Review article
Received: 31. 07. 2021.
Accepted: 17. 08. 2021.

THE IMPACT OF NEW TECHNOLOGIES ON THE DEVELOPMENT AND SECURITY OF COUNTRIES IN TRANSITION

PhD Slavko Vuksa[27], MSc Sergej Vuksa[28]

Foreword

The instrumentalization of international organizations (UN, EU, OSCE, etc.) is taking place before our eyes. The global power elite and the authoritative world order is enthroned on the principles of hierarchy and domination. That is why we can rightly talk about the invasion of the authoritarian world order on nation-states and the inevitability of limiting sovereignty. Open interference and domination of superpowers over underdeveloped areas, such as NATO aggression on the territory of Serbia under the slogan of "humane interventionism" was enabled. In the preface to the book by communications director John Norris, Strobe Talbott, who led the Pentagon-State Joint Intelligence Committee during the bombing of Serbia, said: "The real purpose of the bombing had nothing to do with caring for Kosovo Albanians. The real cause was that Serbia did not implement market, social and economic reforms, which means that it was the last oasis of Europe that did not obey neoliberal programs under the administration of the USA, so it had to be removed. [1]"

1. The impact of globalization on security

Security challenges [2], which arise and affect all areas of social life (foreign and domestic policy, economy, finance, energy, ecology, religion, culture, informatics, etc.), impose the need to involve a number of state institutions in matters that ensure national security. In addition to increasing their number, there is a need to respond to security risks, challenges and threats in a unique and harmonized way.

The roles of state institutions in achieving state security are interpreted differently depending on the approach to security, yet the central role of the state is not disputed. System of national security, as a subsystem of the political system, affects the internal flows of society, primarily economic and political relations (it acts both as a driver and as a barrier to social movements). It must respond to internal, constitutional and legal competencies and international obligations, making it a complex system made up of a series of subsystems and elements, functionally linked. Today, we are witnessing great changes at the global level. The world, at the center of which is the national economy and the nation-state, has begun to change almost from the ground up so that only in the last few years, we can witness a return to the original postulates.

[27] Academician, Prof. Slavko Vukša, PhD, slavkovuksa@gmail.com
[28] Sergej Vukša, MSc, MIANU, sergejvuksa@yahoo.com

The world crisis of 2008 shook the foundations of globalization and "BREXIT" put it under scrutiny again. Although globalization is the official direction and strategy of all "mainstream" politicians and economists, there is a growing awareness of its negative consequences. The current world economic and financial system and relations in the world economy, has led to a concentrated group of developed countries (although interestingly opposed within themselves, still sufficiently homogeneous interests towards the "rest of the world"). On the other hand, there is a huge number of so-called "developing countries" in which about 80 percent of the population lives, with only about 12 percent of industrial production, 15-17 percent of exports, etc. The process of capital concentration and the creation of large financial monopolies, closely related to state administrations, with the obvious dominance of science. The power of innovation and new technologies, the United States and a united Germany create a new lever for the "world of blackmail" and dependence and self-interests practically represent the voting machinery in all world and European institutions, with increasing individual pressures [3]. Significant changes in world and European monetary and financial flows are necessary. In addition, changes in relations between developed and underdeveloped countries must be brought to equal levels, not relations of imposition and domination, and thus exploitation of natural resources of underdeveloped economies.

At the beginning of the 21st century, security, as a concept and area of social activity, has become increasingly important. Taking into account the importance, national security must be regulated normatively and legally in a systematic and detailed manner. This is not the case with us due to the lack of some important provisions, and the existing ones are often vague and widely set, which opens the possibility of their abuse. The national security system is a complex system with several subsystems that perform a large number of activities within their competencies, and the ultimate goal is to protect and improve security. All this indicates the complexity of managing the national security system and the great possibilities for uncoordinated action.

