THE EUROPEAN JOURNAL *of* Critical Services and Infrastructure Protection

ISSUE 01 • OCTOBER 2013

- Resilience
- European Comission and CIP
- Risk and Physical Security
- CIP in Turkey
- EU / NATO on Energy Security
- EOS and CIP
- Bulgarian Defence and CIP
- Space Security and EGS
- Albanians CIP Security
- IRAQ – The Resilient Power

THE EUROPEAN JOURNAL *of*
Critical Services and Infrastructure Protection
VOLUME I – NUMBER 1

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters
–CRS Report for Congress, 2004

CONTENTS OCTOBER 2013

CONTENTS

OCTOBER 2013

THE EUROPEAN JOURNAL *of*
Critical Services and Infrastructure Protection

Issue Editor
Liviu Mureșan

Art Director
Aurel Neagu

Layout & Design
CREA

Semestrial publication
Edited by ARPIC
with the support of
EURISC Foundation

Adress
P.O.Box 2–101,Post Code
011036,Bucharest,Romania
E–mail:office@arpic.org

Price: 5 EUR

The views expressed in this document are solely those of the authors and do not necessarily represent the views of, and should not be attributed to, ARPIC or the EURISC Foundation.

ISSN 2344 – 3790
ISSN–L 2344 – 3790

Iulian Fota,

National Security Adviser to the President of Romania

The new security environment exhibits a complexity and changeability that is challenging the security capacity of companies, municipalities, states and regions. The interdependencies of the numerous infrastructure systems on which quality of life and economic dynamism are based are also a source of vulnerabilities, risks and threats to national security. Taken individually, they challenge the assessment and management capacity of security actors. Taken together, there is the potential for cascading disruptions with long recovery times and significant potential damages, both, human, material and intangible.

Critical Infrastructure Protection has emerged as a key tool for national security efforts, but its proper application brings with it a new set of paradigms, derived from the complexity of infrastructure systems: fostering public-private cooperation in the field of security, fostering European and transatlantic cooperation for the infrastructure system protection, ensuring adequate tools and standards for the myriad security actors and stakeholders, as well as building a security culture.

I would like to emphasize the nearly two decades of activities in this domain of the EURISC Foundation and the newly established ARPIC Association and wish all the success for this new initiative, the launching of the European Journal for Critical Services and Infrastructure Protection.

Sorin Encuțescu,

State Councillor on National Security for the Prime Minister of Romania and Coordinator at national level for Critical Infrastructure Protection

Critical Infrastructure Protection is a field in which Romanian experts have accumulated valuable expertise. The impetus is now on properly applying this expertise to create security mechanisms for managing the new security environment. A concerted effort is underway for the identification of critical Romanian infrastructures, with over 1.000 identified so far, and to create the framework linking their owners, operators and administrators to the competent authorities. The purpose of these efforts is to promote burden sharing in security efforts, provide common standards for security planning and reporting, as well as coordination in the event of the manifestation of a risk.

Given the international nature of many infrastructures, European cooperation becomes paramount in ensuring good security outcomes. Romania is a keen supporter and active participant in efforts to develop the European Programme for Critical Infrastructure Protection and the associated framework. Cooperation takes place not only at the intergovernmental level, but also through exchanges between individual private security providers, branches of multinational security actors, civil society and other stakeholders.
In this regard I want to praise the efforts of professional associations such as ARPIC, the EURISC Foundation and their European and global partners, in this latest effort, of editing a European Journal for Critical Services and Infrastructure Protection.

Foreword

Adrian V. Gheorghe

Critical infrastructures are ubiquitous. They run the gamut from information technology to agricultural systems and energy generation and distribution. With such a high level of interdependency it is difficult to determine where exactly one system ends and another begins. The overlapping fabric of critical infrastructures adds to the level of risk and vulnerability inherent in any system, and requires “students” of the subject to delve deeply into the causality of even the most obscure events to determine their long term ramifications. These interdependencies enable greater control, faster response times and more information than traditional “simple” system models. However, they also induce greater fragility as society becomes more dependent on these complex infrastructures. As the risk management specialist Dan Geer stated, “Risk is a necessary consequence of dependence”. Therefore, the question to be answered is whether the inherent risk of catastrophic failure based on the intrinsic interdependencies of complex systems should limit the expansion of modern systems engineering and critical infrastructure design, especially with regards to connectivity and the internet. The answer, here, should be a resounding no, because prosperity and quality of life and sustainable development can only be achieved through critical infrastructure growth, whose security outcomes depend greatly on critical infrastructure protection efforts. What is required is for a partnership between the authorities, the private sector, academia, civil society and various experts to apply itself towards managing risks and using critical infrastructures to their fullest extent. What is at stake is not only economic gain, but also critical infrastructures as a source for resilience - the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats.

One particular risk that layered infrastructures present and which continues to challenge risk governance capacities is the domino effect. Consider the recent power failures that had a cascading affect that dramatically increased the number of end users that were impacted and the scale of the disaster. The causality of human errors or terrorist attacks has significant downstream effects and the more society gives up security and redundancy for convenience and global access, the more pervasive these risks will become. Clusters of systems that build on each other also impact preventability for these risks. Small, seemingly insignificant fluctuations in normal system operating parameters can create scenarios where there is a real impact or catastrophic system failures.

Many other key challenges exist when attempting to develop a plan to recover from major system disruptions, especially with respect to novel areas, such as the Internet and internet connected systems. Keith Rhodes lists several in his report “Internet Infrastructure” such as “lack of consensus, legal issues, and reluctance of the private sector to disseminate information with leadership/hierarchies”, which are applicable even to other areas of critical infrastructure protection.

This short presentation neglected other emergent aspects of critical infrastructure security, such as the cybernetic angle, or the importance of risk perceptions. What has become evident is the fact that the complexity of critical infrastructure protection issues and the multitude of actors and stakeholders are obstacles in the way of effective security. Their interactions are also an opportunity for burden and experience sharing and, consequently, should greater cooperation be achieved, they will transform from liability to an advantage in ensuring resilience. I would like to applaud efforts such as the editing of the “European Journal for Critical Infrastructures and Services Protection” for their contribution towards a greater exchange of information at European level. Moreover, they are a step forward in managing not only the complexities of the risks we are dealing with, but the complexities of the solutions we must employ. **CIP**

Prof. Dr. Adrian V. Gheorghe
Batten Endowed Chair on System of Systems Engineering, Batten College of Engineering and Technology, Old Dominion University, Virginia, USA
Director of the Homeland Security and Energy Research Cluster at the Batten College Engineering and Technology, Old Dominion University, Virginia, USA
Honorary President of the European Institute for Risk and Communication Management (EURISC), Romania
Vice President of the World Security Forum (WSF), Switzerland

Specialization: M.Sc. Electrical / Power Engineering, Department of Power Engineering, Bucharest Polytechnic Institute (1968)
Ph.D. Systems Science / Systems Engineering, Cass Business School, City University, London, UK (1975)
MBA, Academy of Economic Studies, Bucharest, Romania (1985)
M.Sc. Engineering–Economics, Bucharest Polytechnic Institute, Romania
Interests and Activity: Security and defence planner combining governmental experience with sound theoretical knowledge and background in cybernetics, complexity, and security studies; Specializing in security sector reform, primarily from organizational management perspective; Considerable expertise in leading and participating in national and international research teams. Currently involved in various projects on foresight–based security policy making and planning.

An Emergent Characterization of Complex Interdependent Critical Infrastructures

By Berna Eren Tokgoz and Adrian V. Gheorghe

After September 11, 2001, the U.S. national policy focused on protection of the nation from any terrorist or cyber-attack. Most of the efforts after 9/11 were about critical infrastructure protection nationwide. However, when the Hurricane Katrina hit the New Orleans area, which is a low probability high consequence disaster, new vulnerabilities were realized at the national, state and local level.

Resilience has become a new concept after Katrina, and it has been defined as comprehensive preparedness at local level for extreme disasters like hurricanes, major earthquakes, tsunamis, floods, wildfires, volcanic eruptions and ice storms. In addition, it has become clear that only *protection* of critical infrastructures will not be sufficient when a terrorist attack strikes any part of the nation or any global pandemic threatens the nation. Rather, there is a need for a holistic approach to assure that critical infrastructures are as *resilient* as possible to withstand extreme disasters.

