Crisis management for Cyber issues: going it alone or in a coalition?

Viorel BARBU
Ministry of National Defence - Bucharest (ROU MOD)
viorel_barbu_map@yahoo.com

Abstract: Cyber attacks are executed by organized crime groups, sometimes on the orders of state structures, on Information and Communication Technology (ICT) infrastructures of strategic interest belonging to public institutions or to various companies. With this in mind, governments must adapt their critical infrastructures, both civilian and military, to specific risks and threats, so that they may avoid strategic surprises in the cyber environment. By accessing pre-existing models for protection, as well as specific know-how and best practices in the field, states may allocate scarce resources towards acquisitions and training, rather than redeveloping what others have already mastered. This article argues that a purely National approach to critical ICT infrastructure protection is lacking, since globalization manifests as interconnections in all fields, partly mediated by the cyber environment. Therefore, crisis management in the cyber domain must consider the interconnections of National systems to those of the alliances to which the nation belongs. A medium sized state like Romania, with the current geopolitical situation and a challenging security environment featuring implicit risks to physical and virtual borders, finds it much more difficult to generate and maintain its own cyber monitoring, prevention and protection systems. In this regard, it becomes easier and more financially convenient for government institutions to adhere to the doctrines, organization, training, technical endowment and interoperability capacity of its particular alliance. In the medium and long term, offset procedures are also a more profitable path to development of security capabilities that also serve to reinforce ties with and diminish distances from highly developed states.
Keywords: Cyber issues, risks and threats, coalition, critical infrastructures (CI), critical informational infrastructures (CII), critical infrastructures protection (CIP), critical informational infrastructures protection (CIIP)

INTRODUCTION

Cyber threats have become a constant feature in our lives, with some experts already designating the state of affairs as a real cyber war, and others considering it a permanent terroristic conflict. The past few years have been very dynamic with regards to the evolution of cyber threats, taking into account cyber attacks with their major social implications, as is estimated in 2012 by European Network and Information Security Agency (ENISA [ENISA] Threat Landscape, 2012). Globally, threats and vulnerabilities are increasingly diverse, partly due to the rise of the number of devices connected to the Internet – the so-called Internet of Things, which is fast becoming a reality. By 2020, there will be tens of billions of connected digital devices in the European

Union [EU]. According to Romanian Annual statistics (www.insse.ro), more than 60% of households had at least one PC connected to the Internet and the number of users increases exponentially with the rise of access to smart mobile phones, so the scope of what must be secured increases to encompass the whole of society which is linked to cyber space.

As it was presented in the survey entitled Attitudes towards the impact of digitization and automation on daily life (Eurobarometer, 2017), while 75% of European citizens believe that digital technologies have a positive impact on the economy, 64% on society and 67% on quality of life, awareness and knowledge of cyber security issues is still insufficient. As an example, into another paper (Continental European Cyber Risk Survey: 2016 Report), around two-thirds (69%) of all monitored companies have only a basic (or even not at all) understanding of their company's exposure to potential cyber risks, an almost equally high (60%) percentage of firms have never appreciated the financial losses that can be caused by a major cyber attack, while more than half (51%) of European citizens are not aware of cyber threats. The scale of this phenomenon requires the EU to act at Union level. The latest statistics show a rapidly growing trend, as follows: ransomware attacks have increased by 300% since 2015 and the economic impact of cybercrime has increased five times between 2013 and 2017 and another four times by 2019. Moreover, following the attacks of „Petya" (2016) and „Wannacry" (2017), it was estimated that a major cyber attack could lead to losses of more than EUR 100 billion to the global economy.

In the last decade, the need for a strong EU-level response mechanism to manage cross-border threats has become overwhelmingly apparent. The challenges faced by the EU in coordinating a common response have been highlighted following a number of crises, notably the volcanic ash cloud over Iceland in 2010, pandemics such as the influenza virus A(H1N1) in 2009, as is presented by European Centre for Disease Prevention and Control [ECDC] in their special named report The 2009 A(H1N1) pandemic in Europe (ECDC, Stockholm, 2010) and, with increasing frequency, terrorist attacks on EU Member States, report The Economist (The Economist, 2015). These crises have all sparked EU-level action, and indeed prompted the emergence of common legal and operational frameworks.

