ABOUT SECURITY CULTURE

Sebastian SÂRBU, PhD*

Abstract: *Security culture focuses on a broader scope: the ideas, customs and social behaviors, values of a group that influence the group and also society security at large. Therefore, there is a need to know the cyber risk, the geopolitical influence, the means of preventing terrorism, the security institutions, the warfare information for confronting these problems and global challenges.*

Keywords: *security culture, national security, corruption, terrorism, asymmetric threats, information globalization, cybernetic security, ENISA, Kapersky Lab, civil society.*

The concept of security culture uses a new institutional approach related to promoting dialogue with public institutions, as well as validating their social mission in the spirit of knowledge of new types of threats, risks, and vulnerabilities, at an individual, group, societal, national, regional, and global level. Security culture is a modern institutional approach promoting security issues; knowing the range of public political, military, economic, societal, and environmental urgencies; the amount of notions, ideas, and information available at a given time to the citizens of the state concerning the national security values, interests, and necessities; the ways in which to develop attitudes, motivations, and behaviors which are necessary for the defense and protection of persons, groups, and states, against vulnerabilities, risk factors, threats, states of danger, or potential aggressions, as well as promoting them in the security internal and international environments. (Dictionary of modern public security)

* *Military analyst, scientific researcher, member of the Transatlantic Press Club, vicepresident of National Security Academy for Defense Planning.*

The fight against terrorism, organized crime, cross border criminality are realities which the representatives of civil society must know in order to take part together with state institutions in knowing, preventing, and confronting these problems. And when the challenge is at the security level, it should concern us all equally.

The current geopolitical context has transformed the space of strategic interest in which Romania is found into a real source, transit area, and destination of serious criminal activities consisting in: illegal weapons, ammunition, and explosives trafficking; drug trafficking; illegal immigration and human trafficking; counterfeit products trafficking; money laundering; etc.

The new democracies in this region continue to be confronted with certain negative phenomena which affect the quality of government. In this context, inefficient government - an effect of democratic deficit and institutional corruption, reflecting itself in manifestations of political clientelism, public administration inefficiency, authoritarian tendencies, lack of public transparency and responsibility - undermines public institutions and can become a real threat to national security. In Romania, inefficient government represents a potential risk for national development and national security, in the long run.

Corruption is another threat to national security, but on short term, with a negative impact on living standards, human rights, and fundamental freedoms, as well as a sound economic development.

The new asymmetric threats, economic and information globalization, global issues, the growth of interstate dependency in all fields, global anomie, are sources of insecurity which concern us all.

This is why security education and culture, crisis management, combating disinformation, are necessary for a new collective defense, no longer done by the state, as a political and administrative entity, but by citizens via civil society, in such a way that resources, information, and responsibility decentralization is attained, an outcome necessary for preventing and managing security crises. Nowadays security is a modern concept, which in an open, democratic society represents a systemic reality, comprising economic, social, and cybernetic security, food safety, the protection of citizens' rights and liberties, etc. This is why it is necessary for citizens to have access to information, to be aware of security needs, for

security culture does not belong to interest groups or closed bureaucratic institutions, as it was the case in the era of state Communism.

A modern state is looking forward to identifying new security solutions, to making modern, European laws in this field, and to making available the necessary resources for developing the system of national security. The most important resources to be organized and put to proper use are the informational resource and the human resource. Without long term development and a satisfying GDP, which represents a nation's state of internal sufficiency, allowing it to compete on the international level, we are rather security consumers instead of security generators. The role of civil society is to get involved actively in actions of preventive education and management of the new security reality as an indicator of a Euro-Atlantic and European Community vocation. The pursued objective is stability, peace, and the construction of a modern, democratic society connected to Euro-Atlantic values.

Cybernetic security, terrorism, and critical information infrastructure - new challenges for the management of security culture and the European geopolitical space. The objectives of the European Union in the new global context.

On the 30th of March 2009, the European Commission issued a press statement regarding the protection of critical information infrastructure („Protecting Europe against large-scale cyber-attacks: improving the degree of preparation, security, and resilience") by which it established a plan („the plan of action concerning the protection of critical information infrastructure") for consolidating the security and resilience of vital information technology and communications infrastructure. Its aim was to stimulate and support the development of a high level of response, security, and resilience capacity on a national and European level. This approach was largely approved by the Council in 2009. The plan of action concerning the protection of critical information infrastructure is built on five pillars: preparation and prevention; spotting and reaction; risk reduction and recovery after incidents; international cooperation; and the criteria for the critical European infrastructure in the sector of information technology and communications. It establishes the measures to be taken with respect to

every pillar by the Commission, member states and/or industry, with the support of the European Union Agency for Network and Information Security (ENISA).