2. Business espionage and national defense

Intelligence activity, as an unavoidable link in decision-making by economic entities, appears as a key weapon in the realization of business strategy by acting within a legal framework [4]. The development of intelligence and security activities can be found in the Japanese economy under the auspices of the Ministry of Foreign Trade and Industry (MITI) and in the National Foreign Trade Agency (JETRO), in Sweden under the Technical Attaché (STATT), in the USA under the National Economic Council (NEC), in France under INTELCOM, etc. In addition to government agencies, economic entities themselves, driven by increased competition and fear for their survival in the market, are establishing departments that deal with intelligence and security activities. In our country, there are only mild indications in the public and there are no traces of thinking about this kind of activity. The strategy of survival and economic expansion of a small nation (state) cannot be attributed to the size of its armed forces, population size and territory, but to the perfect organization of its

intelligence and security services, as a base for economic, diplomatic and military activities. Today, internal security has an increasing international dimension. It could be argued that this international dimension significantly determines internal security. The main determinants for this are the import of crime, international drug trafficking, human trafficking and international terrorism. Organized crime is a major challenge to internal security.

Globalization and the information age have created, so to speak, a world crime market. That is why effective international cooperation is necessary to fight organized crime. The situation is similar when it comes to the global war on terror, which some authors value as a political myth propagated to achieve US world hegemony. [5]

2.1. Business espionage

One of the basic characteristics of the modern world is that it is faced with many risks and accelerated changes. Given that the same applies to the business world, this in essence, means that today's business are influenced by three elements, namely: [6]

- opportunities;
- vulnerabilities;
- dependencies

All three elements exist simultaneously and are interdependent. This means that in the conditions of globalization and relentless market competition, every business entity has a chance to achieve success. Business espionage as a system enables management to gain a realistic picture of itself, its competitors and the environment in which it operates. A clear presentation of the real situation and future directions of development enables the making of decisions that should lead to the achievement of previously defined and determined goals. Many authors therefore point out and claim that business espionage is the totality of the company's information, cognitive and action skills. It is indisputable that the business espionage system really represents the totality of the company's information and action skills. Based on the final results of the business intelligence activity, decisions are made, ie. actions are taken.

Table 1. Business espionage and national intelligence systems: a comparative analysis of the role and importance

	National Intelligence the system	**Business espionage (business entities)**
The goal	support to the president, government and ministers	support to the President of the Management Board and top management

justification	the process of making and implementing political decisions	the process of adopting and implementing business policy and business strategy
organization	independent, professional, direct contact with the President / Government	- part of the information-communication system of a business organization - part of the company's management mechanism, function identical to the organization of other business functions (marketing, finance, etc.) - direct contact with the President of the Management Board
internal division of labor	data collection and analysis functions separately	depending on the source, the analytical function has a combined role
sources	HUMINT, SIGINT, OSINT	OSINT - open sources (published and unpublished), internet, consultants, experts in certain fields
connection with decision makers	the chief is a member of the highest authorities in charge of national security	the president of the board participates in managing the process of business espionage and formulating its priorities
area of interest	military, political, security, scientific and technological	market, competitors, customers, suppliers, legal regulations, political processes and decisions and scientific and technological achievements
contribution to management	- participates in making political decisions by making analyzes and assessments - realization of political decisions	participates in the process of formulating and implementing business strategy, business actions and business decisions by making analyzes and assessments

Source: Author's work based on research

The data indicate that business espionage and the system of "monitoring" information on competitors, consumers, business partners, the market and its development, as well as key areas of development in science, technology, economics in general and politics are consistent with the goals and interests of the business entity.

In essence, modern business espionage represents the integration of intelligence methodology and information technologies, applied within the business world, that is, the business entity.

2.2. Economic espionage

Economic espionage is the collection of intelligence from foreign governments, or their intelligence services for use by those governments or their private companies. The FBI has seen a sharp rise in the number of cases attacking U.S. companies, with the vast majority of perpetrators originating in China and linked to the government. At a briefing at the FBI headquarters in Washington in July 2015, the head of the counterintelligence agency Randall Coleman said that, in the last year alone, there has been an increase of 53% in cases of economic espionage. or theft of trade secrets that result in losses of hundreds of billions of dollars. He cited examples of large corporations that were the target of attacks such as DuPont, Lockheed Martin and Walspar, which later worked intensively with FBI experts to further protect their intellectual property.

The purposes of economic espionage are the collection of protected data or confidential data, business secrets of one company by unauthorized persons or another company.

