

Dr. Gordan Akrap

Hybrid Warfare Research Institute, Zagreb

Full captain Ivica Mandić

Center for Defence and Strategic Studies, Zagreb

E-mail: gakrap@yahoo.de

DOI: <https://doi.org/10.37458/ssj.1.2.2>

E-mail: ivica.mandic@suradnik.unizg.hr

Review paper

Received: December 20, 2020

Accepted: December 30, 2020

WHY SECURITY SCIENCES?

***Abstract:** In this paper, the authors are discussing the need to introduce security sciences as a new scientific field within the existing organization of social sciences. The development of quality, usable, and functional human knowledge and skills has been guaranteed the safe and undisturbed development of individuals and communities since the beginning of their existence. The development of society has led to a change of paradigms on which reflections and analyses about security, conflict, and war rested. This, in turn, brings us to the situation of the need to change those paradigms of organization, principles, concepts, and theories of security as a new scientific discipline that should enable the continuation of safe and unhindered development of human society.*

***Keywords:** Security science, Knowledge, Society, Hybrid Threats, Whole-of-Society approach, Smart Governance*

INTRODUCTION

The necessity for human survival and further development of communities, ie safe and undisturbed development and progress, during the century of their existence, has influenced human lives. It was of crucial importance to develop existing knowledge, abilities, and skills. Given that life was full of different, known, and unknown security and safety challenges that people faced, they had to think, and accept useful knowledge and abilities. Both on individual and level of communities. In the center of the development of new knowledge was the need for constant re-examination of the existing knowledge, situation, and relationship. To be able to reach new levels of knowledge and to develop appropriate skills, they needed to know how to ask the right questions, at the right time in the right place, and come up with reliable and sustainable answers. Of course, the answers that were reached did not represent the final truths (even though in science there are truths and knowledge that are, as a product of general agreement, undeniable and are no longer discussed (eg mathematical operations)).

Knowledge and science are not and must not be constants. They are influencing and constantly evolving with each other as products of the thought process. Science is a living organism in its constant change. Therefore, neither knowledge nor science can be viewed as static but only as dynamic processes. Science needs to offer grounded and applicable answers to the challenges we face. And especially at this time when the existing, as well as future, challenges that we face as humanity has changed their appearance into new forms. There has been a change in the domains in which, and from which, crises operate and emerge. They are increasingly intense, have significantly different narratives, and more and more, often, and strongly influence (in the long run) the whole of human life and behavior. As well as human futures.

CROATIAN APPROACH TO SECURITY SCIENCE

Traditional academic disciplines have evolved and are evolving over the centuries to reach their current state of perfection. These traditional disciplines, such as

astronomy, physics, mathematics, medicine, and more recently, biology and environmental science show a set of characteristics by which each can be labeled as a discipline. Some of the features of the discipline include:¹

1. Knowledge corpus: Well-defined and inclusive knowledge corpus.
2. Knowledge structure: The internal structure of knowledge, achieved through internal relationships between concepts so that consistency and logic prevail.
3. Concepts and principles: The building blocks of knowledge of a discipline are concepts, and the relationships between concepts are governed by principles.
4. Theories: Theories have a predictive function and provide a final test for discipline, as outcomes can be predicted.

Security science has yet to achieve the full status of an independent academic discipline because it has no validity in the features of traditional disciplines. As and when the new security science discipline will aspire to these features, continuous research applied to the features of the discipline will respond to ensure the context of knowledge, structure, principles, and prediction theory.

Security currently lacks definition and, therefore, lacks structured knowledge. Besides, security is diverse, interdisciplinary, and without a defined or specified knowledge or skills structure.² However, it should not be concluded beforehand that the current definition of security does not contain a defined knowledge structure. Diversity and the interdisciplinary nature will develop curiously as the discipline becomes more professional, concepts will evolve, and tertiary education programs will increase. Professional development is a crucial component of professional use, as it allows an individual to maintain value in a chosen career. Thus, professional diversity must be limited by accepted structured knowledge. A feature of professional development is durability and focus - that is, to maintain community confidence in the knowledge base and skills of a profession, one must continue to strive to be at the top of knowledge in the chosen discipline.