In addition, surveys suggest that people around the world consider foreign cyber attacks as a major threat to national security. Thus, Estonian Parliament Speaker, Ene Ergma, compared the cyber attack against Estonia (May 2007) with the Hiroshima atomic bomb: "When I look at a nuclear explosion and the explosion that happened in our country, I see the same thing" (as cited in Poulsen, 2007).

For these reasons, the European Commission assess that EU needs more robust and efficient structures to ensure strong cyber resilience, promote cyber security and respond to cyber attacks against EU Member States' institutions and agencies (European Commission [EC] Press release, 2017).

Today, an increasing number of EU countries (also NATO) have developed a National Cyber Security Strategy (NCSS) that includes measures a state should take to combat cyber risks that could affect society and the economy. While CIIP is a priority of most strategies, national approaches are diverse and, depending on their specific requirements, some countries have developed CIIP action plans through national legislation, others have set up working groups for each critical sector, while other countries include CIIP in the remit of the NCSS bodies (ENISA, An evaluation framework for Cyber Security Strategies, Annex A, 2014).

The EU's Directive on security of network and information systems (NIS Directive) is an important step forward in ensuring a minimum level of CIIP functionality in Member States, and the few states which have not yet complied with it, such as Romania, are encouraged to close these gaps, as soon as possible. Of course, macro level policy adoption is not the same as micro level policy implementation, and we can expect the following years to witness efforts at ensuring that the security results are those that were intended by the NIS Directive's adoption.

BACKGROUND

THE EURO-ATLANTIC CII ARCHITECTURE

As a primarily economic union, the EU's main areas of responsibility for cyber security concern important internal security issues, such as the fight against cyber crime and the Protection of Critical Infrastructures (CIP), and then cooperation with other international institutions and organizations. Compared to NATO, the EU later approached the national security and cyber defense issues, and succeeded in finally considering in 2008 the cyber threats as a key challenge including its military valence, besides the economic and political dimensions, according to European Council Report on the Implementation of the European Security Strategy - Providing Security in a Changing World (European Council, 2008). It was only in 2016 that NATO declared cyberspace to be an operational domain, alongside land, sea and air. By that year (2008), the EU's main concern was the security of infrastructures and information, cyber crime and somewhat cyber terrorism, while national policies overlap or intersected with Union ones, making the common effort in this area more difficult, stated the European Parliament in its study Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for cooperation for action within the EU (European Parliament, 2011).

Through the ENISA and the European Defense Agency [EDA], among others, the EU does not provide direct assistance to Member States in the event of a cyber attack, but provides them with guidelines, organizes specialized exercises at European level and supports the education and training of specialists and institutions in charge of these matters, as provided for in the statutes of ENISA. ENISA also offers specialized support to Member States for the implementation of EU legislation in this field and for strengthening the resilience of Europe's CII and networks (About ENISA, n.d.).

In 2012, a permanent Computer Emergency Response Team [CERT-EU] was set up consisting of IT security experts from the main EU institutions (European Commission, General Secretariat of the Council, European Parliament and Committee of the Regions, Economic and Social Committee).

In an emergency, CERT-EU will act in support of EU institutions and agencies and will cooperate with other similar organizations from Member States and specialized IT security companies, according to the description of the role and missions of CERT-EU (CERT-EU About us, n.d.). In 2013, the Emergency Response Coordination Center [ERCC] replaced the Monitoring and Information Center [MIC] and acts as a platform for the European Commission's response to crisis situations and is linked to other EU crisis cells (ERCC Facts&Figures, n.d.). In the same year, Europol's European Cybercrime Information Center [EC3] is set up, which aims to ensure an adequate response to cybercrimes within the EU (EC3 About, n.d.). Also in 2013, the EU defined its own cyber security strategy (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013), a programmatic document to develop public-private partnership and information sharing and cooperation, as well as to promote the European ICT industry and research & development of cyber security capabilities. For all these cyber security research and innovation actions, the EU allocated over €500 million under "Horizon 2020" (Horizon 2020: Work programme 2014-2015. Part 14, 2013).

Compared to the EU, which is primarily a political-economic union, NATO is primarily a political-military alliance dealing with cyber risks and threats from the security perspective of its own members. From this perspective, the Alliance has started to develop its own cyber security capabilities since the 1990s, but mainly to defend its own headquarters and protect agents and operations.

