis of data as well as the methodology of predictions. All of these specific methods coming from Natural Science.

Security Science is indivisible but it can be viewed from several aspects such as environmental security, nuclear, energy, economic, legal security, and so on. In all these aspects of security it is a case about variety of conditions of the state as ordered society. In all of those aspects fact remain that it is a case of basic or fundamental conditions which determine normal function and development of society as whole.

Whether it is a case of state or society at the national or international level, Security Science study, follow and monitor all the processes and phenomena that affect the aforementioned conditions.

In other words, it is completely wrong to put Security Science into discipline of Security Studies within the scope of Science of International Relations. In fact, International Relations depend on the condition within state and conditions of states in their mutual relations. So it is on contrary, International Relation is within scope of Security Science. Furthermore, some authors believe that International Relations is not a science. According to some authors International Relations is Art not Science or like *Stanley Hoffmann argued,* International Relations is not a science but discipline Study program.

Numbers of authors to whom security is not an original field of research or expertise, contributed to the complete misinterpretation of the Science of Security by their works. A careful analysis of the following authors can easily lead into conclusion that all of them consider Security no as a science, but as a discipline Study program within the framework of the Science of International Relations.

3. Technological Security Segments

Unfortunately, technology is in general considered separately from security in its scientific and analytical form, mostly for development of applied technical tools or means for performing security activities. In reality, technology is the integrated part of most of the systems we analyse for security issues or vice-versa (e.g. digital forensics, forensic genetics and its influence on biometric security options, etc.). Perhaps the most characteristic example is cyber security, where the fast development in the field of information and communication technology (ICT) has provided a variety of new functions and services, both for private and business use, creating in the same time a number of vulnerabilities and security issues. Today, cyber security is a separate topic in most of analysis and discussions. Similar case, though on different levels, is with other technologies. Moreover, most of the advanced technologies in use today are interconnected and interdependent among themselves, including cyber component.

In recent years, terrorist organizations have increasingly turned to the Internet as an alternative training ground for terrorists. There is a growing range of media that provide platforms for the dissemination of practical guides in the form of online manuals, audio and video clips, information and advice. These Internet platforms also provide detailed instructions, often in easily accessible multimedia format and multiple languages, on topics such as how to join terrorist organizations; how to construct explosives, firearms or other weapons or hazardous materials; and how to plan and execute terrorist attacks. The platforms act as a virtual training camp. They are also used to share, inter alia, specific methods, techniques or operational knowledge for the purpose of committing an act of terrorism (Trifunovic, 2014). Such misuse of Internet by terrorists is just one minor segment of vast cyber security area that requires modern approach and such need further extends to virtually all aspects of security domain.

Considering the previous, it is logical that *a multidisciplinary approach is needed when talking about security, which would include the technological domain*. Let us use a very characteristic example, the 2006 European blackout. On November 4, 2006 the Europe interconnected grid experienced a serious incident originating from the disconnection of a 380kV line in the North German grid. The interconnection lines were tripped due to overload by the disconnection and the bad coordination between the system operators. The cascading outages of the lines caused the European interconnected network splitting into three islands with different frequencies. In order to re-establish the balance between generation and load, the automatic load shedding procedures were performed, and this resulted in the blackout. Since such and similar incidents also represent serious security threats, the need to assess and react in systematic, global and multidisciplinary way is obvious.

Particular danger occurs when terrorists gather information related to critical infrastructures, which allow them to discover vulnerabilities and set targets. Ranging from airports and other transportation related infrastructures to power and water supply system which are vital for the society (including nuclear power plants), serious damage to critical infrastructures can incur both direct and indirect heavy losses, including loss of lives. For that reason various criminal and/or terrorist activities related to Critical Infrastructure Protection (CIP) and resilience activities should be handled with correct approach, including scientific methodologies, and as a coordinate action (Todorovic et al. 2016).

One step towards such goal is the Security Science and Technology - a collection of monographs presenting science and science policies for mitigating security risks, addressing a range of vulnerabilities including: Individuals in society, their security and wellbeing; National infrastructure and services; and Economic prosperity. The series will encompass three operational domains: the cyber, physical and social spaces, covering aspects of Prediction (prior to the event), Detection (during the event), and Response (after the event). For example, in cyber space, Prediction includes data mining, data analytics, and threat and vulnerability assessment; Detection includes trustworthy systems, information assurance, and anomaly detection; and Response includes security strategies, decision support, and forensics (Hankin, 2016).

