Information Security Journal: A Global Perspective

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uiss20

Information security as a national security component

Rasim M. Alguliyev , Yadigar N. Imamverdiyev , Rasim Sh. Mahmudov & Ramiz M. Aliguliyev

To cite this article: Rasim M. Alguliyev , Yadigar N. Imamverdiyev , Rasim Sh. Mahmudov & Ramiz M. Aliguliyev (2020): Information security as a national security component, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2020.1795323

To link to this article: https://doi.org/10.1080/19393555.2020.1795323

Published online: 20 Jul 2020.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
https://doi.org/10.1080/19393555.2020.1795323

Taylor & Francis
Taylor & Francis Group

Information security as a national security component

Rasim M. Alguliyev, Yadigar N. Imamverdiyev, Rasim Sh. Mahmudov, and Ramiz M. Aliguliyev

Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan

ABSTRACT
The essence and different approaches to the national security are explored in the article. The article interprets the objectives and provision methods of the national security. Different areas and vital interests that are the objects of the national security are classified. According to this classification, the components of the national security, such as socio-political security, military security, information security, food security, energy security, education system security, scientific and technological security, health system security, transport system security, environmental security, mass media security, and cultural-moral security are differentiated. The development of ICT, the growing role and responsibilities of the information society in the national security system in connection with the formation of information security are described. The article also analyzes the relationship between the information security and other components of the national security. Application areas of ICT in each national security component and information security threats are identified. Their solution ways are described. The article uses analysis and synthesis, comparison, generalization and systematic approach. The results obtained in the article can be used for the development of new security concepts, strategies and other regulatory documents for the national security in the context of the information society.

KEYWORDS
National security; information security; military security; economic security; energy security

1. Introduction

Security has always been one of the most important goals and needs of individuals, society and state, as a whole. The formation and development of human civilization have always been associated with the elimination of various threats caused by nature, society, hostile countries, technological facilities, and so on. In other words, security is one of the most important conditions for the existence and development of society and state.

The notion "safety" was first used in 1190 as a "quiet state of the human spirit in which he/she considers himself/herself safe from any danger" (Sidorkin & Iroshnikov, 2019). The problem of security provision has been in the focus of many philosophers, political scientists, historians and lawyers.

Numerous thinkers have come up with interesting ideas about the state structure and security of society and its objectives and functions (Peou, 2014). Plato believed that a state should focus on its military, which provides the security of the state. Aristotle viewed the way to ensure security in society and state as shaping the socio-political culture of citizens. Machiavelli, the Italian socio-political thinker, stated that there were threats both inside (from citizens) and outside (from powerful neighbors) the country. He believed that external threats might be overcome with the help of a good army and reliable allies. As for him, if external threats are eliminated, internal security is possible to be ensured. The French philosopher Russo incorporated the concept of "people's sovereignty' in the theory of "development of society". This concept envisages not only the free and independent development of people but also the security of society.

In the 1950 s, the American psychologist-scientist Maslow proposed a "theory of motivation" (Maslow, 1954). In this theory, the author, who created a hierarchy of basic human needs, rated the issue of security second. That is, according to Maslow, the physical needs of a person's life motivation are followed by his/her need for security.

The term "national security" was first used by the US President Theodore Roosevelt in 1904 in his letter to Congress of the United States (Smith et al., 2008). However, this term became official only in 1947. Thus, the United States adopted a law on the national security in the same year. The US

CONTACT Ramiz M. Aliguliyev r.aliguliyev@gmail.com Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan

National Security Council and the CIA were first established under this law.

In 1994, the UN proposed a new approach to the concept of "security" for the 21st century (Alkire, 2003):

- Security refers not only to the country but also to the public;
- Security is achieved not only through the possession of the military force but also through the development;
- Security refers not only to the state but also to a person at house and at work;
- Security is a protection against the conflicts not only between states but also between nations.

Traditionally, the concept of "security" is defined as "lack of threat, stability, protection, safety and reliability."

According to the legislation of the Republic of Azerbaijan, security is the protection of the state independence, sovereignty, territorial integrity, constitutional order, and the national interests of people and country, the rights and welfares of people, society and state against the internal and external threats. However, some researchers believe that security should not be considered just as some state. From this point of view, security is also the relationship and features of a particular system, as well as the conditions and consequences of the activities of the relevant structures aimed at ensuring a certain level of security.

The concept of the national security of the Republic of Azerbaijan specifies that the security environment of the Republic of Azerbaijan is a combination of factors affecting its sovereignty, territorial integrity, inviolability of borders, national interests, sustainable development, protection of welfare and values of the population (National Security Concept of the Republic of Azerbaijan, 2007).

Recent concepts define security as a level of protection of vital interests of an individual, society and state against internal and external threats. The vital interests include a set of needs that efficiently ensure the activities and development of an individual, society and state (Zelikow, 2003).

The interests of an individual include the realization of constitutional rights and freedoms, the provision of personal security, the improvement of living standards, and the physical, spiritual and intellectual development.

The interests of society include the issues, such as ensuring democracy, establishing a legal and social state, achieving and supporting the public solidarity, and improving the moral environment.

The interests of state include the inviolability of the constitutional system, the sovereignty and territorial integrity, the provision of social and political, economic and social stability, legislation and legal order, and the development of mutually beneficial international cooperation with equal rights. The full coverage of the interests of all three parties is expressed by the concept of "national security".

The sovereignty of any state refers to its national security. Therefore, ensuring the national security is one of the most important functions of the state. The countries that fail to ensure the national security loses their sovereignty, and their domestic and foreign policies are determined by other more powerful countries. The national security of each state is also an integral part of the international security.

The following methods for ensuring security are available (Donohue, 2011):

- risk management;
- increasing the resistance to destructive effects (for example, enhancing immunity in health care, establishing a system to eliminate the effects of destructive effects);
- creating a system and tools for protection against threats;
- destruction of sources of danger.

Three levels are distinguished for their scale of security:

- global security;
- regional security;
- national security.

Security can be classified by specific features as follows:

- object – person, society, state;
- fields – economic, social, socio-political, information and so on;
- scale of damage – excessive, significant, insignificant;

- probability of occurrence – high probability, probability, less probability;
- reasons of occurrence – natural, intentional;
- hierarchical principle – interplanetary, global, regional, interstate, national, internal regional, corporate, local, personal.

National security as a complex and multi-level system covers all fields of activity. It represents a set of subsystems each of which has its own structure.

Each of the fields of activity and vital interests is affected by various threats. Therefore, security objects have to be divided into the components according to their fields of activity. It is of practical significance. Based on this principle, the vital interests, threats and fields of national security can be categorized as follows (Figure 1):

- social and political security;
- economic security;
- military security;
- information security;
- scientific and technological security;
- education system security;
- healthcare system security;
- food security;
- energy security;
- transport system security;
- mass media security;
- environmental security;
- cultural and spiritual security.

Different areas of national security are interconnected and cannot be achieved without one another. This article highlights the growing role of the information security in the national security system in the information society. The interrelationship of various components of the national security with the information security is investigated. The characteristics of ICT application and informatization, the main threats to information security in these areas that constitute different components of the national security and their prevention ways are studied.