Following the September 11 attacks, NATO adopted at the Prague Summit in 2002 a Cyber Defense Program and NATO's Computer Incident Response Capability [NCIRC]. Subsequently, cyber attacks against Estonia (2007) and Russia's aggression against Georgia (2008) helped NATO realize the extent to which it was lagging behind in cyber space as an operational environment. Furthermore, in January 2008, the North

Atlantic Council [NAC] adopted its first Cyber Defense Policy, and for the implementation of its measures and provisions set up the Cyber Defense Management Authority [CDMA]. Last but not least, the Tallinn (Estonia) Cyber Defense Excellence Center for Excellence [CCD COE] was accredited, its main objectives being to improve NATO interoperability, cyber education and training (CCD COE About us, n.d.).

Two years later, at the 2010 NATO Summit (Lisbon). NATO set up the Emerging Security Challenges Division (within the NATO International Staff) and the Defence Policy and Planning Committee/Cyber Defence, which, starting in 2014, was renamed the Cyber Defense Committee, in order to study asymmetrical threats, including cyber threats, and to analyze the Alliance's cyber defense capabilities as well as to provide policy guidance. In 2011, the Cyber Defense Management Board [CDMB], replacing the CDMA, was set up and staffed with IT experts to coordinate cyber defense activities and facilitate the implementation of NATO-level cyber defense policies and associated agencies. The NATO Summit in Wales on September 4-5, 2014 had made it clear that cyber defense is one of the Alliance's basic missions for collective defense, and NATO nations can invoke Article 5 of the North Atlantic Treaty (collective defense clause) in the event of a cyber attack similar to armed one.

NATO's efforts in the field of cyber defense culminated with the NATO summit in Brussels (July 2018), when it was decided to set up a Cyber Operations Center in Belgium to ensure situational awareness and coordination of NATO's cyber operations.

CII FRAMEWORK OF SOME EU/NATO MEMBERS

European countries approach CII differently according to national priorities and their impact on their own societies. Thus, in some countries CIIP is an objective of the NCSS for the state authorities, in order to be able to coordinate the public and private sectors as efficiently as possible, and in other cases the CIIP is part of an autonomous political entity and not of the NCSS, but has implications for technological progress and societal development.

Austria. In the country, CIIP is based on a voluntary understanding between the state and CII companies, where authorities are responsible for identifying and designating critical assets, and CII operators support CIIP with specific security measures (Liveri & Sarri, 2015).

Recently (2014), the Austrian Federal Government has adopted the Austrian CIP 2014 Masterplan, in which the responsibilities of public agencies are regulated under the Federal Security Policy Act. Also, in 2015, Austrian authorities set up the Cyber Security Platform (CSP), which includes companies from the CII field and sectors of strategic importance for the state, such as transport, finance or health.

Czech Republic. The „Cyber Security Act" adopted on January 1st, 2015, requires all CII operators/owners/administrators to comply with standardized security measures, and to report and adopt countermeasures to cyber security incidents. Also, the National Security Authority (NSA CZE) established the National Cyber Security Authority (NSAB) to identify and monitor compliance by organizations operating elements of the CII.

Estonia. The Estonian CIIP approach is based on the concept of „vital services" to ensure vital societal functions such as health, nutrition, security and well-being. These number 43 and expressed in the Emergency Act adopted in 2009 after the 2007 cyber attack on Estonia attributed to the Russian Federation. The first Cyber Security Strategy, adopted for the period 2008-2013, was primarily aimed at bringing public attention to and developing requirements for cyber security. The second version, for the period 2014-2017, went one step further and focused on the cross-dependency between both national and cross-border „vital services".

Finland. The Finnish authorities have taken all necessary measures to protect the CI before the publication of the NCSS in 2013, according to which citizens, authorities and businesses should be able to use the cyber environment effectively and safely at national and international level. According to the strategy, most CIs in the society are owned by the private sector, but the Finnish National Emergency Supply Agency will support the protection

activity through guidance and training courses.

France. From a legislative point of view, the doctrine of national defense and security identifies the main CII, focusing on „vitally important operators". As regards the CIP, the Defense Code is the legal programmatic document regulating the French national security system. Since 2013, the French White Paper on National Security and Defense has, inter alia, set the CIIP as a priority. Structurally, the National Agency for Security of Information Systems (NAISS), created in 2009, has national jurisdiction in this area and reports directly to the General Secretariat for National Defense and Security. Subsequently, NAISS was appointed (February 11, 2011) French Cyber Defense Authority, responsible for overseeing CIIP legislation.