Introduction

Survivability and continuous operation of critical infrastructures is a very serious mission of the US government after unexpected disasters that affected these systems. Critical infrastructures are defined by the US government as follows:

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (CRS Report for Congress, 2004).

Protection of critical infrastructures from unexpected events is both impossible and costly in general. Therefore, the concept of resilience has gained so much popularity in different areas, especially in disaster management area. In early 2006, the Critical Infrastructure Task Force (CITF) recommended Promulgate Critical Infrastructure Resilience (CIR) as the top level strategic objective to the Homeland Security Advisory Committee (HSAC). This statement shows the necessity to address resilience along with protection efforts for critical infrastructures.

Understanding Resilience for Critical Infrastructures

To understand and analyze behavior of large systems like critical infrastructures, traditional system analysis methods can be used. System interactions of critical infrastructures can be considered as complex. Complex systems have at least two defining properties; intricate interdependencies and many components operating at the same time. Systems are said to become complex when they are made up of several parts that depend on and interact with each other to function. In order to explain the overall behavior at system level, one has to decompose the system of interest into its parts and try to understand lower level of interactions. Traditionally, system analysis decomposes the system into its components by using a top-down approach to understand system behavior in order to take protective actions against unexpected threats. However, it may not be possible to explain all complex

system properties with this decomposition process. According to Haimes et al. (2008), system engineers are interested in system characteristics that emerge from the overall system design and its integration, including interactions and interdependencies among and between various component systems. Protective actions or other types of changes in the system can influence system characteristics as well as their interactions. One can say that properties emerge from interactions of lower level components. Therefore, there is a strong relationship between complexity and emergence. Emergence appears when one tries to explain system properties, but at the same time, size and complexity of the system exceed human understanding (Pariès, 2006). Likewise, resilience of critical infrastructures cannot be explained at macro level by using the resilience of system components at the micro level. Therefore, resilience of critical infrastructures cannot be predicted in advance of a disaster. As a consequence, resilience comes out as an emergent property when a disaster happens. That is why, resilience can be considered as an emergent property of critical infrastructures.

Behavior of large systems may be analyzed with emergent properties of these systems. Sage and Cuppan (2001: 326) define emergent behavior of a system of systems as follows:

The system of systems performs functions and carries out purposes that do not reside in any component system. These behaviors are emergent properties of the entire system of systems and not the behavior of any component system. The principal purposes supporting engineering of these systems are fulfilled by these emergent behaviors.

Haimes et al. (2008) define the emergent behavior of systems as follows:

We define emergent properties of systems as those system features that are not designed in advance, but evolve, based on sequences of collected events that create the motivation and responses for properties that ultimately emerge into system features.

Adding resilience to complex systems requires examination of emergent properties of these systems. In order to recognize emergent properties for a large system, the large system has to show emergent characteristics first, because some systems may not show emergent characteristics that can later result in emergent behavior. Haimes et al. (2008) determined the following characteristics of systems with emergent properties:

Broad missions to fulfill: Critical infrastructures are vital to society. Their continuous operation is so important for wellbeing of economy, security of nation and social wellbeing of citizens. Their services can be adversely affected and disrupted by a natural hazard or a terrorist attack. They are interdependent and their opera-

Resilience: An Emergent Characterization of Complex Interdependent Critical Infrastructures

tions influence each other at some degree. For example, loss of electricity can halt operation of pumping stations in a water system or disruption of an oil distribution system can affect generators using fuel.

Interdependencies among lifeline systems became apparent during Hurricane Katrina. Three major pipelines, which are the Colonial, Plantation and Capline, did not receive any crude oil and could not distribute refined petroleum because of loss of electricity at pumping stations. Southern and eastern states were not getting any refined oil as a result of this interruption and about 1.4 million barrels of crude oil supply was lost. These three major pipelines got back to their normal operation seventeen days after Katrina made landfall in southern Louisiana area (O'Rourke, 2007).

Created through the cooperation of many stakeholders who have overlapping, but not identical, objectives: Critical infrastructures are owned by both public and private organizations. Almost 80% of them belong to private organizations. Stakeholders usually have different objectives which do not necessarily overlap totally with each other. For example, residents may have some issues that assume priority, whereas elected public officials may not prefer to spend money on the reduction of risk of their communities since this might hurt economic investment and growth. Elected public officials may have their own political concerns which may be different from those of other stakeholders. In addition, private organizations have their own concerns about maximizing profit and keeping their critical infrastructure data confidential. No group or organization can be equipped with training, experience, knowledge, equipment or legal mandate necessary to deal with every type of emergency. Therefore, it is extremely hard to make protection and preparedness plans with full collaboration of all stakeholders.

Low capital-cost structures of components that reduce the financial obstacles related to emerging properties: Critical infrastructures provide services such as phone and internet services to end users with a reasonable price. For example, the internet is a system with several emergent properties due to low cost of entry for users and availability of technology from various competing companies serving these users. The easiness of having internet access removes the financial obstacle to emerging properties such as cyber-attacks. That is why cyber-attacks can be initiated from anywhere. Nevertheless, some properties of the internet such as routing technology and relevant protocols are not emergent due to significant investment and support from technology companies that they require.

Subject to significant events that, should they occur, can stimulate the emergence of properties that otherwise might not be anticipated: Needs of critical infrastructures change after every major unexpected event. The US government has been taking necessary actions to secure and protect critical infrastructures from adverse consequences of these events. It is possible to explain these actions with the evolving concept of critical infrastructures. Every major event triggers emergent properties of critical infrastructures. Thus, critical infrastructure concept has been evolving for the last thirty years in the US (O'Rourke, 2007). In the late 1980s, the US Government was concerned about the aging public works, and hence the National Council on Public Works Improvement (1988) focused on the improvement of public sector critical infrastructures such as highways, roads, water supply facilities and wastewater facilities. Increased international terrorism threats to critical infrastructures, especially to cyber systems, during 1990s directed the government attention to national security and critical infrastructures had new definition in that environment. President's Commission on Critical Infrastructure Protection (PCCIP) was established in 1996 and this commission generated a report on the protection of critical infrastructures. This report was revisited in 1998, and the primary focus of critical infrastructure protection was cyber threats between 1998 and September 11, 2001. After attacks to World Trade Center on September 11, the Department of Homeland Security was established and the focus shifted primarily to physical protection and secondarily to cyber-attacks. Since 2005, devastating Hurricane Katrina has changed the perspective from protection to resilience. Therefore, it is obvious that emergent properties of critical infrastructures like resilience, which cannot be anticipated before, come out after every major event.

If a critical infrastructure is disrupted, it has to resume its normal operation as soon as possible. Protection actions may not be enough alone in advance of a disaster, because these actions may not be able to minimize adverse effects of a disaster. Therefore, resilience comes out as an emergent property of critical infrastructures.

From the characteristics of systems with emergent properties, it is understood that system features like resilience cannot be designed in advance; they emerge after an adverse event. In order to enhance resilience, two important qualities of resilience which are redundancy and robustness can be implemented in a system.

Robustness refers to the inherent strength or resistance in a system to withstand external demands without degradation or loss of functionality. Improper statistical sampling or miscalculation can cause imprecise estimation of system design parameters which leads to design errors. Improving a system's design or selecting new design parameters can help harden the system against unexpected attacks (Haimes et al., 1998).

Redundancy refers to system properties that allow for alternate options, choices and substitutions under stress. In a critical infrastructure such as a transportation system, redundancy may refer to alternate routing, whereas it may refer to a backup generator in pumping stations for a water system.

Even though robustness and redundancy are functions of resilience, they are implemented in a system at component level. However, resilience requires concentration on system structure, architecture and component interdependencies. Since resilience cannot be assessed at component level, it can be said that its explanation can be made at system level, so it emerges.

Resilience Relation with Notion of Emergence

It is possible to explain the notion of emergence by the broader form of relationship between macro and micro level properties where macro level properties can be both partly dependent on and partly independent from micro level properties. Bedau (1997, 2002) defined three kinds of emergence:

***Nominal emergence*:** Emergence is nominal when macro level properties can be obtained by combining micro level properties, although macro level properties can be meaningless at micro level.