2. The role and place of information security in the national security system

Currently, the concept of cybersecurity is used in the relevant scientific literature in parallel with the concept of "information security". In some cases, these terms are also used synonymously. However,

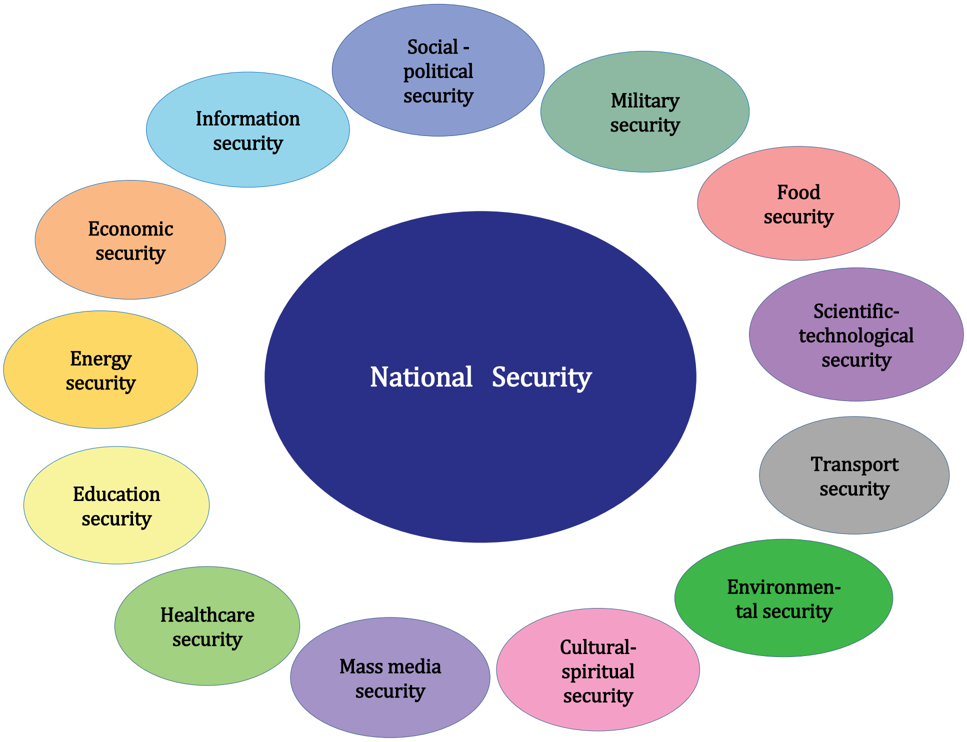

Figure 1. National security components.

we believe that “information security” is a broader concept and that cybersecurity is an integral part of it. Thus, information security covers both the physical and electronic information environment. And cybersecurity covers only the electronic information environment. Today there is a sufficient amount of information resources on physical media that act as an object of security, which constitutes legal categories, such as state secrets, trade secrets, intellectual property, personal information. Therefore, we consider it more appropriate to use the term “information security” in the article.

Information security refers to the protection of information and information systems against unauthorized access, use, disclosure, modification or destruction to ensure confidentiality, integrity and availability (Andress, 2014).

In other words, information security is the protection level of the national interests of the country within the information sphere (on a balanced basis of vital interests of an individual, society and state) against internal and external threats (Imamverdiyev, 2015b).

From another perspective, information security is a set of qualitative indicators that ensure the integrity, management, essence, different potentials and reputations of the object’s features and development directions (Alguliyev et al., 2017).

The interests of an individual in the field of information include the issues such as the information availability, the use of information for the purposes not prohibited by law, for physical, moral and intellectual development, as well as for the protection of personal information and the information that ensure the personal security.

The interests of the society in the information sector include ensuring the interests of an individual in this area, strengthening the democracy, formation of a legal state and achieving the social solidarity.

The interests of the state in information sphere consist of the sustainable and balanced development of the information infrastructure of a country, the creation of favorable conditions for the realization of constitutional rights of citizens in terms of information, protection of the state information resources against illegal access, and ensuring the security of information and telecommunication systems of a country.

According to the relevant concepts of a number of countries, the objects of information security are (Alguliyev et al., 2017):

- information resources (information resources on physical and electronic media that constitute state secrets, trade secrets, confidential and generally accessible information resources);
- systems for the formation, distribution and use of information resources (information systems for various purposes, libraries, archives, databases and banks, etc.);
- information infrastructure (information analysis and processing centers, information exchange channels and telecommunications, information protection systems and facilities);
- the system of formation of public consciousness (worldview, political views, moral values, etc.)
- information and legal system (information rights of citizens, legal entities and the state, protection of confidential information and intellectual property, etc.)

The main objectives of the national security in information sphere may include (Alkire, 2003; Sidorkin & Iroshnikov, 2019; Zelikow, 2003):

- ensuring a sensitive balance between the implementation of information rights of citizens and the information security;
- promoting the information infrastructure, supporting the development, dissemination and application of new information technologies in all required areas, unifying the tools for information retrieval, collection, storage, processing and analysis with the global information infrastructure requirements;
- improving the legal framework for the information security, and coordinating the activities of relevant government agencies;
- developing the national telecommunications and information technology industry;
- reliably protecting the public information resources in government agencies and other strategic areas.

In the modern era, when ICT is rapidly developing and deeply penetrating into all areas of the society and all fields of activity, and as a result, the information society is formed, the information security is closely linked to the national security and its various components.

At the current stage of development of statehood and society, the problem of national security is extremely complex, complicated and multifaceted, and its information components are becoming more vivid. Thus, ICT begins to play an increasingly important role in the provision of the national security and stability. Therefore, all developed countries particularly focus on the creation and development of various information infrastructures and systems to ensure high level of national security.

The level of public awareness, the existence and availability of the reliable information on the status and development of economic, socio-political and social processes define the capabilities of the government structures and society to make effective decisions in the socio-political, military, economic, environmental, social and cultural spheres. In this regard, information becomes crucial for the sustainable development and security of the society.

In the new era, information security is becoming more important than other components in the national security system. Thus, information has become the most valuable resource of mankind, and all progressive innovations in science, education, management, economy, business, society, significant events are related to information and knowledge production. In the information society, all fields of human activity are transferred to the information space, and information processes also cover the social, socio-political, legal, economic, psychological, cultural and other relationships. Simultaneously, the negative effects of information processes are becoming more distinct and increasing the risks of cybercrime, cyberterrorism and information warfare (Alguliyev et al., 2017).

All these fields are important elements in the protection of vital interests in various areas of national security. With the emergence of new development fields and application areas of ICT, the scope and, accordingly, responsibilities of information security are expanding.

With the advent of big data analytics, cloud computing, inexpensive and advanced sensors, and broadband mobile communication, all manufacturing and service industries called the “4th Industrial Revolution” have radically changed (Hofmann & Rüsch, 2017). The main feature of these technologies is that without human intervention and the functioning of an autonomous decision-making system provides foundation for the next – fifth industrial revolution (Özdemir & Hekim, 2018). Industry 5.0 will base on robotics and artificial intelligence. However, the information security threats of these technologies are still poorly studied, and the relevant risks related to their application are required to be assessed (Ataç & Akleylek, 2019; Lu, 2017).

3. Social and political security and information security

One of the most important components of the national security is socio-political security. The level of social and political security is an indicator of the government activities. In other words, the violation of social and political security refers to the paralyzed government and chaos. The status of other components of the national security also depends on the level of social and political security. Security in the military, economic, social and other areas cannot be achieved without the social and political security and stability in any country.

From the point of view of local (national) conditions, the socio-political security means the stability of the social and political system in the society and country, the basic interests of all social groups, the basic human rights and freedoms, and the lack of socio-political conflicts (Margolis, 2010).