¹ Clifton L Smith; David J Brooks: *Security Science: The Theory and Practice of Security*, p. 1

² Hesse, L., Smith, C.L., 2001. *Core Curriculum in Security Science*. Paper is presented in the Proceedings of the 5th Australian Symposium on Security Research, Perth, Western Australia.

The basis for the continuous development of formal knowledge about security and its application for the protection of values in the national and international context will depend on the understanding of the principles and concepts of the new security discipline. Research and development on the structure of security discipline are crucial for the professional application of a new generation of conceptual security principles for value protection. The future of security is very positive given the growth indicated in the discipline. Security has no features of discipline, with a defined and inclusive definition. The concept of security is diverse and multidimensional. Nevertheless, security can be defined in a given context.³

The interested academic community is making discussions about this issue. For some time now, the existing organization of knowledge and science related to the state and sense of security of individuals, communities, societies, states and international integrative organizations has been considered following modern, anticipated, and expected trends and security challenges. The question arises as to whether science or even better-organized knowledge of security, should continue to be treated and accepted as part of the science of international political relations or should it be viewed as an independent scientific discipline. As a new scientific field within the social sciences. Croatia has decided on this issue. Security and defense sciences (code 5.513) were introduced as a new scientific field in the field of social sciences in May 2005 by the Rule book on scientific and artistic areas, fields, and branches.⁴

Should the Croatian approach to the perception of this issue be accepted, should it be rejected? Or should it be further debated and a decision on whether or not security sciences should be a new scientific field has to be delayed?

According to the Oxford Dictionary, science is a systematically organized body of knowledge on a particular subject⁵. The same source offers a more detailed definition of science: The intellectual and practical activity encompassing the systematic study of the structure and behavior of the physical and natural world through observation and experiment.

³ Fischer, R.J., Halibozek, E., Green, G., 2008. Introduction to Security, eighth ed. Butterworth-Heinemann, Boston, p. 482

⁴ Narodne novine; https://narodne-novine.nn.hr/clanci/sluzbeni/2005_06_76_1500.html, access December 1, 2020

⁵ Oxford dictionary; <https://www.lexico.com/definition/science>; access December 1, 2020

Has the topic of security and defense become so important and necessary for secure development, but also the survival, of society and the state that it needs to be improved, in a scientific sense? What are the arguments that support this thesis is a question that we will deal with in this paper? Of course, as already stated in the introduction, these views are not and cannot be final, but are subject to further review, verification, and analysis.

CHANGING THE PARADIGM OF CONFLICTS AND WARS

Conflicts and wars that dominate Europe (as well as the MENA region) in the last 30 years show that there have been several changes in the paradigms of planning, leading, managing, and ending low- and high-intensity conflicts. Until recently four instruments of power were needed to describe the conflicts. For those who wanted to lead, plan, and led conflicts and wars was important to have the ability to use some of those instruments known by heir acronym DIME (Diplomacy, Military, Information, Economy). The main lever for imposing one's own will on the targeted audience was based on military power. And the ability of its (military power) fast, efficient, complete transmission, ie safe, complete, and undisturbed transfer to the desired area and engagement according to individual goals to the extent and level that enables a quick victory in the armed conflict. Achieving overall victory, on the other hand, required a rapid and complete transformation of negotiating abilities into the power to use coercion and its reactivation once the kinetic conflict was moving towards its end.