***Weak emergence*:** Emergence is weak if macro level properties can be weakly explained at micro level, but detailed and comprehensive behavior cannot be expected without performing one-to-one micro level investigation. The reason for this is that there is no condensed explanation of causal dynamics of the system under investigation.

***Strong Emergence*:** Emergence is strong if macro level properties cannot be explained or estimated by any kind of micro level property. It was argued that a system above a certain level of complexity cannot be fully controlled by upward causation (Davies, 2004).

Explanation of different types of emergence might help describe the notion of resilience. From the understanding of complex systems and emergence, resilience can be considered as an emergent property of complex systems. Hence, it might be possible to use the taxonomy for emergence to understand resilience. As a consequence, nominal, weak and strong resilience could be defined as follows:

***Nominally Emergent Resilience (NER)*:** NER addresses resilience characteristics of a system coming from a combination of individual subsystem properties. These properties might be complex emergent properties like consciousness, risk awareness, etc. NER covers everything that contributes to reliability and resilience of interactions between individuals and their environment. NER involves human aspects such as individual cognition, error management and stress management as well as organizational aspects such as designing an error tolerant environment. NER also includes interactions between individuals that can assist combined resilience at different degrees. In addition, it involves the majority of the characteristics of a Safety Management System.

Weakly Emergent Resilience (WER): WER addresses resilience characteristics of a system coming from a combination of individual subsystem properties, but macroscopic behavior cannot be estimated in detail without doing a one-to-one simulation. Leveson (2004) explains that this occurs in complex systems where interactions between feedback and feed forward loops manage behavior of these systems. This may also occur in some large scale systems which become simple when microscopic complexity disappears at macroscopic level. Large scale systems may also become complex when microscopic complexity is amplified and combined to generate a much greater complexity at macroscopic level.

Strongly Emergent Resilience (SER): SER addresses resilience characteristics of a system which cannot be explained by any combination of individual subsystem properties, even in principle. There is no evidence that these types of properties exist, but some recent developments in complexity science show that there is a possibility for their existence provided that a sufficient level of complexity is reached. Notion of culture, for example, might be a good candidate for these properties.

Human societies and organizations show a high level of complexity. Resilience should be considered as an emergent property of these complex systems. Although nominal, weak and strong emergent resilience have been explained above, most of the efforts towards the improvement of robustness of organizations have focused on nominal resilience.

Resilience concept in order to assess the interdisciplinary dimension of security within the effort of protecting interdependent critical infrastructures

As stated before, after September 11, the US national policy had focused on protecting the nation from any terrorist or cyber-attack. Most of the efforts after 9/11 had been about Critical Infrastructure Protection nationwide. However, when the Hurricane Katrina hit New Orleans area, new vulnerabilities were realized at the national, state and local levels. A new paradigm, which is comprehensive preparedness at local level for extreme disasters like hurricanes, major earthquakes, tsunamis, floods, wildfires, volcanic eruptions and ice storms, has emerged after Katrina. Harrald (2007) claims that Hurricane Katrina and the resulting flooding in New Orleans area showed that the US government was unsuccessful in preparing for and responding to this devastating event. The reason behind this is the internal and external complexity of today's systems. Complexity of systems brings extra burden and unexpected consequences that might affect them during disasters. As a consequence, Promulgate Critical Infrastructure Resilience (CIR) was recommended to the Homeland Security Advisory Committee (HSAC) by the Critical Infrastructure Task Force (CITF) as the top-level strategic objective in early 2006. These recommendations have brought new perspective and prioritization to threats to and vulnerabilities of critical infrastructures. In addition, this approach might be a major shift in paradigm from protection to preparedness at federal, state, local and even private levels. Even though regional preparedness plans and their lack of sufficiency were realized by the US Department of Homeland Security (DHS) and these issues were emphasized in a DHS report in 2006 in the wake of Hurricane Katrina, it has been understood that this report did not seriously consider the implementation of emergency plans at jurisdiction level.

It took almost five years between September 11 and Hurricane Katrina to take resilience into consideration in the protection of critical infrastructures. Resilient infrastructures can be defined by Scalingi (2007) as follows:

A resilient infrastructure is a component, system or facility that is able to withstand damage or disruption, but if affected, can be readily and cost-effectively restored.

Resilience has too many components that need to be addressed when it is considered in the protection of critical infrastructures. Resilience requires protection, prevention, deterrence, risk-based mitigation, response, recovery and long-term planning. In addition, it incorporates training, education, research and development as well as application of solutions that operationalize these activities. Thus, all these activities require partnerships among emergency managers, government, private sectors and universities.

Some initiatives have focused on resilience since 9/11. Especially after Hurricane Katrina, these initiatives have given more attention to the incorporation of resilience in the protection of critical infrastructures. Some efforts have been started by business groups. Local and state government officials, economic development associations and non-profit organizations have also led some initiatives about resilience. These initiatives are too important, because they bring all stakeholders that are responsible for critical services and have major interests in regional disaster resilience. Utilities, commercial businesses, non-profit organizations,

The New York Times
WEDNESDAY, SEPTEMBER 12, 2001
U.S. ATTACKED
ACKED JETS DESTROY TWIN TOWERS
ND HIT PENTAGON IN DAY OF TERROR
The New York Times
National Edition
WEDNESDAY, SEPTEMBER 12, 2001
ONE DOLLAR
U.S. ATTACKED
CKED JETS DESTROY TWIN TOWERS
HIT PENTAGON IN DAY OF TERROR
President Vows to Exact
EXTRA EDITION
AMERICA UNDER ATTACK
Newsweek

community institutions, local and state government agencies as well as federal facilities can be given as examples of these stakeholders. Emergency responders and law enforcement communities are also involved in these initiatives besides some state political officials.

It is possible to give examples about these interdependence-focused regional collaborative initiatives for establishing resilient societies. Regions for these initiatives are the Pacific Northwest (consisting of five US states and three Canadian jurisdictions), the Midwest (consisting of Iowa, Wisconsin, the Great Lakes states and business continuity in Chicago area), the Mid-Atlantic (just beginning in Maryland) and the Golf Coast (New Orleans and Louisiana). Some of these efforts are very well-organized, and receive strong support from local and state governments while others have some difficulties in focusing on issues. Some of them developed action plans to address lessons learned from exercises. Louisiana and the state of Washington have established regional cyber coordination groups. These groups have addressed cybersecurity, communications and the necessity for critical information infrastructure resilience by developing a huge cyber-attack scenario.

Conclusion

As mentioned above, there are numerous initiatives towards the incorporation of resilience in the protection of critical infrastructures. An important shortcoming of these initiatives is to make them operational. These initiatives have not progressed to their operational stages where they can effectively and realistically assess and monitor resilience. It will not be clear whether these efforts are realistic and their implementation will be successful unless an adverse event occurs. There is also no measure of evaluating the degree of implementation of these efforts at local, state and federal levels. There is always a question of determining how much resilience is enough. Since resilience is a new concept, it is a very challenging task to find a way of incorporating it in the protection of critical infrastructures. Quantification of resilience will help evaluate the effects of incorporating resilience in the protection of critical infrastructures. **CIP**

References

Bedau, M. A. (1997). Weak emergence. *Philosophical Perspectives*, 11, 375-399.

Bedau, M. A. (2002). Downward causation and autonomy of weak emergence. *Principia*, 6, 5-50.

CRS Report for Congress (2004). Critical Infrastructure and Key Assets: Definition and Identification, *Congressional Research Service*. The Library of Congress, available at **http://www.fas.org/sgp/crs/RL32631.pdf.**

Davies, P. C. W. (2004). Emergent biological principles and the computational properties of the universe. *Complexity*, 10(2), 11-15.

Haimes, Y.Y. Matalas, N.C Lambert, J.H. Jackson, B.A and Fellows, J.F.R. (1998). Reducing the vulnerability of water supply systems to attack, *J.Infrastructure Syst*, 4(4) 164–177.

Haimes, Y. Y., Crowther, K. and Horowitz, B. M. (2008) "Homeland security preparedness: Balancing protection with resilience in emergent systems. *Systems Engineering*. 11(4). 287-308.

Harrald, J. R. (2007). Restoring the National Response System: Fixing the flaws exposed by Hurricane Katrina. *TR News*, May-June, 9-13.

Leveson N. G. (2004). "A new accident model for engineering safer systems. *Safety Science*, 42(24), 237-270.