From the external point of view, the social and political security is the level of protection of the constitutional system, sovereignty, territorial integrity and national interests of a country by the state authorities in the international arena.

The social and political security is also a matter of realizing the principles of social justice in the society, providing citizens with the minimum level of social welfare and high living standards. Ensuring the social and political security is, in fact, a guarantee of the social stability.

Today, ICT plays an important role in both securing and disrupting the social and political security. For example, in the provision of a number of basic human rights and freedoms, including education rights, freedom of expression, freedom of information, creativity, the right to participate in governing, the right to appeal, the right to privacy, the right to life, equality, property rights, housing rights, marriage rights, labor rights, leisure, social security, etc., ICT provides broader opportunities that have been never available before. At the same time, any country has the opportunity to use information warfare technology to disrupt the social and political stability through ICTs (Beskow & Carley, 2019).

There is a great need for the information security measures to safeguard the stability of the technological environment created to secure the rights and freedoms, as well as to protect against the ideological and technological implications targeted at undermining the social and political stability.

The state governing bodies are the most important objects of the social and political security. The current public administration system, which is formed and developed through the use of ICT, is the most responsible field of e-government information security. Provision of the technological infrastructure, electronic document circulation, e-signature authentication system, protection of state secrets, personal information protection, accessibility of the public information resources on the e-government platform, etc., are important tasks in the field of information security.

4. Military security and information security

Military security of the state is the level of protection of the constitutional system, social and political, economic and social stability and the stability of the society against the threats and dangers and military aggression (Brooks, 2005).

The role of the information factor in the military security structures of the developed countries is increasing. These countries effectively use the information resources and technological opportunities to enhance their military capabilities and strengthen their defense systems (Szpyra, 2014).

The information protection system of a state, along with other components, as a complex structure, is also responsible for the military information protection. The main information objects to be protected in the military sphere are: central military management, information infrastructure of the governing bodies of separate types of troops, formations and military units; automated control systems of troops, military equipment and weapons.

In addition, a number of specific tasks are being implemented in the engineering forces, with greater burden of information: preparation of battlefields, surveillance, engineering investigation, concealment of personnel, techniques and positions, defining the routes, removing the obstacles, and so on. In modern world, the capabilities of information technology are widely used to realize such combat tasks (Kramer et al., 2009).

Transmission and processing of information during the engineers' management involve the following processes: collecting military-engineering information about the current situation and converting it from text into graphical form (cryptography), transmitting graphic information to higher authorities, converting the graphic information into text, processing and evaluating the information and relevant decision-making, and converting the decisions made into graphical form and transmitting them to the local military units and converting them back into text again (Imamverdiyev, 2015b).

The process of developing and changing the military maps, which are of the key warfare documents, is also directly implemented through information technology. These maps ensure a flexible and accurate visualization of the current tactical situation. Modern armies are widely using robotic devices and unmanned aerial vehicles for remote investigation and other purposes.

Successful implementation of these processes, first of all, requires high-level information security. In this regard, special military units, i.e., cyber troops are formed in several countries (Imamverdiyev, 2015c).

Information Warfare is one of the issues closely related to the military security (Alakbarova, 2010). History shows that, in each era, along with the military operations, information weapons and information attacks were also used. The party that more successfully uses this method has additional opportunities to achieve its goal.

During the second half of the twentieth century, information technology has been actively and successfully applied in military operations. This is due to the development and new opportunities offered by ICT.

One of the main goals of the information warfare in parallel with the military operations is to spread provocative disinformation, discouraging, frustrating and harassing the opposite army or the entire population. Rapidly developing ICT provides great opportunities for such psychological effects. In this regard, one of the main tasks of information security is to be prepared for the information warfare and take relevant measures to prevent it if real threats occur.

5. Economic security and information security

Economic security is a state of ensuring the minimum required volume of national production by economy and its various sectors (finance, banking, investment, tax, etc.) for independent existence and development of the country. Moreover, protection of the strategic economic resources of the country against the influence and control of adversarial and criminal forces represents the protection level of the basic economic rights and freedoms (Alguliyev and Mahmudov, 2013a).

Ensuring economic security is one of the main conditions for successful provision of the country's sovereignty, stability and normal functioning of society. This is explained by the fact that the economy is one of the most important activities of the state, society and individuals. The national security cannot be ensured if the economic security is absent. Therefore, economic security is considered to be one of the topmost priorities of the state (Alguliyev and Mahmudov, 2013b).

Information technologies, including Internet technologies have been recently widely applied in management, finance, technical infrastructure, production, services, household and others spheres. Affected by these technologies, traditional areas such as banking, public administration, healthcare, education, mass media, transport and communications are undergoing serious transformations. The more the role of information and information technology in the economic field grows, the more information security issues are beginning to play an important role in the economic sector.

The new economy is based on information and knowledge. Information and knowledge have already become increasingly important among the key factors of production and services. An information resource is also added to the traditional resource types in the information economy. High efficiency in material production is possible only due to the collection, processing and use of information resources. Information resources are materialized in the form of documents, databases, algorithms, computer programs, literature, art and scientific works. Information resources of the country, region and enterprise, by their importance, are referred to the strategic resources, such as raw materials, supplies, energy, minerals and so on.

The main technologies of information- and knowledge-based economy may include (Hadad, 2017):

- Big data;
- neurotechnology and artificial intelligence;
- nanotechnologies;
- distributed registry systems (blockchain);
- quantum technology (quantum information, quantum computers, quantum cryptography, etc.);
- Internet of Things;
- robotics;
- virtual and augmented reality technologies;
- 3D printer;
- and so on.

Modern concepts of formation and development of information- and knowledge-based economy mainly address the following issues (Tang, 2015):

- legal regulation;
- education and human resources;
- scientific research;
- development and implementation of new technologies;
- development of information infrastructure;
- provision of information security.

One of the most important aspects of economic security is the security of its infrastructure (Alguliyev and Mahmudov, 2013b). Infrastructural security is a condition for ensuring continuous and unhindered operation of the national economy infrastructure. In this area, continuous and effective implementation of the social production processes is achieved by ensuring fault-tolerance. The goal of providing infrastructural security is to ensure the necessary initial infrastructure conditions for the provision of the consumers with the infrastructure services and the security of the products provided, as well as for the sustainable operation of the country's economic system in the presence of internal and external threats to vital economic interests.

The main threats to the security of the economic infrastructure may include:

- depreciation and technological decline of the infrastructure;
- infrastructure development lagging behind the services and production sectors;
- deformation of the structure of the infrastructure environment;
- high material capacity of the infrastructure complex;
- suppression of the national infrastructure complexes by foreign analogs in the domestic market.

With the widespread and comprehensive use of ICTs, major qualitative changes occur in the economic infrastructure. Micro and macro-economic entities that are left out of the process are guaranteed to lose competitiveness. Therefore, deterioration of the material and technical base and technological decline of the infrastructure complex is the most important factor in the threats to the infrastructure security. Elimination of the deterioration of the material and technical base and technological deficiencies mentioned above can be achieved through effective use of ICT. The high material capacity of the infrastructure complex is also referred to the threats to the infrastructure security. To overcome this risk, the high material capacity of the infrastructure complex is required to be significantly reduced. This can only be realized through the use of information and science-based technology.

Another important aspect of economic security is production security (Alguliyev and Mahmudov, 2013b). Production safety is the protection level of the economic interests in the manufacturing sector. The purpose of production safety is to create conditions for the stable operation of production facilities and the release of competitive products with the most efficient use of all available resources.