4. Scientific Approach to Security Topics

Dealing with security as a domain and its various related topics and subsections requires the appropriate general approach, which is further adjusted on the case-by-case basis. As already mentioned, such approach should be the multidisciplinary one. However, one of the key problems in defining the general approach and what it should contain, is that such definition differs to the large extend depending on who is creating it. Since security science is still not widely recognised as such, scientists and experts in the field of security come from different educational and operational establishments; i.e. sociologists, psychologists, lawyers, police, army, intelligence & counterintelligence, diplomacy and, in far smaller number, from technical sciences like informatics or engineering. Consequently, there is not an unified view and consensus on the general approach to security topics.

As the first step towards the creation of multidisciplinary general approach to security as a science, it would be useful to agree on key elements (phases) contained in the security analysis (SA). One possible classification would be the following:

a. Methodology for data collection
b. Assessment
c. Evaluations
d. Predictions
e. Measures & guidelines

Together with the approach there are various hypothesis and parameters that have to be defined for a security as a domain. As the primary ones might be to select the content and the boundaries for the security analysis. Without aspirations to get involved in definitions of security, for this paper we will use the following elements to delineate the initial parameters for analysis: target (who/what is the focus of SA), security aspects for SA, type of risks/threats to consider, available resources and timeframe for SA. Initial parameters are specified on a case-by-case basis in order to perform security analysis, and once defined a scientist/expert in security can proceed with SA. In following chapters are given basic elements and guidelines for SA approach.

a) Methodology for data collection

Once the initial parameters are set, the proper methodology for data collection can be selected. For example, in cases of security analysis related to sociology and similar topics, data collection would involve interaction with people (e.g. questionnaires and interviews), public and private institutions gathering and storing relevant information, statistical evidence, etc. On the other hand, in cases of security analysis related to physical security (e.g. specific public or other events, buildings, important institutions and infrastructures, etc.) data collection would primarily be focused on locations, organisation and operation, involving different sources of information than in the precious case. However, in both cases *this phase of SA has to provide a comprehensive data set that describes the situation of the observed target within the given initial parameters*.

b) Assessment

This phase of SA deals with the existing security situation. Here a scientist/expert performs initial analysis of the target under observation and defines security vulnerabilities, possible types of risks and threats, etc. Again, the assessment is performed differently and using alternative methods and tools in cases of SA that focuses on people (e.g. related to sociology) versus physical security or some intermediate or third type. In all cases *this phase of SA has to provide* *an assessment of the security situation of the observed target within the given initial parameters.*

c) Evaluations

Once data describing the situation are gathered and security assessment of the observed target is performed, a scientist/expert can proceed with evaluation of the security situation. This phase often involves possible expansion of the situation with alternatives, listing of alternative threats, cross-reference analysis, what-if scenarios and similar. Evaluation phase includes the estimated use of available resources for prevention and mitigation of threats. Due to a large number of variables to be taken into consideration, this phase of SA can be considered as case specific and requires custom approach in most situations. Depending on the initial results, evaluation process might be iteratively repeated by including/excluding elements or adding new factors for SA. If required, additional data collection could also be performed as a part of iterations. *SA evaluation(s) has/have to come up with the report that can be utilised by security stakeholders for work on protection of the observed target and/or application of security measures within the given initial parameters.*

d) Predictions

While the evaluations phase involves fully comprehensive and thorough analysis, predictions phase in essence deals with most likely occurrence of events. As such it can rely on experience, statistics and recorded episodes in many cases, but its main tool is the calculation of probability of incidents in conjunction with other events. Since it is very difficult, in many cases virtually impossible for a number of reasons, to provide the appropriate security protection in various situations, predictions phase actually ranks threats and scenarios, providing guidance for security stakeholders in performing their work in the most effective way. Furthermore, predictions phase can also provide an answer to possible consequences, damages and loss in cases that specific security situation is not dealt with, or that the preventive and mitigation measures were not performed appropriately. For that task a statistical method, in combination with other tools, should be used for calculation. *Prediction phase of SA has to provide an estimate of the preferable actions within the given initial parameters.*

e) Measures & guidelines

Despite the fact that every phase of SA has also as an outcome some outputs and reports, it is necessary to produce final documentation that would contain security measures and guidelines as the result of overall analysis and synthesis of the work performed in all previous SA phases. Such documentation is often produced with different levels of detailing, targeting specific user groups within security stakeholders (i.e. managers, administrators, operators, etc.). As such, *security measures and guidelines represent the final phase of SA, integrating knowledge and presenting the results in usable form.*