National Council on Public works Improvement (1988). Fragile foundations: A report on America's public works. Final Report to the President and Congress. Washington, D.C.: Government Printing Office.

O'Rourke, T.D. (2007). Critical infrastructure, interdependences, and resilience. *The Bridge*. 37(1).

Pariès, J. (2006) "Complexity, Emergenge, Resilience…" *Resilience Engineering:*
Concepts and Precepts, E. Hollnagel, D.D.Woods, and N. Leveson
(Editors), Ashgate Press, Aldershot, UK, pp. 43–53.

Sage, A. P. and Cuppan, C. D. (2001). "On the systems engineering and management of systems of systems and federations of systems". *Information, Knowledge, and Systems Management*. 2(4), 325-345.

Scalingi, P. L. (2007). *Moving beyond Critical Infrastructure Protection to Disaster Resilience*. Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience, *CIP Program Discussion Paper Series*, George Mason University.

Dr. Eng. Berna Eren Tokgoz
Researcher Department of Engineering Management and Systems Engineering, Old Dominion University, Norfolk, Virginia, US

Specialization:
B.SC and M.Sc. in Chemical Engineering, Hacettepe University, Ankara, Turkey.
Ph.D. – Systems Engineering, Old Dominion University Norfolk, Virginia.

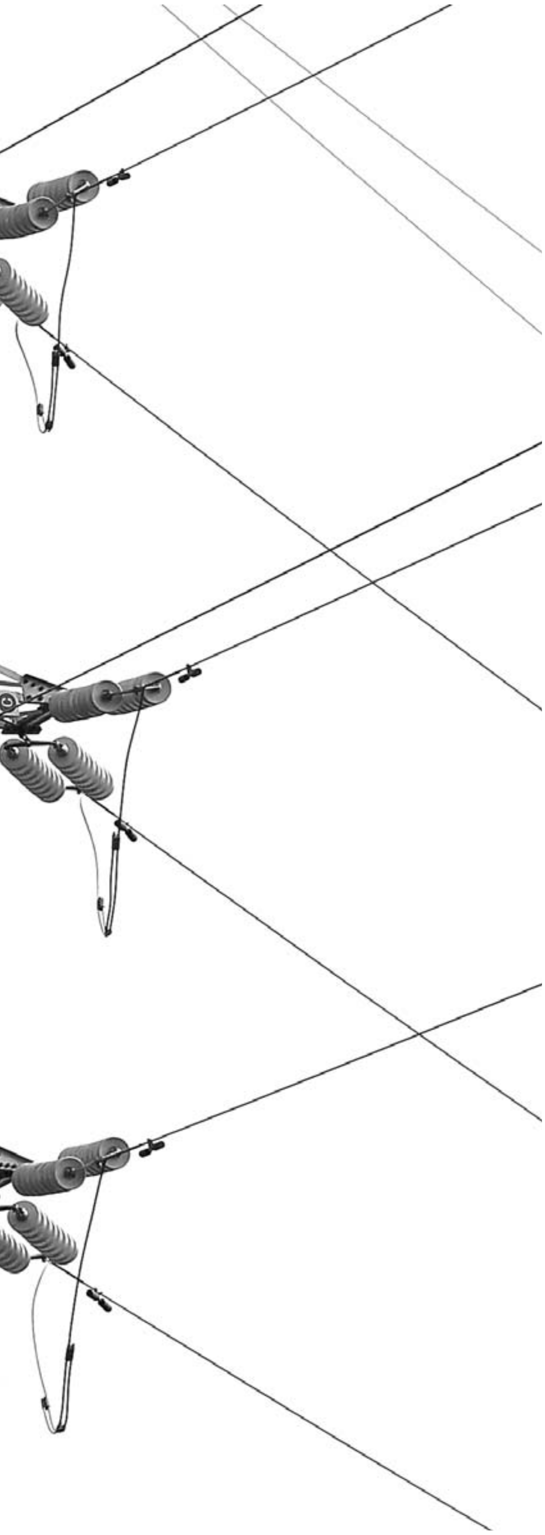
Interests and Activity: risk, vulnerability, quantification of vulnerability and vulnerability assessment, and particularly application of these concepts to critical infrastructures. Team member of "*Critical Infrastructure Resilience for the Hampton Roads Region Project"* in collaboration with Virginia Tech, University of Virginia and ODU's Virginia Modeling and Simulation Center, Norfolk US.

Energy Security – European Perspective and Policy Challenges

By F. Gracceva, G. Fulli, M. Ardelean, M. Masera

Institute for Energy and Transport, Joint Research Centre, European Commission

Disclaimer: The views expressed are purely those of the authors, and may not in any circumstances be regarded as stating an official position of the European Commission.



1. European energy policy and energy security implications

The European Union's approach towards energy security can be derived from several policy legislations and proposals that followed the European Commission's 2000 Green Paper "Towards a European Strategy for the Security of Energy Supply". This stated that "The EU's long-term strategy for energy supply security must be geared to ensuring […] the uninterrupted physical availability of energy products on the markets, at a price which is affordable for all consumers, while respecting environmental concerns and looking towards sustainable development". In 2006, a second Green Paper titled "A European Strategy for Sustainable, Competitive and Secure Energy" of 2006 (COM(2006)105) defined security of supply as one of the three pillars of European energy policy, alongside competitiveness and sustainability.

A central element of the European energy policy is the will to fundamentally change its energy system to a low carbon economy, with the explicit goal of breaking "the cycle of increasing energy consumption, increasing imports, and increasing outflow of wealth created in the EU to pay energy producers" (COM (2008)781). Also, Member States agreed to drastically cut greenhouse gas (GHG) emissions until 2050 (Second Strategic Energy Review 2008). This requires a shift towards new technologies laid out in the Strategic Energy Technology Plan (SET Plan), including renewable electricity, second-generation biofuels, smart grids, electricity storage, transport sector electrification, and carbon capture and storage among others. Clearly, time frames in the lead up to 2020 are too short for fundamental infrastructure changes, but many of the foundations need to be laid, including financial and market structures. The IEA estimates that 2 trillion EUR are needed in energy infrastructure investment by 2030 (IEA 2009), which could be financed by returns from the Emission Trading Scheme or other support mechanisms.

In January 2008 the Commission launched the so called "20-20-20" Energy and Climate package (agreed by the European Council in March 2007), which requires the EU to reduce its GHG emissions by 20%, to increase the share of renewables in energy consumption to 20% and to save 20 % of total primary energy consumption compared to baseline ('business as usual', i.e. no major changes), all by 2020. It is remarkable that all 27 Member States have committed themselves to a legally binding target of introducing 20 percent of renewable into their energy system by 2020, requiring national action plans that establish pathways for the development of renewable energy sources and creating cooperation mechanisms to help achieve the targets cost effectively (Directive 2009/28/EC). In the medium-long-term, the EU's 20-20-20 strategy calls for "an energy system with a diversity of non-fossil fuel supplies, flexible infrastructures and capacities for demand management [that] will be very different in energy security terms than today's system." In the short to medium term, effective provisions for preventing and dealing with supply crises must be made, in order to diminish the vulnerability to energy supply shocks.

The European energy strategy for 2020 – the so-called 20-20-20 agenda – is the starting point for Europe's current energy and climate change policy. This gives all European Member States shared targets on lowering greenhouse gas emissions, increasing the use of renewable energy and using energy more efficiently.

Key elements to reach the three underlying objectives of EU's new energy and environment policy are the idea of energy security as an issue of common EU concern and further integration of energy markets. "Solidarity between Member States is a basic feature of EU membership, and strategies to share and spread risk, and to make the best use of the combined weight of the EU in world affairs can be more effective than dispersed national actions" (Second Strategic Energy Review, COM(2008) 781 final). While the energy mix is still the responsibility of the Member States, the Lisbon Treaty has established the role of the European Union, reflecting the increasing interdependence of national energy systems and the benefits of a more coordinated external energy policy. Notwithstanding the trust in market mechanisms and market integration as the most effective ways for increasing energy security, the explicit goal of reducing energy imports, expressed in the EU Energy Security and Solidarity Action Plan, still reflects a preventive attitude with "energy supply autonomy" as a useful strategy to reduce the exposure of the economy to international energy crises (Gnansounou 2008).