Recently, the process of rapid informatization of traditional industries and services is underway (Petrenko, 2018). Information technology, including e-document circulation, is used in business management, production and service processes. All documents and information stored in paper are converted into electronic form. Various databases and information systems are created at the enterprises. All of them also act as the subjects of information security. Therefore, the importance of information security in manufacturing and service enterprises is highlighted.

One of the main trends in the economy under the influence of information technology, especially the Internet, is digitalization (Ozili, 2018). That is, a person does not interact with real objects, but their images and symbols through advanced technical devices. The process of digitization is more common in financial and monetary systems. In addition, paper currencies and metal coins are replaced by electronic money, cash payments by cashless payments, and electronic payment systems are emerging and developing.

Financial security is one of the most important components of economic security (Abbosh & Bissell, 2019). Financial security affects virtually all economic activities of the country, both at the macroeconomic and microeconomic levels. That is, financial security is an important factor for the sustainable functioning of the entire system of economic relations in the country. Ensuring the financial security of the country is related to the proper implementation of fiscal, monetary and currency regulation policy.

With the advent of electronic money and electronic payment systems, financial security, which is an important area of economic security, has also begun to act as information security.

In general, the main threats to information security in the economy are as follows (Abbosh & Bissell, 2019; Teoh & Mahmood, 2017):

- state statistical system;
- finance and credit system;
- intelligent information systems and bases that ensure the functioning of society and state in the economic sphere;
- accounting system of enterprises and organizations, irrespective of their ownership form;
- systems for collection, processing, storage and transmission of information related to financial, exchange, tax, customs, foreign economic activity of the state and individual enterprises and organizations, regardless of their ownership form.

The purchase of informatization, telecommunications and information security products from abroad also makes the country technologically dependent on imports. This should be considered as one of the serious information threats in the economic sphere. Cybercrime is also one of the main threats to the normal functioning of the economy.

Moreover, one of the serious threats to information security is the insufficient legal and regulatory framework to define the responsibility of business entities for dissemination of disinformation or concealment of information about their commercial activities, as well as about the consumer characteristics of their products.

In general, the following measures at the state level are required to ensure information security in the economic sphere (Abbosh & Bissell, 2019; Teoh & Mahmood, 2017):

- organization and implementation of state control over the establishment, development and protection of systems and tools for collection, processing, storage and transmission of statistical, financial, exchange, tax, customs and other information;
- development and implementation of the national electronic payment systems protected on the basis of intellectual card, electronic money and e-commerce systems;
- improvement of the regulatory framework governing the information relations in the economy;
- improvement of human resources training in the collection, processing, storage and transmission of economic information.

6. Energy security and information security

Energy security is the level of protection of the country, citizens, society, and the economy against the threats to the reliable fuel and energy supply (Ang et al., 2015). These threats are identified by external factors (geo, socio-political, macroeconomic, conjuncture, etc.), as well as by the state and activities of the country's energy sector.

The main principles of energy security may include (Bompard et al., 2017):

- reliable energy supply of strategic and important facilities;
- replenishment of consumed fuel resources;
- diversification of fuel and energy types;
- consideration of ecological requirements;
- prevention of inefficient use of energy resources;
- insufficient revenue of energy resources in domestic and foreign markets and creation of free economic conditions for efficient export;
- and so on.

Power systems and facilities are referred to the critical facilities (Cai, 2018). Because, in modern age, the activities of public life, all services and production areas, and the activities of public administration bodies depend on safe and stable operation of the energy system. Therefore, information security in this area is of critical importance (Onyeji et al., 2014).

Currently, electricity generation, its connection to a single system, transmission and delivery to consumers also cover a very multifaceted and complex process. All these processes are implemented through ICT.

Recovery of alternative energy sources and finding alternative sources using the capabilities of the Industry 4.0, namely of the network of intellectual sensors, cyber-physical systems and supercomputers, in other words, the development of "green" smart energy, which is a part of the "green" economy, is one of the most important challenges for mankind (Biresselioglu et al., 2018).

In the modern world, energy security is one of the most important areas of the national security. The use of ICT in all areas of activity, the processes of information society formation are "nourished" by electricity. Unlike the agrarian and industrial societies, the information society is experiencing a stage of development completely dependent on electricity. Therefore, one of the most important issues in the building of the information society stated in the "ideology of the millennium" is the sustainable and safe energy supply. As a result of power cuts, the activities of the state, manufacturing and service sectors may become paralyzed, with significant financial losses (Venkatachary et al., 2017).

Generally, energy is one of the strategic areas that requires special complex measures to ensure information security. The main object of energy protection is not information, but technological process and management system (Yadav & Paul, 2019). In this environment, security system is required to ensure the integrity of the technological process and continuity and efficiency of control (Khan et al., 2016; Pourbeik et al., 2006). The importance of information security in the energy sector is determined by the consequences of the implementation of relevant cyber-threats. This is not just a material loss or reputational damage, but also a damage of health of citizens, environmental deprivation, serious damage to the military, economic, transport, communications and social infrastructure, and paralysis in all areas.

7. Food security and information security

Food security is one of the main human rights. Therefore, the enforcement of this right is considered an important objective of each state. Food security is the level of sufficient nutrition of every person for healthy and productive lifestyle. Solution to this problem is, first of all, related to poverty reduction, improvement of the efficiency of food supply and consumption (Godfray et al., 2010).

According to another approach, food security is the capacity of national producers to provide the population with acceptable nutrition and calories, in accordance with the appropriate medical norms, regardless of war or military conflict.

Food security is related to a number of areas:

- production;
- raw materials;
- finance;
- scientific and technical;
- socio-demographic;
- labor market security;
- public;
- information security;
- and so on.

ICT capabilities are now widely used to ensure food security. All the necessary information is provided through ICT to carry out farming activities: agro-business models, real-time weather forecast, agricultural and agro-technical information, calendars, and so on (Aker et al., 2016).

The opportunities, such as observation and monitoring of agricultural facilities and real-time processes, sensing operative and accurate information from these facilities, analyzing and making management decisions are important for the safety of food products and drinking water resources. Such analytical information systems act as a common object of both food security and information security (Mohanraj et al., 2016).

Systematic monitoring of food stocks is considered to be one of the most important measures to ensure food security. Such monitoring implemented through advanced ICTs and space satellites includes the followings (Gebbers & Adamchuk, 2010):

- remote probing of agriculture and water resources;
- application of computers, networks, databases, software, Big Data, CIS technologies for the collection, analysis and use of food safety information;
- use of network infrastructure to inform farmers and consumers.

The main task of information security in the field of food safety is to ensure the completeness, confidentiality and availability of the information necessary for relevant management structures, decision makers and consumers (Cooper, 2015).

There are also other important issues that are common to food security and information security: unauthorized seizure and disclosure, misuse, destruction or loss, falsification of food information, and manipulation of such information and so on. These threats can also be realized by external agents, cyber criminals, dissatisfied employees, and spies of the rival company.

Formation and development of electronic agriculture further enhances the role of information security in the food sector. The use of ICT in electronic agriculture involves the planning, development and implementation of innovative methods in plant growing, livestock, fishing, forestry and water management. In a broader sense, e-agriculture covers the issues, such as the application of relevant technologies, activities, support for the development and implementation of norms and standards, capacity building, human resources training and dissemination of knowledge (Fernando et al., 2016).