However, the rapid and comprehensive development of information and communication technologies, means and techniques, the development of society in the direction of its digitalization, and the creation of a strong dependence on the same digitalization, created the conditions for an almost complete paradigm shift in the process of imposing one's will on others. This was already evident in the Croatian Homeland War when the Yugoslav political and military leadership, assisted by the Serbian government with the help of information, media, economic, financial, and influence operations against certain ethnic, national, and religious groups tried to prevent the first free multi-party elections in Croatia and Slovenia in 1990. After failing to prevent elections, in the second phase (second half of 1990) they continued to apply the same models of action to overthrow the newly elected democratic government.

When these activities failed, they launched a kinetic force and carried out armed aggression. First against Slovenia, then against Croatia, and later against Bosnia and Herzegovina.⁶

The paradigm shift of conflicts and wars is especially visible in the conflicts and wars taking place in this century. There has been a change in the instruments of projecting its power (as well as in their order of use) and the targets being attacked (there has been also a change in the order of targets being attacked primarily, secondarily and which one as tertiary targets).

NEW INSTRUMENTS OF POWER - MPECI

Attempts to forcibly overthrow political power in Montenegro, the impact on the election and referendum processes in the United States, North Macedonia, the United Kingdom, France, Germany, Serbia, Syria, Yemen, Venezuela, Ukraine, the NATO-Serbia war of 1999, and the process is known as the "Arab Spring" only show that the primacy in influence operations was taken by non-kinetic operations. They also show that it is necessary to introduce a new instrument of power that is available to the attacker: organizations and individuals from the domain of civil society, as well as modern technological and technical solutions and communication systems. At the same time, there was a change in the diplomatic instrument into a political one. Therefore, today we are talking about five instruments for projecting one's power against the target audience: Military, Political, Economic, Civil, Information (or even better and more appropriate: Intelligence).⁷ There has also been a change in the order of use of instruments of power. Military power is used only necessarily and only if other instruments have not obtained the desired effect. Military power can also be used as a threatening possibility (the so-called Sword of Damocles) given the illusion (to the targeted audience) of the possibility to choose between the offered possibilities: "carrot and stick". Carrots represent the use of non-kinetic instruments, and the stick those from the domain of kinetic threats.

⁶ Gordan Akrap, Viacheslav Semenienko: Hybrid warfare case studies: Croatia and Ukraine, National Security and the Future, Vol 21, No:1-2, 2020, p. 15

⁷ According to MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare, p. 13

At the same time, there was a change in the domains that are targets of offensive activities: Political, Military, Economic, Social, Infrastructure, Information (PMESII).⁸ Here, in particular, comes one of the facts from the area of influence operations where information is used to fight against information and for information that needs to be collected. Although it is stated only in the fourth place of the goals that the attacker attacks, society is still a priority goal of modern attackers because the destruction of cohesive ties that connect a community or society, violates its ability to defend and effectively resist the attacker.

As a result of previously said, we come to a situation that we need to recognize, understand, and redefine new threats, ie the introduction of hybrid threats as a new paradigm of offensive actions. Hybrid threats make significant changes in the processes, vectors, and instruments of attack and influence to impose attackers' own will on the target audience. At the same time, it points to a change in the focal activity domains that these instruments are trying to influence. Either individually or at the group level. Hybrid threats are an important novelty in changing the paradigm of recent conflicts. Namely, the concept of hybrid threats implies the reality by which actions and processes at the tactical level can yield significant results at the strategic level. At the same time, non-military means can achieve goals in military and non-military domains and vice versa: military means can strongly influence military and non-military domains. Aggression using some of the activities from the spectrum of hybrid threats can be used imperceptibly towards a specific target audience. In other words, the target audience does not have to be aware of the reality that they are under a hybrid attack. This will especially come to the fore if the defense system of the attacked audience is not working if the early warning system and indicators are not (or badly) defined and if the communities that makeup society itself are sufficiently divided. Those internal divisions prevent their ability to notice and understand the reality that surrounds them. Lack of knowledge about new security challenges, as well as those that may arise, and threats to security and stability, leads to challenges that unprepared societies cannot face effectively.