The described SA methodology is universal and can be adapted and used both for research in security science and for practical/operational work. Furthermore, it can be also applied for evaluation during the security event, or in cases when an incident has already occurred. It is important to emphasize that in those cases timeframe for SA is very limited and some phases might be shortened or omitted.

5. Mathematical Modelling in Security

Security science, as most of other scientific disciplines, relies heavily on applied mathematics and various mathematical tools for data analysis and interpretation (e.g. mathematical statistics, computational mathematics, etc.). Quantitative analysis, followed by derived associations, correlations and connections, provides valuable information to security practitioners. To illustrate a possible scientific approach, an example of one possible mathematical procedure follows: in order to effectively evaluate the security of some system, a quantitative information evaluation method might be used which would combine analytic and fuzzy logic process. Once the common criteria for problem definition are established, a security evaluation hierarchy model is created. Then the analytic hierarchy process (AHP) method could be used to calculate the security factors' weights to the evaluated system. Based on derived weights, fuzzy logic evaluation method might be applied to calculate the final quantitative security level. Being only the illustration, described procedure cannot be discussed regarding potential results. However, it is important to note in general that the effectiveness of selected method with applied mathematical tools should be validated by evaluation of a practical example before adopting it for use in security domain. On the other hand, in recent decades the use of a qualitative research approach has significantly improved in social sciences, including security. Qualitative approach is based on the principle that complex problems should be studied in their totality because such phenomena cannot be reduced to independent elements. Security domain usually involves the investigation of complex phenomena, thus emphasizing the need for application of various advanced research procedures. Mathematical modelling is perhaps the most advanced and flexible tool for such purpose.

Modern societies are characterized by a variety of complex networks, including networks of agents, computers, or States that are highly interdependent. Examples are computer networks (internet, intranet); communication networks (fixed and mobile phones); socioeconomic networks (transport, energy, demographic, technology, production, and distribution networks); neural and cognitive networks (human brain, artificial intelligence); biological networks (spread of infectious diseases, metabolic circuits); environmental networks (pollution, climate system, population dynamics, resource management). The performance of these networks crucially depends on their stability against critical events which are uncertain and have a potentially high impact on the network structure, sometimes with disastrous consequences. Identifying the critical couplings is essential to use anticipative incident management and limit the risks of interactions between complex networks and uncertain incidents. To reduce vulnerability against attack and improve disaster response, most relevant is to develop criteria for adaptive and stable network design, and to define thresholds for qualitative change in network structure. This is of particular interest with regard to network survivability against terror attacks, but could also contribute to understand, prevent, and counter the emergence of terrorist networks and their societal basis as well as the effectiveness of their actions. Understanding these problems can help to identify key principles and criteria for network design, using advanced methods in mathematical modelling and computer simulation (Scheffran, 2008).

A practical example of applied mathematical modelling in security science could be the approach to case of the London riots. In August 2011, several areas of London experienced episodes of large-scale disorder, comprising looting, rioting and violence. Much subsequent discourse has questioned the adequacy of the police response, in terms of the resources available and strategies used. In one article the authors have presented a mathematical model of the spatial development of the disorder, which can be used to examine the effect of varying policing arrangements. The model is capable of simulating the general emergent patterns of the events and focuses on three fundamental aspects: the apparently-contagious nature of participation; the distances travelled to riot locations; and the deterrent effect of policing. The authors demonstrate that the spatial configuration of London places some areas at naturally higher risk than others, highlighting the importance of spatial considerations when planning for such events. They also investigate the consequences of varying police numbers and reaction time, which has the potential to guide policy in this area (Davies, et al., 2013).