8. Scientific and technological security and information security

In the modern era of the emergence and development of the information society and knowledge economy, the importance of the scientific and technological field for national security is growing. The economic and military power of any state is linked to its scientific and technological potential (R.M. Alguliyev & Imamverdiyev, 2010). The great French scientist L. Pasteur wrote that "science should be of the highest value in the country; the nations that are ahead of others in the field of intellectual activity will always be leaders in other areas." Indeed, the countries that are more advanced in science and technology, today, are more involved in political, economic, military, cultural, etc.

They also have the potential to significantly influence other countries in mentioned areas.

Science and technology play a key role in ensuring the national security in all areas, and they also need to be secured. In particular, there is a great need to protect scientific and technological activities from the information security aspect in the modern era.

The main objects of scientific and technological security of the state are (Mowery, 2009):

- results of fundamental and applied scientific researches important for scientific, technological, socio-economic development of the country;
- inventions, non-patented technologies, industrial designs, utility models and experimental equipment;
- scientific and technological personnel and their training system;
- management of complex research facilities;
- and so on.

External threats to information security in scientific and technological activities may (Halbert, 2016; Mayers, 2018):

- unauthorized access attempts to national scientific and technological resources by developed countries;
- restrictions of the development of national scientific and technological potential through providing the privileged terms for foreign scientific and technological products in the local market;
- realization of the industrial espionage within the country by foreign state and commercial organizations;
- attraction of perspective scholars and specialists working in strategically important areas of the country by foreign countries through socio-economic motivation.

Internal threats may include:

- decrease in financing of scientific and technological activity;
- decrease in the youth's interest in these areas as a result of reduced prestige of the scientific and technological fields;
- lack of production of competitive products in the field of information technology and other high technologies which ensure technological independence of the country;
- presence of serious problems in the field of patent protection of the results of scientific and technological activities.

The following issues are to be solved to ensure scientific and technological security of the state (Tabansky, 2016):

- realization of national scientific and technological capacity building;
- development of priority areas of scientific research and technology, ensuring international competitiveness of the national economy;
- provision of the confidentiality and protection of high-risk industries, research organizations, strategic enterprises and organizations that are the objects of state secrets;
- control over the export of technology and scientific developments;
- protection of intellectual property rights in the field of foreign economic activity and scientific and technological cooperation;
- intelligence and counter-intelligence activities in the field of technological and scientific developments of strategic importance;
- regulation of physical and virtual "brain drain" to foreign countries.

9. Education system security and information security

The education system is of vital importance for national security (Klein & Rice, 2014). In other words, human factor is at the forefront of security. The education system plays an exceptional role in the development of human resources, personality, formation of their outlook, intellect, national-moral values and patriotic spirit.

Thus, one of the strategic foundations of the national security system is related to education. Education is equally vital for all three levels of national security: personal, social and state (Orikpe, 2013).

The specific weight of the information component of the education system and process is very high. Thus, the content of textbooks, manuals and lessons taught by teachers must meet the requirements of national security and information security which is an important component of it. The educational process should be protected from advertising and promotion on any subject matter prohibited by law.

Digitalization of textbooks, manuals and libraries, the emergence of electronic textbooks, and the availability of additional knowledge and information beyond the control of the educational system used by students and pupils on the Internet make the security issues even more complicated. Therefore, security of information related to the education system is entrusted with a lot of responsibilities (Dai et al., 2016).

One of the major threats to information security in education system is the seizure of confidential information, for example, the theft of exam questions stored in electronic databases. In addition, the issue of ensuring the security of online exams, as well as distance learning processes, is also relevant.

The following measures have to be taken to ensure information security in the education system (Bialaszewski, 2015; Pires & Moreira, 2012):

- protecting computers used in the educational process against unauthorized access (viruses, hacker attacks, etc.);
- filtering the Internet traffic at educational institutions;
- conducting serious expertise of printed and electronic versions of textbooks and manuals, protection of their integrity;
- informing the teachers, pupils and students about the essentials of information security and mastering an information culture.

One of the key elements in ensuring information security is the training of highly qualified specialists in this field who are able to apply their knowledge in real-time and respond quickly to emerging cyber threats. There is a great demand for information security specialists in the global labor market (Thomson et al., 2019).

10. Healthcare system security and information security

The strategic goals of ensuring national security in the health sector may include (Feldbaum et al., 2006): to extend life expectancy, to reduce disability and mortality; to improve timely provision of first medical aid and high-tech medical care; to improve the standards of medical care; to improve the quality, effectiveness and safety control of medicines, reliable protection of patients' rights, etc.

The main threats to national security in health care may include (Fidler, 2003):

- spread of large-scale epidemics and pandemics;
- spread of immunodeficiency virus, tuberculosis, drug addiction and alcoholism;
- increase of availability of psychoactive and psychotropic substances;
- and so on.

It is required to improve the quality and availability of health services through the use of ICTs to strengthen the national security in healthcare sector, to provide state support for promising research in pharmaceuticals, biotechnology and nanotechnology, to improve economic mechanisms and to reinforce the material and technical base (Blaya et al., 2010).

Hospitals, medical centers and other health care facilities generate large amounts of personally identifiable information about patients. Many documents refer to the legal category of physician-patient privilege. These data and documents are currently circulating electronically in various information systems and stored and analyzed in certain databases. Medical institutions are shifting to the electronic document management system, and the patients' electronic registration system is formed. Note that medical data are the most sensitive category of personal data (Chenthara et al., 2019).

With the application of ICT in the field of medical activity, e-medicine, cyber-physical and cyber-biological systems are formed. In addition, remote medical services are provided, e-health cards are issued to citizens, and the ICT is widely used in the diagnostic and investigative procedures and numerous surgeries.

Many medical devices are also widely using operating systems, so they are also vulnerable to attacks, conventional computers. However, devices with special operating systems can also be exposed to cyber-attacks, and a software update mechanism is often used for it (Pandey et al., 2019).

As a result of the fast informatization of the health care system and the emergence of electronic medicine, the level of dependence of the medical system on ICT and information security is also increasing (Y.N. Imamverdiyev, 2016).

11. Transport system security and information security

The transport system is a very critical area in terms of security. Security of transportation infrastructure and facilities requires large amounts of financial and human resources. Because this area is concerned with the human safety, and the security of valuable raw materials and finished products, and the accidents in this field often lead to mass casualties and large financial losses (Theoharidou et al., 2011).

The transport system is designed to meet the transportation needs of people and includes vehicles, transport facilities (infrastructure), transport enterprises, hierarchy of transport system management, and the environment.

Transport infrastructure includes highways, railways, air corridors, waterways, canals, tunnels, bridges, pipelines, transport nodes or terminals (airports, highways and railway stations, seaports, etc.).

Vehicles include conveyors, ships, elevators, wings, loading cranes, jets, cars, bicycles, motorcycles, buses, trams, trolleybuses, trains, planes, and so on.

Transport and communication are closely interconnected areas. The fast development of transport and services in the modern world is also due to the rapid growth in telecommunications.

At the same time, the modern transportation system cannot be imagined without information technology. Intellectual transport management systems are being successfully implemented around the world today, enhancing productivity in this area, providing high-quality services, providing optimal management and security directly through the capabilities of information technology (Thomopoulos et al., 2015).