The digital agenda for Europe, adopted in May 2010, and the associated conclusions of the Council have underlined the common vision according to which confidence and security are fundamental preliminary conditions for using information technology and communications on a wide scale and for thus achieving the objectives concerning the dimension of „intelligent growth" of the Strategy Europe 2020. The digital agenda for Europe underlines the necessity that all interested parties unite their forces in a global effort in order to guarantee the security and resilience of information technology and communications infrastructure by emphasizing prevention, degree of preparation, and sensitivity, as well as to develop efficient and coordinated mechanisms in order to react to the increasingly sophisticated forms of attacks and cyber crimes. This approach guarantees that the preventive, as well as the reaction dimensions are challenges which are taken seriously.

The Commission adopted in September 2010 a directive proposal regarding the attacks on information systems. It concerns the consolidation of the fight against cybernetic attacks by better cooperation among the criminal law systems of member states and among judicial authorities and other competent authorities. Moreover, the proposal introduces some dispositions regarding the ways of fighting new forms of cybernetic attacks, namely botnets. At the same time the Commission forwarded a proposal for a new mandate of consolidation and modernization of the European Union Agency for Network and Information Security (ENISA) in order to increase networks' degree of reliability and security. The consolidation and modernization of ENISA will allow the European Union, member states, and interested parties from the private sector to develop capacities and training to prevent, detect, and approach challenges pertaining to information security.

Moreover, the digital agenda for Europe, the Stockholm program/its plan of action, and EU's Strategy of internal security in action underline the Commission's commitment to constructing a digital environment in which all Europeans could express their full economic and social potential. This is why security culture involves cyber security, but at the same time involves

proactive solutions for using human potential and community democratic participation, which could discourage security threats. The press statement of the European Commission reviews the results that have been achieved since the adoption of the plan of action concerning the protection of critical information infrastructure. It describes future expected measures for each action both at an European and at an international level and it focuses at the same time on the global dimensions of the challenges and importance of increasing cooperation among the national administrations of member states and the private sector on national, European, and international levels, in order to handle global interdependencies.

New, more technologically sophisticated threats have emerged

The global geopolitical dimension of these threats is becoming increasingly clear. We are experiencing at present a tendency to use information technology and communications in order to achieve political, economic, and military supremacy, including that acquired through offensive capabilities. „Cybernetic warfare" and „cybernetic terrorism" are sometimes mentioned in such contexts.

Moreover, as shown by the recent events in the Southern Mediterranean region, some regimes are ready and capable to forbid or undermine arbitrarily the access of their own citizens to IT means of communication - especially the Internet and mobile communications - for political reasons. Such unilateral internal interventions could have severe consequences on the rest of the world.

In order to better understand such diverse threats, it can be useful to divide them into the following categories: exploits, such as „persistent advanced threats", for the purpose of economic and political espionage (for example, GhostNet), identity theft, the recent attacks against the marketing systems of emissions quotas or against government information systems; sabotage, such as DDoS attacks, or spam generated via botnets (for example, the Conficker 7 million computers network or the Spanish Mariposa 12.7 million computers network); and destruction - this is a scenario which has not materialized yet, but, given the increasing use of information technology and communications in critical infrastructures (for example, intelligent networks and water distribution networks), it is not

excluded for the coming years. Future challenges are not specific to the European Union and cannot be solved by the EU only. The increasing degree of use of information technology and communications and the Internet allows for more efficient and profitable communication and coordination between interested parties and has for result a dynamic innovative ecosystem in all areas of life.

The experts of the Kaspersky Lab group issued a report regarding threats for 2013 and 2014, which was published in December 2013, containing the following statistical data, accompanied by a map of IT crimes:

1. Maximum risk (over 60%): four countries (Vietnam at 68,1%; Bangladesh at 64,9%; Nepal at 62,4%; and Mongolia at 60,2%).

2. High risk: 67 countries, including India (59,2%), China (46,7%), Kazakhstan (46%), Azerbaijan (44,1%), Russia (41,5%), most African countries.

3. Moderate cyber attacks rate (computer viruses) (21-40,99%): 78 countries from all over the world, including European countries such as Spain (36%), France (33,9%), Portugal (33,1%), Italy (32,9%), Germany (30,2%), the UK (28,5%), Switzerland (24,6%), Sweden (21,4%), as well as other relevant countries such as the USA (29%), Ukraine (37,3%), Brazil (40,2%), Argentina (35,2%), Chile (28,9%), South Korea (35,2%), or Singapore (22,8%).

4. Low/local degree of infection (0-20,99%): 9 countries.

As we can see, we had a moderate infection rate for the European Union in 2013. As for 2014, although there were no significant differences, and being too early for a full evaluation performed at the end of each year, the same experts predicted important cybernetic threats/information crimes in the financial field and in cyber espionage. The target here is individual citizens' money, as well as obtaining illegal economic information such as banking secrets. The conclusion that can be drawn here is that cyber attacks of any kind represent an asymmetric, but real threat to economic welfare and national security. It is the role of civil society, as well as mass media, to inform and implement security culture and the technical solutions devised by the innovative intelligence analysis centers, which promote educational excellence.

At present, threats can arise anywhere in the world and, because of global interconnection; they can affect any part of the world.