⁸ Ibid

This brings us to the situation that we need to change our thinking about the field of security as knowledge and part of science conditioned not only by the diversity of political processes in the direction of perceiving, increasingly complex, relations on a global level. Until recently, the main actors in the process of imposing their own will on others were states, ie subjects of international law (regardless of whether they were internal or external threats). Today, in addition to the state actors, we recognize and accept the existence of several other actors who can influence the processes of imposing their own will on others: non-state actors as well as individual organizations that possess individual (or more) instruments of power and can apply them to a specific target audience. Regardless of its territorial distribution.

It is clear from the above mentioned, that there has been a significant change in the narrative of existing (and future) threats, conflicts, and wars, which must necessarily be reflected in the change of scientific narrative in the perception of this issue.

WHOLE-OF-SOCIETY APPROACH

All these changes point to the need to change the current approach in perceiving the complexity of modern security challenges that societies and states are facing. The issue of security can no longer, and should not, be treated as an area that depends on political activities but comprehensive social action and reaction. Regardless of whether they were offensive or defensive. Security is no longer just an issue that should be and can be addressed by individual bodies and institutions of the state and international organizations. It is because all the complexity of modern security challenges cannot be effectively addressed by applying present methods and means. Given the above change of the possible usage of instruments of power with which the attacker is trying to project his own will towards others as well as areas of offensive action, it is necessary to approach a comprehensive action at the level of the whole society (whole-of-society approach). The aim is to create conditions for the development of the ability for early-warning indicators and systems, the ability to understand and recognize hybrid threats early enough and to plan and implement an effective response to them. Therefore, it is necessary to develop a new model of risk and threat analysis in different areas of action (different target domains) that will cover and assume and understand their hybridity.

It is quite certain, as the examples of modern conflicts and wars show, that future conflicts will begin with offensive actions using one (or coordinated action of several of them - which is much more likely) from power instruments of projecting one's own will from a spectrum of non-kinetic instruments. Experience indicates that the attacker's priority goals will be to break the cohesive forces of the community and society, encourage existing and create new divisions as well as an attack (from the cyber domain) on one of the three critical infrastructures (water and food, energy, information, and communication).⁹

As key cohesive links that unite an individual community and society, are identity issues as well as values, beliefs, and principles on which that community and society (or more of them) are based. They represent a special and primary goal of security challenges and threats coming from the hybrid spectrum. It is, therefore, necessary to work on developing the ability of social resilience which is key to an effective defense. At the same time, it is necessary to strengthen the population confidence in state institutions (especially during the development of the state's defense capabilities). A special challenge that states are facing, is the integration of knowledge and skills that exist in other segments of society (private, academic, non-governmental, social) into an effective system of building mutual trust and understanding as a prerequisite for the successful defense at the predictive level.

HYBRID THREATS

Therefore, the hybrid threats, which we are increasingly facing, require a different approach in the processes of planning an effective defense and security to maintain the ability of society and state to function safely and smoothly. This means a different, even more serious, and complete scientific approach to the field of modern security challenges outside the current context of political relations. Given the complexity of current and future security threats, an interdisciplinary scientific approach to this issue is necessary. As has already been said, we can no longer deal with it effectively within the concept of National Security. It is necessary to promote the

⁹ Akrap, Gordan: Suvremeni sigurnosni izazovi i zaštita kritičnih infrastrukture; Strategos, Znanstveni časopis Hrvatskog vojnog učilišta „Dr. Franjo Tuđman“, Vol.3, No2, 2019, <https://hrcak.srce.hr/231009>

Homeland security concept and strong and full interaction of the whole of society: state, public, private, academic, and civil sector and the population in general. The knowledge and skills that exist in these sectors need to be integrated within the security and defense sciences, which should offer new knowledge and science-based models for strengthening resilience, primarily at the level of society and the community.