Hungary. The Hungarian National Directorate for Disaster Management (NDGDM) is responsible for the CIP and its main mission is to identify and designate potential CI elements, as well as to keep them under the supervision of governmental authorities. Although the Parliament in Budapest has adopted the CIP Act since 2012, there is still no Critical European Infrastructure element designated on Hungary's territory. According to the CIP Act, in transport, finance, health, industry, IT, justice and government apparatus, further legislative acts (decrees) are needed to start the process of identifying the CI elements. However, Hungary has created a Network Security Center (for CIP area), which acts as a National Security Authority, to support operators (only if they are CI elements) to protect themselves against cyber and network security incidents. Last but not least, another role of the NDGDM is monitoring, control and coordination in the field of CI and also includes HUN CIP CSIRT [Hungarian Computer Security Incident Response Team].

Lithuania. The Law on Cyber Security introduced the definition of CII at national level in 2015 and established the responsibilities of the Ministry of Interior to develop the methodology for identification/designation and to draw up a list of CII elements, which it then submits to the Government for approval. Institutionally, the law establishes the NSCS [National Security Cyber Centre] as the national authority responsible for CIIP, and at government level the Cyber Security Council [CSC] was established, consisting of representatives of the public and private sectors, but also members of the academia. As its tasks, the CSC is responsible for analyzing the situation, trends and threats in the cyber domain, as well as advising on improving the CIIP and national cyber security as a whole. In addition, the law requires a cyber security platform for information exchange between authorities and CII elements or operators. Currently, Lithuania has in force the Program for the development of electronic security of information (cyber security) for the period 2011-2019, one of the three objectives of the program being the CIIP itself (Government of the Republic of Lithuania, Resolution no.796, 2011).

Poland. In 2013, under the „Law on crisis management", the Government Security Center established the CIP Program in collaboration with Ministers and Heads of Central authorities with national security attributions, but also with other officials from certain sectors, public or private, considered vital or critical for the functioning of the state. The general objective of the program is to improve the security of the CI elements and to prevent their malfunctioning, to prepare for crisis or emergency situations, to react in case of disturbance or destruction of the CI and to reconstruct the affected CI elements. From a Polish point of view, CI can be assimilated as „systems and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance for the security of the state and its citizens, as well as serving to ensure efficient functioning of public administration authorities, institutions and enterprises" (CIPedia©, Critical Infrastructure, Poland, n.d.).

Spain. In 2011, the Government of Madrid elaborated the CIP Law no. 8 which includes protection measures and basic requirements in the field of CIP for the public and private sectors. This law has a dual role in the sense that, in addition to complying with the EU CIP legislation, it aims to coordinate the

collaboration of the Spanish administration with national CI operators. Subsequently, in 2013, the National Security Council (NSC) adopted the NCSS which, according to the CIP forecasts of the National Security Strategy (NSS), establishes the structure and how to implement the actions of prevention, detection and counteraction to cyber threats. Also, one year later (2014), the Ministry of Internal Affairs (MIA) set up (through Instruction 15) the Cyber Coordination Office (CCO), whose main mission is to coordinate the various agencies with responsibilities in ensuring cyber security. Another important function of this CCO is to advise the Ministry of Internal Affairs on cyber security issues and to provide the information needed to make the best decisions and coordinate CERT for security and industry (CERTSI) with the various state law enforcement agencies, such as the National Police or Civil Guard.

THE ROMANIAN CIIP LEGISLATION AND ORGANIZATIONAL FRAMEWORK

From the legislative point of view, 1999 was the first time in Romanian legislation when the term „computer crimes" appears in the sense of money laundering crimes (Romanian Parliament, 1999). Subsequently, Romania acceded to the Council of Europe's Convention on Cybercrime in Budapest (2001) and in 2003 signed the Additional Protocol to the Convention on Cybercrime, regarding the criminalization of racist and xenophobic acts in cyber space.

Until 2010, there were no significant cyber activities in Romania, largely due to the country's sustained efforts to integrate into NATO (2004) and the EU (2007). After that, Government Emergency Ordinance [GEO] no.98/2010 (Romanian Government, 2010) on the identification, designation and protection of critical infrastructure fully transposed the provisions of the Directive 2008/114/EC and aligned the Romanian national legislation with the European norms and exigencies. This document established the legal framework for identifying and designating Romanian and European critical infrastructures and assessing the need to improve their protection in order to increase the capacity to ensure the stability, security and safety of economic and social systems and the protection of persons. This law is the cornerstone of the CIIP in Romania, which designates the responsible public authorities and subdomains of national critical infrastructure.