Passengers, vehicles and equipment are also automatically identified. In addition, online monitoring of traffic, passengers and cargo are realized. Online video surveillance systems and sensor networks are used to safeguard the transport infrastructure (roads, bridges, tunnels, pipelines, channels, etc.). Intelligent systems are used to regulate the traffic. Moreover, all types of vehicles themselves become intelligent and “smart”.

Moreover, in the transport system, there is a large volume of personal data concerning the passengers, service personnel, information that is a state secret, a trade secret.

In addition, although the e-mail system evolves, it is advisable to transmit some official letters, documents in hard copy through physical mail for security and privacy reasons.

All processes implemented in the transport system with the use of ICT, infrastructure facilities, vehicles, information circulating in this system, including physical mail information become the object of information security (Dellios et al., 2015).

12. Ecological security and information security

Ecological security is a state of the environment and normal living conditions protected against the consequences of negative economic activities of the, as well as natural disasters and so on.

In the relevant legislation of the Republic of Azerbaijan, ecological safety is defined as “ensuring the vital interests of the person and society and protection of the environment against the anthropogenic and natural impacts on it.”

The state has a number of responsibilities to ensure ecological security. One of these tasks is to organize and implement information support. Appropriate information support includes monitoring of the environment and natural resources, gathering and analyzing the necessary information, making adequate decisions and taking measures, as well as disclosing information on the condition of the ecology, ecological damage and hazardous ecological impacts.

In modern times, all these processes are implemented using information technology. Thus, the use of the Internet of Things, sensor networks to obtain accurate and operative information from ecological objects. Security of these information systems is of critical importance in terms of ecological security. Accurate and reliable information on any ecological disaster should be timely obtained so that preventive measures can be taken (Popović et al., 2017).

With the development of ICT, a new trend in ecological security, namely electronic waste security is becoming more relevant (Alghazo et al., 2018). In recent years, the volume of e-waste has been increasing rapidly. Such wastes seriously harm human health and environment. Some of the electronic waste includes data storages. Practice shows that data storages thrown away as waste contain confidential information of a different nature. Alternatively, such data may, at first glance, be viewed as insignificant, however confidential information can be obtained from them through Big Data technology. Therefore, relevant electronic waste acts as an object of information security. The main task of information security in this area is to reliably destroy the data stored on those electronic storages (Aghayev & Aliyeva, 2013).

13. Mass media security and information security

Provision of mass media security is of particular importance in the national security system. Thus, any inaccurate, biased, provocative information disseminated by the media that serves as an information provider for citizens can pose serious problems for national security and socio-political stability in the country (McLeod & Shah, 2014).

Since information is an object of mass media performance, the activities of this area are common for information security. The main task of information security related to media is to protect the national interests.

One of the key indicators of the level of information security of the media is its sustainability to information warfare operations. In this regard, the necessary technological base and human resources are required to ensure this sustainability (Taylor, 2015).

Particularly in case of emergency situations, the function and importance of the media increase much, and it is necessary to provide operative, comprehensive and reliable information to the citizens, public, so that no any negative tendencies, such as confusion, frustration, and so on, do not occur. In this regard, one of the key objectives of information security in media is to ensure the availability of certain information sources (Henrichsen et al., 2015).

Media transformation and convergence with the influence of ICT, the emergence and development of the Internet media, the opportunities to meet online demand for information operatively, and the formation of civic journalism further complicate information security in this area. Under these conditions, the opportunities for various information crimes also increase (Thakur et al., 2019).

14. Security of cultural and spiritual sphere and information security

Cultural and moral security is the protection level of the public consciousness and the spiritual and moral health of people, as well as the protection of the traditional moral values and lifestyles against the internal and external negative effects. The state's responsibility in this area is to protect the moral norms, traditional confessions, national and cultural traditions, historical traditions and values (Giles, 2011).

The main objects of information security in the cultural and moral sphere of the state are:

- personal dignity;
- freedom of conscience;
- freedom of choice and dissemination of religion and other beliefs;
- freedom of speech and expression;
- freedom of literary, artistic, scientific, technical and other creativity;
- inviolability of personal life, personal and family secrets;
- main communication language and language of the national minorities, moral values, historical and cultural heritage;
- intellectual property.

The main threats to national security in the cultural and spiritual sphere are as follows (Colarik & Janczewski, 2015):

- negative effects of mass cultural products (clothing, behavior, lifestyle, etc.) aimed at the spiritual needs of different groups of population;
- illegal aggression against cultural objects;
- illegal propaganda to promote national values;
- generation of a negative opinion about the history of a country, its people and historical personalities;
- promotion of racial, national, religious discrimination and intolerance;
- activities aimed at violating the literary norms of the state language or the main communication language.

To develop the culture of the national minorities against the national security threats in the cultural sphere, it is important to enhance the effectiveness of state regulation, to promote tolerance and mutual respect in society, to strengthen the intercultural relations, to protect and develop the cultures of the national minorities and the cultural values of nationalities and citizens, to strengthen the technical bases of cultural and leisure facilities, to propagate and develop the cinematographic and print products, television and radio broadcasting and the Internet content promoting the national and moral values, to provide their accessibility, to organize the state orders to increase the volume and quality of such products, to develop the ethnotourism and to take relevant measures.

Serials, TV programs, Internet video-materials, e-books, and other digital resources produced by various countries for cultural and spiritual purposes directly become the subject of information security.

Ensuring information security of the country in cultural and spiritual spheres is related to the use of a number of constitutional rights and freedoms, namely information rights, cultural and moral values, historical traditions and norms related to the development, formation and behavior of a person.

Obviously, each of the above-mentioned strategic cultural objectives of the state in the cultural field, and the threats and measures to address them, is informative and has a high information burden. In other words, both positive and negative processes taking place in the cultural sphere are implemented through ICT and electronic media tools.

In order to ensure information security in the cultural and spiritual sphere, the state has the following responsibilities:

- to create socio-economic conditions for creative activities and activities of cultural institutions;
- to provide the access to the best national, foreign cultural and art samples for the general population by generating modern distributed information resources;
- to create opportunities for self-realization in the field of creativity through the improvement of cultural and educational work;
- to organize leisure time for the population and out-of-school mass creative education for children;
- to protect the cultural heritage of regions and national minorities and to support the initiatives in this area.
- to introduce the civilized forms and methods of social control over the formation and development of moral values that meet the national interests of the country;
- to develop the legal and organizational mechanisms for the prevention of negative information and psychological impacts on the public consciousness; to protect the moral, spiritual and historical values;
- to prevent TV and radio programs and Internet resources that promote violence, cruelty, and other behaviors contrary to public morality;
- to prevent the foreign missionary organizations in the country.
- and so on.

15. Conclusion

New attitudes, approaches, and methodologies are required to ensure the national security in the modern era where ICTs are rapidly developing and successfully being applied in all areas of human activity, and an electronic state and information society are emerging. The national security cannot be ensured through traditional methods and tools anymore. As the traditional society is replaced by the information society, its security issues are highly dependent on information and information technology factors.

The analysis of the informatization features of individual components of the national security and their relationship to information security also confirms that the concepts of "national security" and "information security" do not differ in content and essence. All components of national security are the object of information security.

All these require the revision of existing doctrines, concepts and strategies on national security, legal and regulatory acts in this field, and their adaptation to the modern conditions dictated by the ICT and information society.