Yet striving for energy independence alone would be too narrow a view of energy security. In a global economy, to seek independence would be an exception to the wider free trade Western policy and could on balance be negative for consumers. The EU has thus developed advanced dialogues with important energy producers, transit and consumer countries, including Early Warning Mechanisms to deal with energy supply disruptions. Energy security is thus embedded in a context of international organizations, institutions or mechanisms, such as the Energy Community, the Energy Charter Treaty, the IAEA, IEA, UNECE, and the EU-Russian Federation Partnership.

2. Energy Security Challenges for Europe

To identify the main European energy security challenges, it is useful to briefly consider some current trends. World demand for energy is set to increase by around 40% between 2007 and 2030 (IEA 2009). China is now the second biggest economy, and non-OECD countries already account for more than half the world energy consumption. The EU's gross inland energy consumption reached 1806 Mtoe in 2007, corresponding to about 15% of the world's consumption. Europe's primary energy demand is projected to grow by just 0.2% per year by 2030 (IEA 2009). At the same time, Europe's indigenous hydrocarbons resources are shrinking as well as its overall energy production. As a result, the European Union imports more than half of its energy, a trend that is expected to continue through 2030. Russia is still the EU27 main energy partner, providing about 33% of imported oil, 42% of imported gas and 26% of imported coal. The EU is becoming increasingly exposed to the effects of price volatility and price rises on international energy markets. Energy security concerns in European Member States differ widely as a result of different energy national consumption patterns. Transnational energy transport is increasing and European infrastructure is highly interdependent. Some Member States depend fully on imports. For example, after the decommissioning of its nuclear reactor, Lithuania lost 80 % of its electricity production capacity, which was largely replaced by (nuclear) electricity imports from Russia. Therefore, initiatives like the Baltic Energy Interconnection Plan and Mediterranean Energy Ring promote regional integration.

As a result of these trends, on the world stage Europe is still an important consumer, but increasingly sharing this role with other emerging players. Europe is and will continue in the medium term to be highly dependent on import from a small number of producer countries and long reaching transport corridors. If prices could adjust freely, security of supply could in principle be guaranteed (Helm 2002). But if market failures occur, a pure market approach does not produce a desirable outcome for society. To the extent that access to energy is a *public good*, public intervention (through subsidies, taxes or carbon pricing for example) can be justified.

Making energy production more sustainable through the introduction of renewable generation also presents energy security challenges. A reduction of hydrocarbon energy consumption will decrease imports, but also implies fundamental changes to the European electricity and wider energy system. In order to comply with the energy and climate change policy targets of the EU by 2020, the grids must be capable to host 'Renewable Energy Sources for Electricity' (RES-E) covering at least 30 - 35 % of the EU electricity consumption compared with a 16 % share recorded in 2006. To meet this objective, it is necessary to change the electricity infrastructure, primarily in order to cope with large amounts of variable generation from renewable energy sources such as wind and solar power generation. Adjectives such as 'super' and 'smart' are therefore more and more adopted when analysing future electricity grids to reflect features such as improved adequacy, flexibility, reliability and controllability (SET-Plan technology map (JRC 2009).

Flexible, coordinated and adequate electricity networks designed according to new architectural arrangements and embedding innovative technological solutions, are essential to address the risks of deterioration of reliability and security of supply. Information and Communication Technology (ICT) can contribute to increase the adequacy and robustness of the system, thus reducing the need for building new infrastructures, as well as augmenting its monitoring and governing.

While there is much debate on how Europe's ambitious targets can be reached, it is clear that one of the most important ways is to increase energy efficiency. Consumer behaviour does not yet support these ambitious goals, although average energy savings benefits for a household per year can be up to 1000 EUR (COM (2008)772). Energy consumption is about 20% higher than for economic reasons necessary.

One important step to reduce energy consumption is to curb oil utilization, which remains the most important energy carrier. Transport in Europe is still almost exclusively dependent on oil, making demand highly inelastic. Consequently, replacing oil as a transport fuel is a focus of development and research. The capacity of EU policymakers to put in place efficient policies on transportation will play a key role. In the meantime, however, the classic energy security concerns associated with oil still apply and oil price volatility remains a major concern.

3. The role of ICT in the new energy system and cybersecurity

Energy networks make extensive use of ICT means: their control, protection, measurement, management etc. at the company level are all ICT based. Not least, links with the customers are mediated by cyber means for the metering and billing of consumption. Moreover, the operation of the energy infrastructure requires the exchange of data over wide-area networks among operators and with authorities. The evolution of the energy networks in Europe will require more ICT interconnections, crossing national borders and jurisdictions. The lack of common accepted cybersecurity standards and criteria, does not contribute to the confidence on the existence of proper protection of the ICT systems.

This cybersecurity risk was negligible until a decade ago, but it has had to be taken into consideration with the connection of energy systems to open communications networks like the Internet. The security of industrial ICT is so impending because most technologies have not been designed with cybersecurity in mind. Control protocols are old and vulnerable to attacks. Security countermeasures derived from the general purpose ICT field (such as firewalls and anti-viruses) are only partially applicable in energy systems. Those solutions rarely considered the real-time and other particular requirements of industrial ICT.

On the one hand, the security of those ICT functions is crucial for the efficient management of the installations, but increasingly it is the security of energy supply that is at stake. Malicious actions affecting the availability of the data or their integrity could have direct impact on the operations of the energy systems. One can easily imagine how the failure of a control system might cause the impairment of a technical installation, and possibly bringing it to a halt. A key aspect to consider is the use of similar technologies in many different installations. This might be the cause of common failures - for instance in case of some malware affecting that technology. In addition, ICT components age rapidly, much faster than the electrical and mechanical components of the energy infrastructure. This requires appropriate responses, which at times should be coordinated across systems (e.g. for solving problems of interoperability). In Europe there is still no common agreed approach to tackling these issues.

In the last years, some initiatives have tried to discuss the cybersecurity problems in energy infrastructures in Europe, most notably the expert group on energy supply within the working group organized by the European Committee for Standardization (CEN) on the “Protection and Security of the Citizen (formally called CEN BT/WG 161).

4 Protection of European critical energy infrastructure

The previous brief discussion on some key challenges regarding the European energy networks demonstrates how energy systems extensively deployed over EU territory are exposed to security threats. In particular, LNG terminals and pipelines, the power grid and substations, are soft targets. So far, energy infrastructures in Europe have not been subject to major attacks by terrorist groups, which may be due to terrorist targeting rather than lack of opportunity (Toft, Duero et al.). Beyond the EU borders, attacks were more frequent, for example in 2008, when the BTC gas pipeline was attacked in Turkey. While so far, the only substantial interruptions to energy supplies have been accidental (e.g. the 2003 blackout affecting Italy) or the result of trade disputes (2006 and 2009 for gas supplies from Russia), an increasing complexity makes these networks vulnerable to malicious attacks with more severe impacts.

The Council Directive 2008/114/EC on the identification and designation of European critical infrastructures was designed to ascertain the vulnerabilities of European relevance in the energy system (i.e. with incidents possibly affecting two or more Member States) and improve their protection. In synergy with this, the European Programme for Critical Infrastructure Protection (COM(2006) 786) emphasized the need for Member States to manage their national critical infrastructures. It is based on an all hazards approach, not confined to terrorism, but also including criminal activities, natural hazards and other causes of accidents.

5. Concluding remarks

Given the challenges to European energy security, a comprehensive and coherent approach to energy policy is essential. A major task, both for policymakers and policy oriented research, is to select economically rational strategies for energy security and to assess the interactions of different energy strategies. This will require adopting a rigorous, robust and transparent approach to assess the future energy security challenges, not only to verify that the implementation of EU policies is not self-defeating, but also to identify new opportunities for synergy between policy domains. **CIP**

References

Gnansounou, E. (2008). “Assessing the energy vulnerability: Case of industrialized countries.” Energy Policy 36(10): 3734-3744.

Helm, D. (2002). “Energy policy: security of supply, sustainability and competition.” Energy Policy 30(3): 173-184.

IEA (2009). World Energy Outlook.

JRC (2009). Technology Map of the European Strategic Energy Technology Plan (SET-Plan).

Toft, P., Duero A., et al (2010). “Terrorist targeting and energy security.” Energy Policy 38(8): 4411-4421

Marcelo Masera
Head of Unit of “Energy Security” in the Institute for Energy of the Joint Research Centre (JRC), European Commission based in Petten, the Netherlands.