The new science must pay special attention to identifying threats and security challenges that come beyond existing domains. Namely, the existing risk analyses consider the possibility of the emergence of threats coming from known sources-of-risk domains (let's call them "black" domains). The attention of the security and defense system is also focused on the possibility that certain security challenges may arise from the so-called gray areas or areas of reduced risk. The hybridity of threats indicates the need for organized and systematic monitoring of activities and threats that might appear from the so-called white zone, ie an area from which the previous knowledge and assessments did not assume the occurrence of a particular security challenge or risk. This is one of the key items to which modern security research needs to provide reliable, high-quality, unambiguous, and trustful answers to protect the population and societies at the preventive level.

As a terminological example of how and why it is possible, but also necessary, to separate the field of security from the science of international political relations, we can use the development of the concept, names, and domain that we now call cyberspace. Namely, the name cyber, which described the first phase in the development of today's cyberspace, is derived from the name cybernetics. Over time, the development of new and useful knowledge, technologies and techniques, information and communication systems, and computing, has led to a situation where the derived name has become more dominant concerning the domain from which it was extracted. The field covered by the term cyber today encompasses a whole range of logical processes, physical components, human persons (real and virtual), and artificial intelligence, which was almost unthinkable when the term was introduced into scientific discourse.¹⁰ In the same way, it is necessary to extract the thematic area of security and

¹⁰ Gordan Akrap, Slavko Vidović, Hrvoje Sagrak: Digital Sovereignty – what, why, how; paper presented at the 5th Zagreb Security Forum, September 2020

defense from the field of international political science and introduce it as a new scientific field within the social sciences.

SMART GOVERNANCE

The change in approach to security and defense issues as a new scientific field is neither abrupt nor revolutionary. It is the result of perceiving the complexity of processes that have been on the academic scene for some time. In this regard, the necessity of planning and realization of this concept is emphasized, because the society plans its future development based on new technologies. One of those concepts on which development is planned is the smart cities concept that should enable a better, faster, more sustainable, more efficient, safer, and more useful life. The networked system of smart cities concepts brings us to the concept of smart societies and smart states. The crown of these concepts is the process that needs to be established to meet all established goals and tasks, to monitor their development, maintain the security and integrity of systems and protect all their activities so that they are not used against the interests of its stakeholders. This is a process we call smart governance. It is at the same time activity and a process that needs to be established for the functionalities of the unified system to be of benefit to their end-users: individuals, groups, communities, companies, civil society, the state.

A necessary precondition for fulfilling the established goals is the incorporation of security procedures and protections that would prevent, ie reduce to a minimum level of risk of any form of activities that could compromise these systems. Activities such as erasure and/or alteration of personal and business data, entering inaccurate data, disabling their malicious use, harming private and public persons, theft, inciting hatred, violence and terrorism, attacks on critical infrastructure, must be prevented, identified, and disabled. The security of such systems adds additional arguments to the claim that the existing concept of security and defense should and must be separated from the scientific field of international relations because security threats, as well as defense planning against new security challenges, face new threats. In this sense, it is necessary

to develop and build the concept of societal and group resilience through the concept of smart security governance and continuous education of users (especially in the domains of media, scientific, medical, hygienic, digital literacy, and critical thinking). This differs from the activities covered by the scientific field of international security.

CONCLUSION

Modern attackers threaten the security of individuals and communities, and society, through their aggressive actions. Attacks on society are extremely dangerous because a society can exist without a state, but a state cannot exist without a society. An attack on a system of cohesive values of a society can cause serious negative consequences for the whole society and the state. This directly affects the capabilities and integration connections of the international organizations of which that state is a member. The state, as a subject of international relations, can use repressive measures to prevent threats and challenges that it faces or has yet to face. However, in situations where the attacker is not aware that he has been attacked when the attack is detected after the attack has already started, and especially in situations where the attack has already passed, and the attacker was not even aware of that, what activities state can and should initiate to show its determination in effectively face those threats to its security? Against whom, how, when and to what extent will the state retaliate? How certain is the state that it has irrefutably identified the attacker and that the revenge attack will be aimed at the right target? These are all questions to which there must be an unambiguous answer and to which active rethinking of the new concept of perceiving security and defense sciences in the modern world could and should provide answers. The answers to these questions should be given by security science, ie security and defense science.