ORCID

Rasim M. Alguliyev http://orcid.org/0000-0003-1223-7411
Yadigar N. Imamverdiyev http://orcid.org/0000-0002-3710-1046
Rasim Sh. Mahmudov http://orcid.org/0000-0003-1553-2395
Ramiz M. Aliguliyev http://orcid.org/0000-0001-9795-1694

References

Abbosh, O., & Bissell, K. (2019). *Securing the digital economy. Reinventing the Internet for trust*. Accenture.

Aghayev, B. S., & Aliyeva, K. T. (2013). Electronic waste and some aspects of information security of information carriers. *Problems of Information Society, 4*(1), 67–74. https://jpis.az/en/journals/76

Aker, J. C., Ghosh, I., & Burrell, J. (2016). The promise (and pitfalls) of ICT for agriculture initiatives. *Agricultural Economics*, *S1*(47), 35–48. https://doi.org/10.1111/agec.12301

Alakbarova, I. Y. (2010). Analysis and classification of information war technology. *Problems of Information Society*, *1* (2), 80–91. https://jpis.az/en/journals/29

Alghazo, J., Ouda, O. K. M., & El Hassan, A. (2018). E-waste environmental and information security threat: GCC countries vulnerabilities. *Euro-Mediterranean Journal for Environmental Integration*, 3(13), 1–10. https://doi.org/10.1007/s41207-018-0050-4

Alguliyev, R. M., & Imamverdiyev, Y. N. (2010). E-Government Information Security Management: Research Challenges. *Problems of Information Society*, *1(1)*, 3–13. https://jpis.az/en/journals/12

Alguliyev, R. M., Imamverdiyev, Y. N., & Mahmudov, R. S. H. (2017). Multidisciplinary scientific-theoretical problems of information security. *Problems of Information Society*, *8*(2), 32–43. https://doi.org/10.25045/jpis.v08.i2.04

Alguliyev, R. M., & Mahmudov, R. S. H. (2013a). Interactions between economic security and information security. *Proceedings of the First Republic scientific-practical conference on the problems of information security devoted to the 90th anniversary of the National leader Heydar Aliyev* (pp. 7–10).

Alguliyev, R. M., & Mahmudov, R. S. H. (2013b). The issues of ensuring the security of information economy. *Problems of Information Society*, *4*(1), 3–13. https://jpis.az/en/journals/69

Alkire, S. (2003). *A conceptual framework for human security*. University of Oxford: Queen Elizabeth House.

Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Ang, B. W., Choong, W. L., & Ng, T. S. (2015). Energy security: Definitions, dimensions and indexes. *Renewable and Sustainable Energy Reviews*, *42*, 1077–1093. https://doi.org/10.1016/j.rser.2014.10.064

Ataç, C., & Akleylek, S. (2019). A survey on security threats and solutions in the age of IoT. *European Journal of Science and Theology*, *15*, 36–42. https://doi.org/10.31590/ejosat.494066

Beskow, D. M., & Carley, K. M. (2019). Social cybersecurity: An emerging national security requirement. *Military Review*, *2*(99), 117–127. https://www.questia.com/library/journal/1G1-583695738/social-cybersecurity-an-emerging-national-security

Bialaszewski, D. (2015). Information security in education: Are we continually improving? *Issues in Informing Science and Information Technology*, *12*, 45–54. https://doi.org/10.28945/2253

Biresselioglu, M. E., Nilsen, M., Demir, M. H., Røyrvik, J., & Koksvik, G. (2018). Examining the barriers and motivators affecting European decision-makers in the development of smart and green energy technologies. *Journal of Cleaner Production*, *198*, 417–429. https://doi.org/10.1016/j.jclepro.2018.06.308

Blaya, J. A., Fraser, H. S., & Holt, B. (2010). E-health technologies show promise in developing countries. *Health Affairs*, *2*(29), 244–251. https://doi.org/10.1377/hlthaff.2009.0894

Bompard, E., Carpignano, A., Erriquez, M., Grosso, D., Pession, M., & Profumo, F. (2017). National energy security assessment in a geopolitical perspective. *Energy*, *(2017*(130), 144–154. https://doi.org/10.1016/j.energy.2017.04.108

Brooks, R. A. (2005). The military and homeland security. *Public Administration and Management*, *10*(2), 130–152. https://spaef.org/article/179/The-Military-and-Homeland-Security

Cai, T. (2018). Energy infrastructure security in the digital age. *International Journal of Public Administration in the Digital Age*, *2*(5), 12–22. https://doi.org/10.4018/IJPADA.2018040102

Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE Access*, *7*, 74361–74382. https://doi.org/10.1109/ACCESS.2019.2919982

Colarik, A., & Janczewski, L. (2015). *Establishing cyber warfare doctrine. In current and emerging trends in cyber operations*. Palgrave Macmillan.

Cooper, C. (2015). *Cybersecurity in food and agriculture. Protecting our future*. Excelsior College.

Dai, N. H. P., András, K., & Zoltán, R. (2016). E-learning security risks and counter measures. *Engineering Research and Solutions in ICT*, *1*(1), 17–25. https://doi.org/10.20544/ERSICT.01.16.P02

Dellios, K., Papanikas, D., & Polemi, D. (2015). Information security compliance over intelligent transport systems: Is IT possible? *IEEE Security & Privacy*, *3*(13), 9–15. https://doi.org/10.1109/MSP.2015.59

Donohue, L. K. (2011). Limits of national security. *American Criminal Law Review*, *4*(48), 1573–1756. https://scholarship.law.georgetown.edu/facpub/1010/

Feldbaum, H., Patel, P., Sondorp, E., & Lee, K. (2006). Global health and national security: The need for critical engagement. *Medicine, Conflict and Survival*, *3*(22), 192–198. https://doi.org/10.1080/13623690600772501

Fernando, E., Assegaff, S., & Rohayani, A. H. (2016). Trends information technology in E-agriculture: A systematic literature review. *3rd International Conference on Information Technology, Computer, and Electrical Engineering* (pp. 351–355). https://doi.org/10.1109/ICITACEE.2016.7892470

Fidler, D. P. (2003). Public health and national security in the global age: Infectious diseases, bioterrorism, and realpolitik. *George Washington International Law Review*, *35*, 787–856. https://www.repository.law.indiana.edu/facpub/416

Gebbers, R., & Adamchuk, V. I. (2010). Precision agriculture and food security. *Science*, *327*(5967), 828–831. https://doi.org/10.1126/science.1183899

Giles, K. (2011). “Information troops” - A Russian cyber command? *3rd International Conference on Cyber Conflict* (pp. 45–60).

Godfray, H. C. J., Beddington, J. R., Crute, I. R., Haddad, L., Lawrence, D., Muir, J. F., Pretty, J., Robinson, S., Thomas, S. M., & Toulmin, C. (2010). Food security: The challenge of feeding 9 billion people. *Science*, *327*(5967), 812–818. https://doi.org/10.1126/science.1185383

Hadad, S. (2017). Knowledge economy: Characteristics and dimensions. *Management Dynamics in the Knowledge Economy*, *2*(5), 203–225. https://doi.org/10.25019/MDKE/5.2.03

Halbert, D. (2016). Intellectual property theft and national security: Agendas and assumptions. *The Information Society*, *4*(32), 256–268. https://doi.org/org/10,1080/01972243.2016.1177762

Henrichsen, J. R., Betz, M., & Lisosky, J. M. (2015). *Building digital safety for journalism: A survey of selected issues*. UNESCO Publishing.