Interests and Activity: security of energy systems, networked systems and systems of systems, risk governance of infrastructures, and assurance cases for security. He joined the European Commission in November 2000, and up to December 2010 he was leader of the Security of Critical Networked Infrastructures group at the JRC’s Institute for the Protection and Security of the Citizen, Ispra (Italy). There he managed the support to European policies in Critical Information Infrastructure and cybersecurity aspects in other Critical Infrastructures. Among other activities, he managed the labs on Internet resilience and industrial networking security. His background is in electronics and electrical engineering, and has more than 30 years of professional experience in the fields of risk, safety and security.

Physical Security Risk Management in Critical Infrastructures

By Stelian Arion

If you think that technology can solve your security problems,
then you don't understand the problems
and you don't understand the technology
(Bruce Schneier)

Two recent activities highlighted the growth of the acceptance of security risk management as a way of improving the protection of people, goods, information, assets, infrastructures, processes and of society itself.

These are the formulation of the framework for the protection of critical infrastructures and the debates surrounding the new law for private security services.

In both cases, the intent is for security measures to be chosen and implemented based on risk assessment and for them not only to respond to damage reduction and continuity requirements specific to the business environment, but also to requirements on citizen security, public order or societal security. The security risks assessment and the implemented plans (either the security plan or the operator security plan) must facilitate the cooperation between the competent authorities and the business sector (or civil society, on a case by case basis) and ensure that both sides are fulfilling their security requirements while optimizing their cost structure.

Paradigm changes in the field of security

The last 50 years of development in this field highlight a paradigm shift, wherein solutions focused either on physical security, or on that of information and communication.

The first doctrines advocated for a technological solution to a technological issue. Any problem was viewed in purely technical terms, with the assumption for the existence of a corresponding technical solution. From this viewpoint, the unauthorized use of a computer is treated by an access control function, and a virus infection by an antiviral software. While still applied to a certain degree, this doctrine is inadequate as a full response.

Towards the end of the 1960 auditing became more prevalent, attempting to identify deficiencies in a system's security controls. Auditing had to be performed in reference to a standard that defined what is "good" or "acceptable", bringing up the issue of who establishes the standards and the degree to which they are representatives for the system being audited. It is a relatively simple matter to obtain a certificate of conformity with standards, as the result of an audit, which nevertheless still does not reflect current risks associated with the use of a system in real situations. Security standards are popular to this day, especially modern ones, which replace a simple checklist of elements with risk and processes analysis, such as the ISO27000 family.

During the 1990s, there was a shift towards risk management concepts, incorporating ideas previously developed for the insurance industry. Risks can be identified, analysed and classified in a hierarchy. A risk manager can avoid a certain risk by refraining from certain activities, reduce other risks through the use of technical measures, mitigate the damage through insurance policies or accept the risk as a result of the prohibitive cost of the alternatives. Risk management techniques are also utilised in relation to market risks, operational risks and financial risks. These techniques provide peak performance when paired with reasonable levels of information regarding the risks under scrutiny, such as when likelihoods and potential financial losses are clearly defined. Technical risks are much more difficult to evaluate, since the rapid progression of technological generations precludes most efforts at building up representative databanks concerning risks. There are also notable obstacles in the way of measuring intangible losses, such as reputation or lost opportunity costs.

Towards the end of the 1990s, analysts began using the phrase "information assurance". This is another form of analysis, entirely, which recognizes the fact that, in the absences of solid statistical data on risks, one should identify every element which could, conceivably, lead to a security breach. The approach maintains key features of risk analysis and the virtues of security standards, but also borrows from social sciences: organization management to understand how organizations function and how security considerations are ultimately assimilated within them; anthropology and criminology to identify how individuals and groups act and are motivated; psychology to account for the human factor in security and technological design and Economics, to understand the organization's decision making process in areas of security.

The management of risks in critical infrastructures

Risk management can take place at different levels, starting from highly detailed and specific processes regarding a piece of equipment and ending in an all-encompassing risk assessment which affect a nation or a transnational infrastructure.

There are three aggregate levels for the application of risk management to critical infrastructure protection: at company level, sector level and national level.

At company levels, risk management is employed to control risks that can negatively affect the pursuit of business goals. The focal point of this attention is the protection of the company itself. Sometimes, the process includes the management of threats generated by the company's activity in relation to the surrounding environment (i.e. a chemical plant), but only when such concerns are specifically enforced by existing legislation.

Although business continuity is the main goal of risk management at company level, its application by critical infrastructure operators has beneficial side effects for critical infrastructure protection. Since the most important objective for a company is to continue to deliver products and services to its customers, risk management processes at company level target plausible threats to the continuity of production and control measures for associated risks. Should the application of risk management processes be cyclical (as is recommended), then periodic revisions should determine whether risk mitigation measures are effective. This leads to more resilience on the part of the company, which is the main concern for critical infrastructure protection.

At sector level, risk management is employed towards ensuring sector resilience, taking into account the individual controls applied by sector specific organizations, but also factoring in the overall impact on society, on the basis of national and EU policies. Risk management at sector level is keyed into addressing the risks not already targeted through company level efforts. In this regard, the uniformity of risk management activities at company level simplifies their evaluation and helps to identify areas of unmanaged risk.

At national level, risk management is focused on societal impacts and goes beyond the scale of critical infrastructures, for instance by including pandemic risks into the security calculus. In general, critical infrastructures are taken into consideration in risk management at national level, since they play an inordinately important role in how a security incident plays out (keeping with the pandemic example, one has to consider whether the supply of electricity can be maintained and the consequences should it not).

At national level, there is an effort to track risks that affect the entire nation, with the potential for drawing risk maps for communities. These holistic perspectives include critical infrastructures since they profoundly influence the propagation of crises and their available solutions. It is to be expected that valuable conclusions can be drawn regarding the role critical infrastructures play during crises and the readiness levels of various sectors when it comes to the protection of critical infrastructures. During evaluations, one can also map the interdependencies between critical infrastructure sectors, aspects which are rarely pointed out during company or sector level risk evaluations.

These activities can correlate with a long-term policy of security exploration, or can be applied to immediate benefit, but both situations provide data for politicians and decision makers to improve the quality of their activity.

Towards a method of security risk management

While company level security risk management is not uncommon, there are no common standards for its application. This leads to differing levels of quality and incompatible results, which undermines these efforts from a critical infrastructure protection perspective, or that of the protection of people and valuables.

A way to bypass this obstacle is to provide common risk management tools based on a common framework of reference. This development would support the adaptation of risk management processes in companies which had not done so under pressure from their partners. It creates a basis for establishing a common level of protection, while the existence of a common framework of reference encourages information sharing with regards to risk management. Another advantage to the provision of such tools by governments is that they can also be influenced by said governments, which can include elements of social impact or use them to underpin the introduction of legislations, incentives or penalties.

Another way to support the progress of critical infrastructure protection is enshrining, into legislation, the obligation of critical infrastructure sector companies to comply with accepted methodologies for risk management. This policy can only achieve results if it is accompanied by the relevant standards and tools. Through this method, specific issues of critical infrastructure protection may be introduced, such as dependencies on other infrastructures as a class of threat and consideration for different types of security impacts, which

Physical security risks in critical infrastructures

would, otherwise, not directly elicit the interest of the organization.

A risk assessment method must form a coherent series of steps that may be used by the target group as a guideline and which should prove their security worth. Every step must be clear enough to ensure easy application by the target group.

The steps included in most methods are:

- determining the context of the risk assessment;
- the identification of potential risks;
- the evaluation of threats, vulnerabilities (sometimes as a subset of threat evaluation) and of impacts;
- determining the resulting risks and performing their analysis;

The most important elements to consider for ease of practical applications are;

- clear terms and uniform definitions;
- the types of threats which must be included;
- the types of impacts which must be considered;
- an objective mechanism to determine likelihood, impact and, ultimately, the risk itself.

Finally, one of the most important defining characteristics of the risk assessment method is its alignment with the expectation and requirements of the target group.