At the organizational level, the first step was taken in 2008 by the Romanian Intelligence Service, the Cyber-Intelligence National Authority [CYBERINT], which created the CYBERINT National Center as a platform for collaboration between institutions within the National Defense System and the interface with similar structures in NATO (Romanian Intelligence Service, Cyberintelligence, n.d.). The role of the Center is to prevent, analyze, identify and respond to incidents of cyber infrastructure that provide public utility functionality, develop and disseminate public policies to prevent cybercrime incidents and counteract incidents (Early Alert System and Real-Time Information on Cyber-Incidents) and provide advice to public authorities responsible for the identification and protection of critical infrastructure.

In 2010, the National Supercomputing Center was set up in Bucharest, an institution that provides advanced technical solutions for the prevention of any disruptive actions on electronic systems and for ensuring the simulation of complex nuclear processes as close as possible to the real conditions, as well as analyzing and testing ICT solutions (Romanian Government, Decision no.139, 2010).

The next year (2011) saw the creation of the National Cyber Security Incident Response Center [CERT-RO], which manages the virtual environment generated by cyber infrastructures, including processed, stored or transmitted information content, as well as users' actions. CERT-RO cooperates with the other national defense system institutions as well as the specialized structures of Ministry of Defence [MoD] and the Ministry of Interior (Romanian Government, Decision no.494, 2011).

Starting in 2013, the cyber domain begins to be present in all programmatic documents for the Romanian defense and security fields (Romanian Government, Decision no.271,

2013). Thus, the Government adopts the Cyber Security Strategy of Romania and the National Action Plan for the implementation of the National Cyber Security System [NCSS]. The strategy defines cyber security as the state of normality resulting from the application of a set of proactive and reactive measures to ensure the confidentiality, integrity, availability and authenticity of electronic information, public and private resources and services in cyberspace.

In 2015, the Romanian Presidency issued the National Defense Strategy [NDS], which provides cyber security and defense policies as well as designating the responsible institutions, all of which are documented in the NDS Handbook for the period 2015-2019 (National Country Defense Strategy for the period 2015-2019, 2015). The NDS establishes the mechanisms for inter-institutional cooperation between the National System for Prevention and Counter Terrorism, NCSS (through CERT-RO and the Operational Council for Cyber Security), the National Public Order Management Center, the Interministerial Group Strategy for Preventing and Combating Macro-Criminality, the National Military Command Center and the Romanian Inter-ministerial Group for Integrated State Border Management. The NCSS, which is subordinated to the Supreme Defense Council of the Country and brings together public authorities and institutions with responsibilities and capabilities in the national defense field, is responsible for supervising the coherent implementation of all prevention and response measures for cyber-attacks against public institutions or private companies.

Romania aligned itself in 2015 with the Digital Agenda for Europe 2020, which aims at a Single Digital Market, through a governmental decision approving the National Strategy for the Digital Agenda for Romania 2020 (Romanian Government, Decision no. 245, 2015).

Currently, although it was initiated in 2015, the Law on the Cyber Security of Romania is still in draft form and it is in public debate on the MoD website (https://dlaj.mapn.ro/arhiva2018.php).

GOING IT ALONE OR IN A COALITION?

Analyzing national legislation and organizational framework in the cyber domain of the states mentioned above, we can conclude the following main ideas:

• national plans for CIIP differ from state to state: in some, national security authorities have full responsibility for specific activities, and in others there is a decentralized model, all depending on state priorities, but also on budgets and resources;

• cooperation with the private sector does not necessarily need to be formalized, i.e. through working groups and public-private partnerships or, in some cases, even legal procedures to ensure that all relevant operators participate in the CIIP;

• in most cases, legislation is the way to ensure that the CIIP process will be complete and respected; however, many countries also have non-binding voluntary schemes that work just as well;

• some of the specific cybersecurity requirements, such as incident reporting and implementation of basic security measures, must be part of the national CIIP action plan and must be implemented by all service providers, public and private;

• critical sectors are basically the same for each country, with little change depending on national risk assessments and the impact that any interruption will have on vital services to society.