Hofmann, E., & Rüsch, M. (2017). Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry*, *89*, 23–34. https://doi.org/10.1016/j.compind.2017.04.002

Imamverdiyev, Y. N. (2015a). *Explanatory dictionary of information security terms*. “Information Technology” Publishing House.

Imamverdiyev, Y. N. (2015b). Problems of formation of the national cryptography policy in the information society. *Problems of Information Society*, *6*(1), 12–23. https://jpis.az/en/journals/104

Imamverdiyev, Y. N. (2015c). Cyber troops: Functions, weapons and human resources. *Problems of Information Society*, *6*(2), 15–25. https://doi.org/10.25045/jpis.v06.i2.02

Imamverdiyev, Y. N. (2016). E-health: Actual problems of information security. *The First Republican Scientific-Practical Conference “Multidisciplinary Problems of Electronic Medicine”* (pp.31–38).

Khan, R., Maynard, P., McLaughlin, K., Laverty, D., & Sezer, S. (2016). Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid. *The 4th International Symposium for ICS & SCADA Cyber Security Research* (pp. 53–63).

Klein, J. I., & Rice, C. (2014). *US education reform and national security*. Council on Foreign Relations.

Kramer, F. D., Starr, S. H., & Wentz, L. K. (Eds.). (2009). *Cyberpower and national security*. Potomac Books, Inc.

Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, *6*, 1–10. https://doi.org/10.1016/j.jii.2017.04.005

Margolis, J. E. (2010). Understanding political stability and instability. *Civil Wars*, *3*(12), 326–345. https://doi.org/10.1080/13698249.2010.509568

Maslow, A. H. (1954). *Motivation and Personality*. Harpaer & Row.

Mayers, A. M. (2018). *A study on how cyber economic espionage affects US national security and competitiveness* [Unpublished doctoral dissertation]. Northcentral.

McLeod, D. M., & Shah, D. V. (2014). *News frames and national security*. Cambridge University Press. https://doi.org/10.1017/CBO9781139022200

Mohanraj, I., Ashokumar, K., & Naren, J. (2016). Field monitoring and automation using IoT in agriculture domain. *Procedia Computer Science*, *93*, 931–939. https://doi.org/10.1016/j.procs.2016.07.275

Mowery, D. C. (2009). National security and national innovation systems. *The Journal of Technology Transfer*, *5*(34), 455–465. https://doi.org/10.1007/s10961-008-9100-4

National Security Concept of the Republic of Azerbaijan (2007). Qanun: http://www.e-qanun.az/framework/13373

Onyeji, I., Bazilian, M., & Bronk, C. (2014). Cyber security and critical energy infrastructure. *The Electricity Journal*, *2*(27), 52–60. https://doi.org/10.1016/j.tej.2014.01.011

Orikpe, E. A. (2013). Education and national security: Challenges and the way forward. *Journal of Educational and Social Research*, *10*(3), 53–59. https://doi.org/10.5901/jesr.2013.v3n10p53

Özdemir, V., & Hekim, N. (2018). Birth of industry 5.0: Making sense of big data with artificial intelligence, “the internet of things” and next-generation technology policy.

OMICS: A Journal of Integrative Biology, *1*(22), 65–76. https://doi.org/10.1089/omi.2017.0194

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, *4*(18), 329–340. https://doi.org/10.1016/j.bir.2017.12.003

Pandey, A., Singh, B., Saini, B. S., & Sood, N. (2019). Medical data security tools and techniques in e-health applications. In book: *Medical Data Security for Bioengineers*, 124–131, IGI-Global. https://doi.org/10.4018/978-1-5225-7952-6.ch006

Peou, S. (2014). *Human security studies: Theories, methods and themes*. World Scientific Publishing Company. https://doi.org/10.1142/8670

Petrenko, S. (2018). *Cyber security innovation for the digital economy*. River Publishers.

Pires, E., & Moreira, F. (2012). The integration of information and communication technology in Schools: Online Safety. *Procedia Technology*, *5*, 59–66. https://doi.org/10.1016/j.protcy.2012.09.007

Popović, T., Latinović, N., Pešić, A., Zečević, Ž., Krstajić, B., & Djukanović, S. (2017). Architecting an IoT-enabled platform for precision agriculture and ecological monitoring: A case study. *Computers and Electronics in Agriculture*, *140*, 255–265. https://doi.org/10.1016/j.compag.2017.06.008

Pourbeik, P., Kundur, P. S., & Taylor, C. W. (2006). The anatomy of a power grid blackout - Root causes and dynamics of recent major blackouts. *IEEE Power and Energy Magazine*, *5*(4), 22–29. https://doi.org/10.1109/MPAE.2006.1687814

Sidorkin, A. I., & Iroshnikov, D. V. (2019). Theoretical issues of "security" concept. *Journal of Politics and Law*, *3*(12), 34–39. https://doi.org/10.5539/jpl.v12n3p34

Smith, S., Hadfield, A., Dunne, T., & Dunne, T. (2008). *Foreign policy: Theories, actors, cases*. OUP Oxford.

Szpyra, R. (2014). Military security within the framework of security studies: Research results. *Connections: The Quarterly Journal*, *2*(13), 59–82. https://doi.org/10.11610/Connections.13.3.04

Tabansky, L. (2016). Towards a theory of cyber power: The Israeli experience with innovation and strategy. *8th IEEE International Conference on Cyber Conflict* (pp. 51–63).

Tang, S. M. (2015). Rethinking economic security in a globalized world. *Contemporary Politics*, *1*(21), 40–52. https://doi.org/org/10,1080/13569775.2014.993910

Taylor, R. (2015). The need for a paradigm shift toward cybersecurity in journalism. *National Cybersecurity Institute Journal*, *3*(1), 45–47. http://publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf

Teoh, C. S., & Mahmood, A. K. (2017). National cyber security strategies for digital economy. *International Conference on Research and Innovation in Information Systems* (pp. 217–221).

Thakur, K., Hayajneh, T., & Tseng, J. (2019). Cyber security in social media: Challenges and the way forward. *IT Professional*, *2*(21), 41–49. https://doi.org/10.1109/MITP.2018.2881373

Theoharidou, M., Kandias, M., & Gritzalis, D. (2011). Securing transportation-critical infrastructures: Trends and perspectives. In: Georgiadis C.K., Jahankhani H., Pimenidis E., Bashroush R., Al-Nemrat A. (eds) *Global Security, Safety and Sustainability & e-Democracy. e-Democracy 2011, ICGS3 2011. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol 99. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-33448-1_24

Thomopoulos, N., Givoni, M., & Rieltveld, P. (Eds.). (2015). *ICT for transport: Opportunities and threats*. Edward Elgar Publishing.

Thomson, K. L., Futcher, L. A., & Gomana, L. (2019). Towards a framework for the integration of information security into undergraduate computing curricula. *South African Journal of Higher Education*, *3*(33), 155–175. https://doi.org/org/10,20853/33-3-3011

Venkatachary, S. K., Prasad, J., & Samikannu, R. (2017). Economic impacts of cyber security in energy sector: A review. *International Journal of Energy Economics and Policy*, *5*(7), 250–262. https://www.econjournals.com/index.php/ijeep/article/view/5283

Yadav, G., & Paul, K. (2019). Assessment of SCADA system vulnerabilities. *The 24th IEEE International Conference on Emerging Technologies and Factory Automation* (pp.1737--1744). https://doi.org/10.1109/ETFA.2019.8869541

Zelikow, P. (2003). The transformation of national security: Five redefinitions. *The National Interest*, 71, 17–28.