Further conclusions:

- the acceptability of the method depends on a maintaining a close relationship with current practices;
- it is to be expected that attempting to impose methods of risk evaluation to private organization will be met with fierce resistance. A voluntary assimilation approach, supported with attendant incentives and penalties for levels of compliance, should be a more successful strategy for adoption in the private sector;
- the application of a common method for risk evaluation can have a positive impact on risk information share between partners and the level of understanding of risks;
- developing such a common methodology demands a high level of general and specific expertise regarding the target group. This method should be developed in close cooperation and consultation with risk assessment experts and specialists from target groups;
- since information overload is always a significant threat, a measure of success for any method is whether it manages to propose realistic and limited objectives. Limitations to be considered include the size of the target group (for instance, organizations which provide emergency services) or the area of application for the method (for instance, limiting the use of risk management to the risk assessment).

Public private partnership in security

In risk management application, companies are more interested in issues affecting business goals than in those with an impact on society.

The government, on the other hand, is interested in protecting the citizen and the attendant society/community, a feat which it cannot manage on its own. This calls for cooperation, from whence the idea of a public-private partnership.

An important aspect of this partnership is the notable difference between the missions and the primary objectives of the two sides – we can refer to them as budgetary units versus the business environment. The first are oriented towards the maintenance of control over attributions established by law and financed through political approval of a budget, the second are concerned with maximizing profits in a competitive field. The first prefer an unambiguous area of authority, and will not stand for involvement from other authorities or from business actors. The others consider that citizen and societal security aspects are the sole purview of the state and if the private sector is to be involved, then this will be done with the state financing of these investments.

The imposition of supplementary costs, especially by direct intervention of the government, is very distressing to the private sector. The application of risk management methods can be satisfying, at least in the sense that private actors are allowed a level of autonomy in administering the investment they need to make.

Given the considerations outlined above, a security risk management method should:

- overlap both areas of interest:

  - of business continuity and damage reduction;
  - of preventing major consequences for society.

- assign reasonable control over

security requirements and the implementation methods to the party which is paying for them (the private organization);

• provide an instrument by which the competent authority may check, correct and sanction the way in which the company is fulfilling its legal obligations;

• create a medium of information exchange between the government and the private sectors, between business partners within the same sector, between beneficiaries and specialty contractors (security providers);

• create a framework of dialogue with civil society;

• create a framework for trust consolidation, such as certifications by a third party.

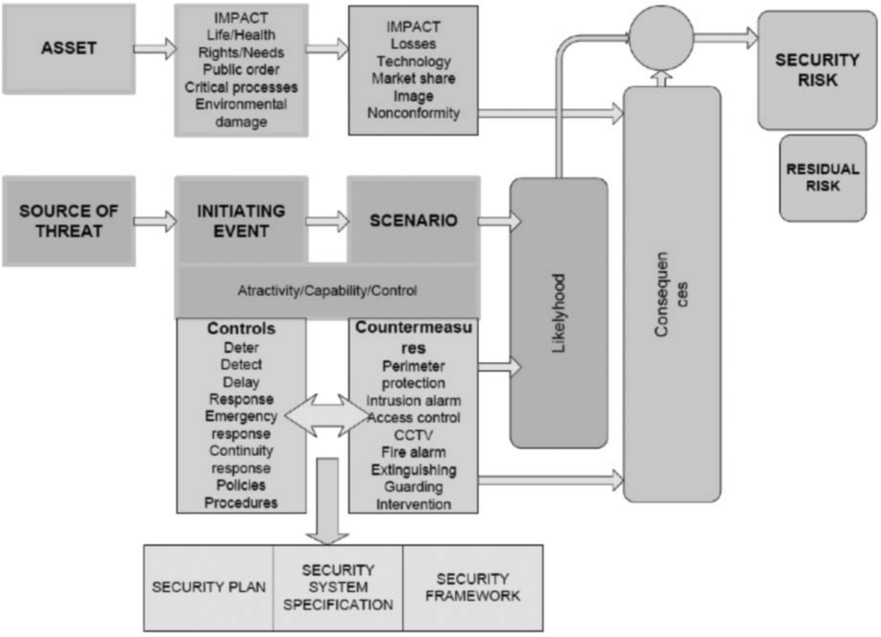


Figure 1: A method for risk management of physical security

In *figure 1*, I outline a method a risk management for physical security at company level. This method incorporates the relationship:

R = R(EI, S) > (C, L), where
EI = Initial Event
S = Attack Scenario
C = Consequences
L = Likelihood

The starting point is the identification of impact criteria of interest to the competent authorities and the company, as well as the identification of plausible sources of threats and scenarios of attacks. The authority can take an active role in formulating criteria and providing the company with relevant information from available data regarding the national and local security context. On the other hand, these criteria constitute the basis for negotiation between the authorities and the company as to how the company's legal obligations are to be met.

Understanding and assessment of sources of threats, their motivations and capabilities, as well as the target's vulnerabilities may aid in identifying and analysing the plausible attack vectors (the initial events) and their application (the scenarios) within the specific context of the objective. In line with the steps of plausible attack operations, different countermeasures are selected, such as deter, detect, delay, response, emergency response, continuity response, policies and procedures, as well as practical methods of application – perimeter protection, intrusion alarm, access control, closed circuit television, physical protection, intervention etc.

When applied to relevant assets within the company - whose selection can also be influenced by the competent authorities, as is the case with critical infrastructures – the method will produce a list of risks, which can be displayed in various forms (such as a risk matrix) for understanding and further classification and a list of security measures and means of implementation to which one may apply optimization techniques, such as ALARP (the reduction of risk to the lowest applicable level), cost effect analyses and so on.

Finally, the list of adopted security measures and their means of application are at the core of three basic documents, the security plan, the security system specification and the security framework of the company. **CIP**

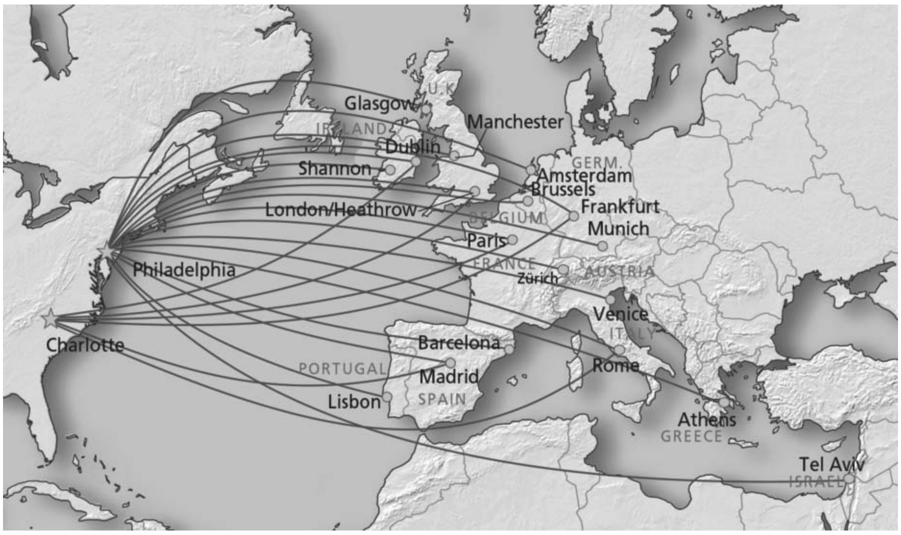
Ing. Stelian I. Arion
General Manager, of Secant Security
Vice–president, of Romanian Security Technique Association
Member of Directorial Council of Romanian Association for Promoting Critical Infrastructure Protection
President of 'Alarm Systems' and 'Information Security' Technical Committees of Romanian Standardization Association
Member of Technical Committee at Romanian Accreditation Body

Specialization:
Electronics and Communications at Bucharest Polytechnic Institute (1981)
Management at National School for Political and Administrative Studies (2001)
ISMS Auditor
Registered in the National Register of Physical Security Risk Assessors (2013)

Interests and Activity: Physical security, Information Security, Cyber Security, Security Management, Critical infrastructure protection, Security Risk assessment, Risk management, Continuity Management; Standardization for alarm systems, information security, societal security, risk assessment;
Security related occupational standards, and training; Contribution to security related national legislation.

A Transatlantic Overview of Critical Infrastructure Protection

By Sandro Bologna



Ensuring the security and resilience of the Nation's critical infrastructure is a shared responsibility among multiple stakeholders that takes a "whole community" approach—neither government nor the private sector alone has the knowledge, authority, or resources to do it alone. Within the critical infrastructure security and resilience mission space, partnerships and information sharing are perhaps two of the most important concepts, yet are often complicated to implement effectively.