In Romania, critical infrastructures face a challenging security environment for at least two essential reasons:

• they mostly stem from the development of a rigid communist economy, inflexible and difficult to adapt to the market economy, whose traces have not yet been deleted and whose crises have led to underinvestment in maintenance and development;

• the Romanian economy and society are still in a condition specific to the long and repeated transition periods in which vulnerabilities are heightened and society lacks resilience.

However, these disadvantages could turn into an advantage in the sense that Romania

can design and build the critical support infrastructures of crisis management utilizing the latest knowledge and insight, while Western societies are already confronted with the definition and management of these risks with significant sunk costs in infrastructure, making their replacement much more difficult.

Romania aims to ensure its normality in cyberspace by reducing risks and capitalizing on specific opportunities, improving knowledge, capabilities and decision-making mechanisms. In this regard, the Cyber Security Strategy of Romania bases the objectives, principles and directions of action in a coherent and unitary manner in order to identify, prevent and counteract the risks and threats to the cyber security of Romania.

Certainly, many countries have adopted their own CSS and we can note both the similarities between the chosen strategies but also many differences generated by the different importance given to this subject as well as due to the economic effects that the functioning of the cyber infrastructure elements have on each country. It is certain that, in most of these strategies, international cooperation in this field is a desideratum of many countries, a desire for cooperation that has the potential to widen cooperation in related fields and which ultimately can only lead to a greater stability in international relations and conflict avoidance. The fact that more and more countries have adopted their own CSS is a positive signal that allows policymakers to realize the importance of this area and to ensure that what has happened in Estonia in 2007 will not be repeated in other NATO and EU Member States.

Romania needs an up-to-date and efficient cyber security law that serves national strategic interests, synchronized with the European, Euro-Atlantic and international cooperation agenda. The development of international cooperation on cyber security must remain a constant at the level of policy-makers, economic actors and the education system. Romania's participation in the European cyber security exercises ("Cyber Europe") and adherence to the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) will support Romania in a faster implementation of the cyber security policies. For this, the private and public sectors need to work together to implement the CSS, and this can be done through mutual exchange of information, the implementation of a code of good practice in the management of cyber incidents and the organization and participation in cyber security exercises.

In the field of IT security, Romania is on an upward trend, with an increase in the volume of investment in products and complete security solutions. It is worth noting that Romanian IT specialists have developed two world-class anti-virus applications, RAV (now owned by Microsoft) and BitDefender, of which BitDefender has about 40 million customers. For both organizations (NATO and EU), the cyber defense of their own networks and facilities is a fundamental priority, and their missions are complementary: NATO focuses on national security and to defend the allies, while the EU has expanded its capacities on internal issues such as cybercrime, CI resilience, data protection, freedom and governance on the Internet, online privacy and fundamental rights, etc.

But national, regional and international security is highly dependent on critical infrastructures, and two axioms are accepted in the analysis of this area: the first is that 100% protection of a critical infrastructure cannot be ensured, and the second is that there is no unique, universal or one-size-fits-all solution to solve this problem. Because of these facts, we advance that there might be a third option - joining a coalition or alliance.

Now it is time to ask ourselves: Why do states join coalitions or alliances? Of course, there are political and military reasons as well. First, nations join alliances to safeguard their own national interests. Historically, alliances have formed in order to provide sufficient force to counter or deter an enemy. For military reasons, nations which lack sufficient military strength will seek coalition partners to protect their interests or borders. On the other side, powerful countries will seek alliances to gain increased military capabilities and access to strategic bases or national infrastructure.

The essence of alliances is power - especially the Balance of Power - NATO has become a

central figure in international politics and, although changed from the end of the Cold War, will persist in its global importance. So, a small and militarily weak state would actively seek membership in an alliance or coalition if it were attacked or felt threatened by another state, while a relatively strong state would encourage other states to join in order to present a formidable force to the enemy or to increase international legitimacy. The Anti-Iraq coalition demonstrated both of these ideas: Gulf States like the United Arab Emirates and Bahrain sought protection while the United States sought legitimacy in the coalition.

From a military point of view, the paradox is that, while often a source of strength, coalitions/alliances are just as often a weakness as well. The differences between national doctrines, levels of interoperability and military capability, languages, cultural and ethnic sensitivities of each coalition member can hinder alliance warfare for obvious reasons. Aditionally, each part of a coalition has a unique vision of the desired end-state and different national goals will cause different perceptions about progress as well, and maintaining cohesion within the alliance will mean making adjustments for other partners.