2.3. Industrial espionage

"Industrial espionage is the espionage of certain companies run by certain companies from the country or abroad. As a rule, it causes direct damage to the company being spied on, and indirectly to the country to which the company belongs. [7]" On the other hand, this espionage directly benefits the companies that realize it, and indirectly the countries whose companies they are. The 1996 U.S. Business Espionage Act[8] stipulates that a person who collects classified business information about public and private business facilities in the U.S. for the benefit of a foreign government will be fined up to $ 10 million or imprisoned for up to 15 years. When it comes to industrial espionage, the fine is five million dollars or 10 years in prison. The first to be convicted in the U.S. under this law for industrial espionage was Chinese engineer Pen Yen Yang. As an example, it could be called "Volkswagen leaves with the secrets of General Motors". When Jose Ignacio Lopez, GM's head of production for Opel, left his job and moved to work for Volkswagen, he reportedly took a large number of confidential documents with him. He also took seven senior executives with him, which made GM, a car manufacturer from Detroit, feel uncomfortable and humiliated. Of course they wanted revenge. GM claimed that their secrets were used by Volkswagen. The battle in court lasted four years and was resolved in 1997 by the companies agreeing to an out-of-court settlement of a dispute in which the German

carmaker agreed to pay $ 100 million and pledged to buy auto parts from GM for $ 1 billion. for seven years[9].

In this regard, we believe that the arrival of even more foreign companies in Serbia will initiate a change in the thinking of our businessmen, the state, about the importance of industrial espionage, especially protection from it, but also all other threats to property in all its forms.

2.4. The concept and significance of critical information

Critical information is any information or data that is essential and vital to the functioning of a system or whose disclosure or disclosure could harm or impede the profit of the person who possesses it. The notion of critical information is strongly related to the notion of critical infrastructure. In reality, critical infrastructure relies on critical information and represents any infrastructure that is of strategic importance to a state or nation. Examples of critical infrastructure include power plants, airports, telecommunications systems, government departments, information or cyber infrastructure, transportation systems, and anything that plays a vital role in the life of a country and its people. In the business of companies, critical information can also be client lists, business secrets, expansion plans, marketing plans, personal data, Manufacturing Process, confidential financial information, customer account information.

Information that is of interest in the collection and analysis of data in economic espionage, and which is largely provided by employees can be divided into: information of commercial content and information of a personal nature.

2.5. Professional secrecy

The US Uniform Trade Secrets Act (UTSA) defines a trade secret as[10]:

- information, including formulas, patterns, compilations, programs, devices, methods, techniques or processes,
- which produce an independent economic value, real potential, if they are not known to all or easily recognizable by other persons who may derive economic benefit from their publication or use, and
- are subject to understandable efforts to maintain their secrecy.

This definition has been transposed into law in 40 countries and a list of six factors was used before its adoption to determine whether or not something is a trade secret:

- the extent to which the information is available to people outside the company;
- the extent to which it is known by employees or others involved in the business process;
- scope of protection undertaken by the owner to preserve the confidentiality of information;

- value of information for the business and its competitors;
- effort and money invested to obtain that information;
- ease or difficulty for someone else to obtain or duplicate.

Appropriation of a trade secret is considered a form of unfair competition. Unlike patents, trade secrets do not last for a certain period of years. The protection of a trade secret continues indefinitely until it is made public. Thus, the inventor must choose between a patent or the protection that a trade secret brings with it. The same thing cannot be protected in both ways. Intellectual property includes industrial property (inventions, trademarks, industrial design) and copyright (for textbooks, literary, musical, artistic, cinematographic works). These goods are considered "free goods" in the sense that their use does not consume the substance. The issue of intellectual property protection today occupies the attention of governments, international organizations and industrial groups, as almost every country is forced to choose "something" between completely free access to all ideas and a complete monopoly on innovation.

Based on that, each country is forced to assess the social benefits and prices of possible alternatives. This is inevitable, because the degree of protection of intellectual property directly affects the profitability of research and development projects and the money allocated for innovation[11]. In normal economic relations, good, high-quality, cheap and powerful commodity producers survive on the market, while bad, low-quality, unproductive, expensive and weak ones fail.

Piracy most often occurs in the field of software production, ie programs and programming languages, film and video industry, so-called music production. sound carriers - CDs and cassettes, electronics and production of video and audio equipment, fashion and textile industry, especially "marked" products, production of footwear and sports equipment, cigarettes, etc. The United States loses billions of dollars a year due to unauthorized use of trademarks, patents, licenses and trade secrets. Since 1992, the United States has been compiling a list of trading partners who use piracy. At that time, there were 31 countries on the list, led by India, China and Thailand. In the field of software alone, due to piracy, the United States lost 237 million dollars in Italy, 290 million in Taiwan, 250 million in Thailand, 100 million in Poland and J. Korea $ 123 million[12].