We must take a step forward in the direction of global awareness of the risks incumbent to the massive use of information technology and communications by all segments of society. Moreover, we must develop strategies to manage such risks adequately and efficiently, be it for the purposes of preventing, fighting, reducing, or approaching them. The digital agenda for Europe launches an invitation to „organize the cooperation between relevant actors... on a global level so that they are able to fight against and reduce security risks" and establishes the objective of „cooperating with interested parties on a global level to consolidate global risk management in the digital and physical spheres and to adopt specific internationally coordinated measures against information crimes and security attacks".

Education, scientific research, and security culture

We have to also take into account the intellectual, educational, and cultural dimensions of national security. Defending one's country and achieving a state of national security represents first and foremost a creative intellectual endeavor, by prioritizing education, research, and security culture.

As such, a nation that cannot be internationally competitive and cannot use the resources, technology, and human potential at its disposal is a security consumer, not a security provider. Development is a condition of liberty, and security is the means by which the values and norms created by society can generate the state of balance and safety needed for every citizen's exercise of freedom. The right to information becomes a commitment from society, which is aware of this right as an obligation when security, democracy, peace, and freedom are under threat.

Education is the first pillar which permits national defense and security sectors to adapt in order to respond to new challenges. We need a new standard of quality in military, public order, and information education, which may lead towards achieving full compatibility with the education programs of NATO and EU countries.

The private security industry represents the future for the security industry and the public security system.

Technology is the materialization of new concepts and innovations which satisfy modern security demands.

The second pillar is scientific research, an important endeavor for understanding the nature of current threats, by studying their implications. This understanding must be transferred to state institutions, which allows them to develop adequate policies. It is equally important that public opinion, civil society, various think-tanks participate in this effort, by contributing their own expertise. The third pillar is security culture by which we mean norms, values, attitudes, or actions which determine the comprehension and assimilation of the concept of security and other derived concepts: national security, international security, collective security, insecurity, cooperative security, security policy, etc. The development of education in the field of social sciences - especially political science, international relations, security studies - has led to the democratization of the field of defense and national security. As a consequence of the ever growing number of students and graduates in these fields, expertise is no longer the privilege of the state, which has a positive effect on the dialogue between the state and civil society, contributing to a higher quality of government in the area of defense and national security. (National Defense Strategy, 2010). With the help of OSINT and HUMINT-type information (by evaluating, corroborating, analyzing, and interpreting data), we can draw conclusions and identify possible ways in which events can unfold; specialized structures create a security culture via the projects that they develop and implement (by acting both preventively and offensively, through initiatives meant to discourage actions against personal, group, or societal security, as well as to consolidate security); they manage to grow in real terms the value of security indices in the field of reference and to proactively build the premises for the preservation and future affirmation of communities' interests.

In order to establish the concrete ways to prevent risk materialization and/or fight a threat, security culture provides the necessary expertise, by offering information with the purpose of knowing tendencies, facts, as well as events' circumstances, including:

1. Relevant territory (location, region, zone, country);
2. Fields of interest (directions of action);
3. Specific problems and cases;
4. Risks to national development;
5. Defense of fundamental and social values;
6. Information security;
7. Social environment.

The objectives of civil society with respect to education and security culture involve:

1. Stimulating interest and preoccupation by institutions and private individuals towards security culture/education, via mass media and other visibility actions targeted for this purpose;
2. Integrating in learning institutions - at the primary, secondary, high school, and university levels - security education both for children and adolescents, as well as adults, by organizing classes, conferences, symposiums, trainings, seminaries, meetings, colloquiums, presentations, workshops, talk groups, round tables, camps, trips, and other recreational and educational activities;
3. Editing, publishing, and disseminating informative and scientific materials, books, magazines, flyers, and other printing and audiovisual materials;
4. Establishing contacts and permanent collaboration with scientific institutions both home and abroad, with experts, as well as with other organizations, government or nongovernmental institutions which have security culture or adjacent fields as their field of interest;
5. Drawing, supporting, and counseling private or legal entities that wish to be initiated or develop in the fields of security, personal protection, educational management of security culture, as well as anyone interested in security culture;
6. Undertaking concrete actions, within the limits of academic competence, for preventing and stopping aggression/violence, for ensuring personal, group, and societal protection;
7. Taking part in projects, conferences, and other scientific events on the subject of the security field, organized/supported by higher education

institutions in Romania and abroad, local and central public authorities, as well as by institutions that have responsibilities in the field of national security.

It is necessary to promote, develop, and implement projects/models and standards of community and individual security in order to create a security culture, through research, studies, information, and education via partnerships with both state and private educational institutions, as well as medical, military, police, justice, and religious institutions, with governmental and nongovernmental organizations, for the purposes of developing a community that cares about the safety of its citizens, as well as of promoting knowledge, respect, and mutual trust between the members and the institutions of the community.

BIBLIOGRAPHY

COM (2010) 2020 and the conclusions of European Council – 25 &26 march 2010 (EUCO 7/10)

Kaspersky Lab Group*, Financial cyber threats in 2013*, in „Kaspersky Lab Report", April 2014.