In some cases security science overlaps with other disciplines in instances where security is not the main factor, but a segment of a larger picture. For example, mathematical modelling in the field of fluid mechanics counts among efficient methods of the prevention, solution, or retrospective analysis of large scale of emergencies regarding emergency planning, industrial safety and chemical terrorism prevention. One development trend in mathematical modelling tends to study single details of various emergency situations and also to integrate specialized modelling tools into one complex unit. This results from the growing need to model more complex physical processes in more complex terrains and urban areas. The ability to evaluate the influence of buildings and surrounding terrain is on the biggest advantages of Computational Fluid Dynamics (CFD) tools. Simple and statistical models in this context work well only for an initial estimate of the development and effects of emergencies or as a quick screening of emergencies during their course. If a detailed knowledge of the situation for better understanding of its course, planning and preparedness is required, it is advisable to employ detailed CFD modelling tools. This trend is also reinforced by the increase in performance and availability of computer technology (Zavila, et al., 2015).

6. Conclusions

Security is related to many other disciplines, ranging from social sciences to national defence. Security is often a segment of an integrated approach targeting the analysis of complex phenomena or a tool for behaviour analysis and policy drafting in sociology or law domains. In those and many other cases security plays the role similar to applied mathematics, physics or chemistry. When considered as a separate discipline, security covers a very broad and heterogeneous area with a number of unique challenges. As such, security has overgrown its old role of being just a social science discipline. Observed in its complexity, security is the scientific discipline that applies its own procedures and methodologies for security analysis (SA).

In this paper authors have demonstrated that security is science, with emphasize on technological security segments as very complex organisation-wise, critical for the society well-being and with high vulnerability to incidents of various types. The paper presents a detailed concept of the scientific approach to security topics as one possible way of performing SA, hoping that it will be further improved and enhanced in the future. As examples of how Security Science utilises segments from other scientific disciplines, the last chapter discusses some use of mathematics modelling in security domain.

References

Davies, T.P., Fry, H.M., Wilson, A.G. & Bishop, S.R. (2013). *A mathematical model of the London riots and their policing*, Sci. Rep. 3, 1303; DOI:10.1038/srep01303.

Hankin, C. (2016). *Book Series: Security Science and Technology*, ISSN (print): 2059-1063.

Scheffran, J. (2008). *The Complexity of Security*, Wiley Periodicals, Inc., Vol. 14, No. 1. 13-21.

Todorovic, B., et al. (2016). *Chapter 22 - Contribution to Enhancement of Critical Infrastructure Resilience in Serbia, Resilience and Risk - Methods and Application in Environment, Cyber and Social Domains*, Proceedings of the NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructure Safeguarding, ISBN 978-94-024-1122-5 (HB), Azores, Portugal, 26–29 June 2016, pp 531-551.

Trifunović, D. (2014). *Islamic Terrorism and al-Qaeda in the Balkans (Testimony of a former al-Qaeda lieutenant),* International Strategic Studies Association ISSA, Alexandria, VA, US.

Zavila, O., Dobes, P., Jakub Dlabka, J., Bittaet J. (2015). *The Analysis of the Use of Mathematical Modeling for Emergency Planning Purposes*, Journal The Science for Population Protection, No. 2. 1-9.

Branislav Todorović,
Institut za nacionalnu i medjunarodnu bezbednost

Darko Trifunović,
Institut za nacionalnu i medjunarodnu bezbednost

NAUKA O BEZBEDNOSTI KAO NAUČNA DISCIPLINA - TEHNOLOŠKI ASPEKTI -

Rezime

Rad razmatra činjenice da rast i ekspanzija odgovarajućeg domena, u kombinaciji sa sopstvenim procedurama i metodologijama, opravdava postojanje nauke o bezbednosti. Rad započinje globalnim pregledom mišljenja o bezbednosti kao naučnoj disciplini. Uz fokusiranje na tehnološke segmente, detaljno je predstavljen odgovarajući naučni pristup analizi bezbednosti (SA – security analysis). Takodje su dati primeri koji se odnose na upotrebu matematičkog modeliranja i alata za analizu i interpretaciju podataka u bezbednosnom domenu.

Ključne reči: nauka o bezbednosti, analiza bezbednosti, sajber bezbednost, matematičko modeliranje.