3. Business systems protection

The rapid development and wider application of information technology in all spheres of social life significantly contribute to the growing dependence on that technology. This dependence refers not only to the society as a whole, but also to all its group and individual subjects, among which are certainly business systems. From a practical point of view, this means that any disorder caused by this addiction, not only accidental, but above all intentionally caused incidents, can potentially cause very serious problems with consequences that are difficult to predict and perceive. When it comes to business systems, their tendency to automate their activities and jobs as quickly and widely as possible is visible, knowing that this will enable them to do better, faster and more efficiently, and thus higher profits, business stability and a

certain future. Unfortunately, the speed of automation was not adequately and adequately monitored by the construction of information security systems. Due to the speed of development in most companies, the security component has been "temporarily" pushed into the background, with the explanation that appropriate attention will be paid to it as soon as business pressures "ease" a little. However, these pressures do not subside, because automation itself, by its nature, imposes growing business dynamics, creating and forcing new conditions and opportunities for business operations. What makes the situation especially difficult is that automation brings with it new threats and risks, many of which did not exist before, and which are impossible to eliminate with known and available physical-technical methods and techniques, because they have largely become primitive in the new conditions. Therefore, every business system, if it uses information technology, would have to, regardless of size, make additional efforts to build an information security system that will be able to meet current but near future needs. What is very important to understand and understand is the fact that building an information security system is an extremely serious and complex task, which does not tolerate incompetence, arbitrariness and improvisation.

For the realization of information security, business systems have at their disposal a large number of methods and techniques based on equally numerous measures and activities, which together form a strong information security system.

CONCLUSION

The strategy of survival and economic expansion of a small nation (state) cannot be attributed to the size of its armed forces, population and territory, but to the perfect organization of its intelligence and security services, as a base for economic, diplomatic and military activities[13]. It is necessary to encourage the creation of a national approach to the intelligence and security capabilities of Serbia at the highest state level, as the basis for the competitiveness and survival of the Serbian economy. Arranged political relations and economic progress are important factors in both internal and external stability, and thus security. For any government, internal security is one of the main policy areas, which can no longer be viewed unilaterally. Moreover, the connection and dependence of the internal security of the state on economic, financial and social security is becoming clear very quickly.

Today, internal security has an increasing international dimension. It could be argued that internal security is significantly determined by this international dimension. The main determinants for this are the import of crime, international drug trafficking, human trafficking and international terrorism. Organized crime is a major challenge to internal security. Globalization and the information age have created, so to speak, a world crime market. That is why effective international cooperation is necessary to fight organized crime.

References

1. http://www. https://chomsky.info/200005_/ (accessed: 30.01.2020).
2. According to Orlic, D .: "Conceptual determination of challenges, risks and threats in the process of reshaping international security", Vojno delo, 3/04, p. 84, challenges, risks and threats are listed.
3. Komazec, S., Kovač J., Ristić, Z., Labyrinths of Debt Economy, '' ABC GLAS '', Belgrade, 1993, p. 401 – 405
4. Petković, L., T., Business Espionage and Economic Warfare, '' Protexi Group System '', Novi Sad, 2009, p. 195-197
5. Vukadinović, R., Politics and Diplomacy, '' Political Culture '', Zagreb, 2004, p.p. 36-38.
6. Petković, L., T., Business Espionage and Economic Warfare, '' Protexi Group System '', Novi Sad, 2009, p. 272-275
7. Modli Duško, Korajlić Nedzad, '' Crime Dictionary '', Tesanj, 2002.
8. Economic Espionage Act, 18. U.S.C., paragraphs: 1831-1839 u: Potter, Leslie, Value Shift, Chicago, 2009.
9. http://www.therichest.com/rich-list/10-of-the-most-infamous-cases-of-industrial-espionage/, (date of access: 10.01.2021.).
10. https://www.law.cornell.edu/wex/trade_secret (date of access: 10.01.2021.).
11. Ristić, Z., Knowledge Management, Belgrade, 2001, p. 33-35.
12. Prvulović, V., Economic Diplomacy, Belgrade, Megatrend University, 2002, p.p. 157
13. Petković, L. Todor, 2009, Business Espionage and Economic Warfare, Protexi Group System, Novi Sad, p. 195-196.