But the advantages of participating in a conflict within a coalition/alliance far outweigh the inconveniences. Coalition members will usually only contribute the minimum level of support required to receive the desired level of protection from other members. Partners benefit from shared military strength and varied capabilities, as well as access to each other's national CII and strategic bases, which cannot be underestimated.

Although material contributions may be uneven, sharing the costs of war can significantly reduce the burden on national budgets, financial cost sharing being both a benefit of collective effort and an expression of coalition support.

Furthermore, participation in a coalition yields enduring cooperative relationships that can make a future colaboration between former coalition members more likely in various areas, such as political, social-economic, IT, cyberspace, CII and more.

CONCLUSIONS

We conclude that even in the near future or in the medium term, military coalitions will continue to be the main guarantor of international security. Today, multinational operations are the norm in combat, stability operations, or in crisis intervention.

Although the coalitions generally have their own history and historical baggage, however the advantages outweigh the disadvantages because they have the role of aggregation of forces and providing international political legitimacy for military intervention.

Indeed, as Churchill once quoted (Chequers, April 1, 1945), "there is at least one thing worse than fighting with Allies - and that is fighting without them" (winstonchurchill.org, n.d.).

In the present heyday of globalization, the central system of infrastructure for any nation, whether we are talking about telecommunications, agriculture, water, energy, public health, finance, banking or transport, is reflected in the cyberspace formed by the interconnection of thousands of computer networks, servers, routers, switches and fiber optic lines, the healthy functioning of which is essential for any nation's economy and security.

The dependence of modern economies stemming from interconnectivity, and the lack of physical borders of cyberspace require the adoption of unitary measures to secure the cyberspace, which must be coherent at international level. We can estimate that cyberspace is global in scope and no longer a jurisdictionally delineated space, and any threat of this area becomes a generalized problem. A first step in ensuring information security at a global level could be to develop a worldwide strategy to secure global critical infrastructure.

Based on its geostrategic position and international IT competitiveness, Romania can assume a key role in working with the EU and NATO as strategic partners to successfully implement strategies and measures for enhanced IT security. It is accepted in the NSS of Romania that national security cannot be assured individually by any state, and the new challenges of the security environment

require a real and efficient collaboration through international cooperation mechanisms and organisations (National Country Defense Strategy for the period 2015-2019, 2015, p.6).

In the future, Romania's participation in various crisis management and peacekeeping missions within its coalitions and partnerships will likely generate a new type of threat to the citizens and vital infrastructures of the economy, society, information and living conditions, to which the Romanian state authorities, as well as those of the partners of the Union or the Alliance, must adapt and react.

REFERENCE LIST

CIPedia© - A service of CIPRNet (n.d.), Critical Infrastructure, Poland, Retrieved from https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure#PolandComputer Emergency Response Team [CERT-EU] (n.d.), CERT-EU About us, Retrieved from https://cert.europa.eu/cert/plainedition/en/cert_about.html

ENISA - European Network and Information Security Agency (n.d.), About ENISA, Retrieved from https://www.enisa.europa.eu/about-enisa

ENISA (2012), ENISA Threat Landscape 2012, p.2, Retrieved from https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape

ENISA (2014, September), An evaluation framework for Cyber Security Strategies, Annex A: Mapping of cybersecurity strategies, Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1

European Commission (n.d.), ERCC Facts&Figures, European Civil Protection and Humanitarian Aid Operations, Retrieved from https://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en

European Commission (2013), Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, High Representative of the European Union Forforeign Affairs and Security Policy, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, Retrieved from http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission (2013, December 10), Horizon 2020: Work programme 2014-2015. Part 14, Decision C (2013)8631, Retrieved from http://www.statewatch.org/news/2013/dec/com-2013-horizon-2020-security-wp.pdf

European Commission (2017), Attitudes towards the impact of digitization and automation on daily life, Special Eurobarometer 460, Retrieved from https://ec.europa.eu/digital-single-market/en/news/attitudes-towards-impact-digitisation-and-automation-daily-life

European Commission (2017, September 19), State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks, Press release, Brussels, Retrieved from http://europa.eu/rapid/press-release_IP-17-3193_en.htm

European Council (2008, December 11), Report on the Implementation of the European Security Strategy - Providing Security in a Changing World, Brussels, Retrieved from https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf

European Parliament (April 15, 2011), Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for cooperation for action within the EU (Study), Directorate-General for External Policies of the Union, Policy Department, Brussels, Retrieved from http://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf

EUROPOL (n.d.), EC3About, European Cybercrime Centre - EC3, Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Gauci, A.A.J., Zucs, P., Snacken, R., Ciancio, B., Lopez, V., Broberg, E., Penttinen, P., Plata, F., & Nicoll, A., (2010), The 2009 A (H1N1) pandemic in Europe, European Centre for Disease Prevention and Control, Stockholm, Retrieved from https://ecdc.europa.eu/sites/portal/files/media/en/publications/Publications/101108_SPR_pandemic_experience.pdf

Government of the Republic of Lithuania (June 29, 2011), The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019, Resolution no.796, Vilnius, Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf

International Churchill Society (n.d.), Chequers, 1 April 1945, Retrieved from https://winstonchurchill.org/uncategorised/quotes-slider/2014-11-3-16-25-06/

Liveri, D., & Sarri, A. (July 2015), Critical Information Infrastructures Protection approaches in EU, Critical Infrastructures and Services Unit, ENISA, Retrieved from https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf

Marsh&McLennan Companies (2016), Continental European Cyber Risk Survey: 2016 Report, Retrieved from https://www.marsh.com/content/dam/marsh/Documents/PDF/eu/en/Continental%20European%20Cyber%20Risk%20Survey%202016%20Report.pdf

National Institute of Statistics, Romanian Annual statistics, Bucharest, n.d., Retrieved from www.insse.ro

NATO Cooperative Cyber Defence Centre of Excellence [CCD COE] (n.d.), CCD COE About us, Tallin, Retrieved from https://ccdcoe.org/about-us/

Poulsen, K., (2007), Cyberwar' and Estonia's Panic Attack, Retrieved from https://www.wired.com/2007/08/cyber-war-and-e/

Romanian Government (April 7, 2015), Decision no. 245/2015 for the approval of the National Strategy on the Digital Agenda for Romania 2020, Bucharest, Retrieved from http://www.ancom.org.ro/uploads/links_files/Strategia_nationala_privind_Agenda_Digitala_pentru_Romania_2020.pdfRomanian Parliament (January 18, 1999), Romanian Law 21/1999 on the prevention and sanctioning of money laundering, Bucharest, Retrieved from https://lege5.ro/Gratuit/giytsmrt/legea-nr-21-1999-pentru-prevenirea-si-sanctionarea-spalarii-banilor

Romanian Government (November 3, 2010), GEO 98/2010 on the Identification, Designation and Protection of Critical Infrastructure, approved and amended by Law 18/11.03.2011, Bucharest, Retrieved from https://lege5.ro/Gratuit/geztqmzxhe/ordonanta-de-urgenta-nr-98-2010-privind-identificarea-desemnarea-si-protectia-infrastructurilor-critice

Romanian Government (February 23, 2010), Decision no. 139/2010 regarding the Establishment, Organization and Functioning of the National Supercomputing Center, București, Retrieved from https://lege5.ro/Gratuit/geztenbyg4/hotararea-nr-139-2010-privind-infiintarea-organizarea-si-functionarea-centrului-national-de-supercomputing

Romanian Government (June 02, 2011), Decision no. 494/2011 regarding the Establishment of the National Center for Cyber Security Incident Response - CERT-RO, Bucharest, Retrieved from https://cert.ro/vezi/document/hg-494-2011-infiintare-cert

Romanian Government (May 23, 2013), Decision no. 271/2013 for the approval of the Cyber Security Strategy of Romania and the National Action Plan on the implementation of the National Cyber Security System, Bucharest, Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf

Romanian Intelligence Service (n.d.), Cyberintelligence, Bucharest, Retrieved from https://www.sri.ro/cyberint

Romanian Parliament, Law on the Security and Cyber Defense of Romania (Project), Retrieved from https://dlaj.mapn.ro/arhiva2018.php

Romanian Presidency (2015), National Country Defense Strategy for the period 2015-2019 – A strong Romania in Europe and in the world, Bucharest, Retrieved from http://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf

Romanian Presidency (2015), National Country Defense Strategy for the period 2015-2019 – A strong Romania in Europe and in the world, Bucharest, p.6, Retrieved from http://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf

The Economist (Nov 16, 2015), Terror attacks and arrests in Western Europe, Retrieved from https://www.economist.com/graphic-detail/2015/11/16/terror-attacks-and-arrests-in-western-europe