Security science is an emerging academic discipline that integrates concepts and principles into a structured body of knowledge. In their simplest area of knowledge, they include security management, security theories and principles, the built

environment, and security risk management, both existing and future. These concepts can and should be expanded into an integrated framework that includes business continuity, development of security technologies, physical and personal security, corporate and industrial security, security and safety of unhindered flow of ideas and knowledge. Thus, the context provides many parts of security with a clear understanding of its operational boundaries from which further consensus can be reached on the whole of knowledge.

From all the above mentioned, we feel free to propose a definition of security sciences as a new scientific field: An organized and structured set of knowledge that enables the creation of conditions for secure, safe, and undisturbed development of society and the state, and effectively, based on developed early-warning identification, can face against present or future security challenges.

References

1. Akrap, Gordan: Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura; Strategos, Znanstveni časopis Hrvatskog vojnog učilišta „Dr. Franjo Tuđman“, Vol.3, No2, 2019, <https://hrcak.srce.hr/231009>, access December 1, 2020
2. Akrap, Gordan; Semenienko, Viacheslav: Hybrid warfare case studies: Croatia and Ukraine, National Security and the Future, Vol 21, No:1-2, 2020, <https://www.nsf-journal.hr/online-issues/focus/id/1295>, <https://doi.org/10.37458/nstf.21.1-2.1>
3. Akrap, Gordan; Vidović, Slavko; Sagrak, Hrvoje: Digital Sovereignty – what, why, how; paper presented at the 5th Zagreb Security Forum, September 2020
4. Fischer, R.J., Halibozek, E., Green, G., Introduction to Security, eighth ed. Butterworth-Heinemann, Boston, 2008.
5. Hesse, L.; Smith, Clifton L.: *Core Curriculum in Security Science*, 2001.
6. MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare; A Multinational Capability Development Campaign project; editor and project lead: Sean Monaghan; March 2019
7. Oxford dictionary: , <https://www.lexico.com/definition/science>; access December 1, 2020

8. Pravilnik o znanstvenim i umjetničkim područjima, poljima i granama
https://narodne-novine.nn.hr/clanci/sluzbeni/2005_06_76_1500.html, access
December 1, 2020
9. Smith, Clifton L.; Brooks, David J: Security Science: The Theory and Practice
of Security; Butterworth-Heinemann; 2003

Dr. Gordan Akrap
Institut za istraživanje hibridnih sukoba, Zagreb

Kapetan Ivica Mandić
Centar za odbranu i strategijske studije, Zagreb

ZAŠTO NAUKA BEZBEDNOSTI?

Rezime:

U ovom radu autori razmatraju potrebu uvođenja nauke o bezbednosti kao nove naučne oblasti u okviru postojeće organizacije društvenih nauka. Razvoj kvalitetnih, upotrebljivih i funkcionalnih ljudskih znanja i vještina garantovan je za siguran i nesmetan razvoj pojedinaca i zajednica od početka njihovog postojanja. Razvoj društva doveo je do promene paradigmi na kojima su počivale refleksije i analize o bezbednosti, sukobu i ratu. To nas, pak, dovodi u situaciju potrebe da se promene te paradigme organizacije, principi, koncepti i teorije bezbednosti kao nova naučna disciplina koja treba da omogući nastavak sigurnog i nesmetanog razvoja ljudskog društva.

Ključne reči: Nauka bezbednosti, znanje, društvo, hibridne opasnosti, pristup celokupnom društvu, pametno upravljanje