To help enhance public-private partnerships and information sharing, the US President Barack Obama signed Presidential Policy Directive-21 (PPD-21), Critical Infrastructure Security and Resilience (CISR) on February 12, 2013. PPD-21 aims to strengthen the effectiveness of existing and new public-private partnerships and significantly expand current information sharing efforts.

On February 7th 2013, the "Cybersecurity Strategy of the European Union: an Open, Safe, and Secure Cyberspace" was presented through a press conference with the important remarks of Catherine Ashton, EU high representative, Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda and Cecilia Malmström, EU Commissioner for Home Affairs. The remarks revolve around the fact that we rely on cyberspace in almost every sector of our lives, and thus the importance of defending it from cyber-attacks. Neelie Kroes underlines one of the critical point of the EU Strategy, that's to say cyber resilience: "We need to protect our networks and systems, and make them resilient. That can only happen when all actors play their part and take up their responsibilities. Cyber threats are not contained to national borders: nor should cybersecurity be. So our strategy is accompanied by a proposed Directive to strengthen cyber-resilience within our single market. It will ensure companies take the measures needed for safe, stable networks. [...] Europe needs resilient systems and networks. Failing to act would impose significant costs: on consumers, on businesses, on society. A single cyber incident can cost from tens of thousands of euro for a small business — to millions for a large-scale data breach. Yet the majority of them could be prevented just by users taking simple and cheap measures."

In the document "Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace", achieving cyber resilience is the first of the five strategic priorities of the EU to efficiently tackle cyber threats. The pivotal factor for achieving a status of resilience for critical infrastructure is promoting Public – Private Partnership and collaboration. The additional factor is that EU could permit further security, in cases of threats with transnational characteristics, also coordinating a collective response. For these reasons the mandate of the European Network and Information Security Agency (ENISA) is being strengthened and modernized. In order to try and close the gap among Member States, the strategy of the European Union is associated with a proposal of legislation, that aims at setting for example "common minimum requirements for Network and Information Security (NIS)at national level which would oblige Member States to: designate national competent authorities for NIS and set up a well-functioning Computer Emergency Response Team [that would coordinate with the] Computer Emergency Response Team responsible for the security of the IT systems of the EU institutions, agencies and bodies (“CERT-EU”) [that] was permanently established in 2012” The strategy stresses the importance of the Public – Private engagement as a paramount step, given the fact that most of the infrastructures are property of, and operated by, private bodies. On the other hand, from the private point of view, it is necessary to raise awareness on the risks of cyber threats and establishing a risk management culture, in order to make the network and the information systems of a given infrastructure resilient.

The infrastructures' owners should also share information with the national NIS authorities and report any incident, in the same way that US infrastructures report to the US-CERT. One mean to foster the Public – Private Partnership could be the European Public-Private Partnership for Resilience (EP3R), which is a platform for public – private cooperation “on the identification of key assets, resources, functions and baseline requirements for resilience as well as cooperation needs and mechanisms to respond to large-scale disruptions affecting electronic communications”. The last two aspects that the strategy reviews are the financial support for critical infrastructures that would come from the Connecting Europe Facility (CEF) and the organization of cyber incident exercises at EU level, after the Cyber Europe 2010 and 2012 the second one included also the private sector. A set of nations have now publically developed and published their National Cybersecurity Strategy (NCSS) or, alternatively named, a National Information Security Strategy. Due to the global nature of cyberspace, international collaboration could be expected to be one of the highest priorities of each of the NCSS.

On December 6th, 2012, the Council of the European Union has released the Document “Proposal for a Council decision establishing the Specific Program implementing Horizon 2020 - The Framework Program for Research and Innovation (2014-2020)” In this document, attention is devoted to the subject of Security in general and Cybersecurity in particular, listed as one specific theme of research. The time span of H2020 will be characterized from an increasing complexity and uncertainty, with consequent increase in the vulnerability of Critical Infrastructures. The conventional approach on risk management, based on a “a priori” classification of all the potential risks is not sufficient any more. “Think about unthinkable” is becoming a mandatory strategy in the field of Critical Infrastructure Protection (CIP). These new dimensions of the CIP require a new approach to resilience, going well beyond the past approach to fortress.

On January 23rd, 2013, the Italian Prime Minister Office has announced a Decree on National Cybersecurity Strategy, published on the Italian Gazette GU n.66 of March 19th, 2013. The Decree is not a National Cybersecurity Plan, but more in general it defines the “constitutional architecture” of the different governmental offices involved in the National Cybersecurity. The Decree also celebrates public-private partnerships and information sharing.

In Romania, the office of the Prime Minister emitted a decision regarding the approval of methodologies for creating and revising security plans of the owners, operators and administrators of national or European critical infrastructures. Also covered were the framework of the security plan and the responsibilities and competences of the security liaison officer within the designated specialty compartment within the competent public authorities and within the owners, operators and administrators of national or European critical infrastructures.

All the above reported actions and decisions celebrate public-private partnerships and information sharing as well as shared responsibility among multiple stakeholders based on a “whole community” approach. On this line of thinking the cooperation started between AIIC and ARPIC is a very important step. Through that cooperation it is guarantee a constant exchange of knowledge and experiences between Italy and Romania on the subject of Critical Infrastructure Protection. AIIC has now about six years of experience contributing to the creation of public awareness on the subject of Critical Infrastructure Protection in Italy, through the organization of Workshops and Conferences. From the very beginning AIIC has also supported the organization of the annual conference CRITIS International Conference on Critical Information Infrastructures Security. **CIP**

Dr. Sandro Bologna
Head of “Large Infrastructure” Group at ENEA

Specialization:
Physics at University of Rome in 1972

Interests and Activity: After the graduation and up until today, he has been working at ENEA, where he has covered different positions as Researcher, Head of Research Units, Head of Research Projects at national and international levels. While working at ENEA he has been on leaving for different periods, working at Riso National Laboratory (DK), Gesellschaft fur Reaktorsicherheit (D), Westinghouse (USA), Institutt for Energiteknikk (N). His main research activities deal with the achievement and assessment of software safety and reliability, operator decision support systems that make use of artificial intelligence, plant control room design and assessment, critical infrastructures protection and complexity science. In these fields he has co authored several publications and coeditor of books. Sandro Bologna has served the international scientific community in the preparation of many events and conferences and as guest editor of special issues of international journals. He has served EU several times, both as Evaluator and Reviewer of EU Projects.

Critical Infrastructures and Services Protection in Turkey

By Mitat Çelikpala

Critical infrastructure is an umbrella term referring to a country's assets that are essential to the nation's security, public health and safety, economic vitality, and way of life. Critical infrastructures are those physical and information technology facilities, networks, services and assets, which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of the government. From energy systems that power our neighbourhoods, to transportation networks that move us around our communities and the country, to facilities that provide our families with safe drinking water, critical infrastructure and key resources affect nearly every aspect of our daily lives.

These infrastructures are owned or operated by both the public and the private sector. However, "[t]he reinforcement of certain security measures by the public authorities in the wake of attacks directed against society as a whole and not at the industry players must be borne by the State." The public sector has therefore a fundamental role to play.[i]

Introduction

Some basic questions like "Why is critical infrastructure important?" or "Why is critical infrastructure protection important?" have the utmost importance and require a reply. The answer is straight and essential to think about: Any attack on critical infrastructure or its destruction could significantly disrupt the functioning of government and business alike while producing cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, man-made, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence.

How can the states respond to those threats on critical infrastructure? The commonly accepted basic reply is that "[n]ot all infrastructures can be protected at all times." Therefore, all those agencies responsible to protect the critical infrastructure act to mitigate the risks through implementing risk management techniques. With that, it is possible to focus on areas of greater risk for the states. This necessitates identifying the critical infrastructure, the type of threat and measuring its effects on national security. There are three fundamental criteria for identifying potential critical infrastructure: scope or the extent of the geographical area that could be affected, magnitude, and effects with respect to time.

Defining and Securing Critical Infrastructure in Turkey

Defining and securing Turkey's critical infrastructure is now seen as a core part of the nationwide legal, administrative and security systems. This makes both central authorities and local bodies – such as municipal administrations, provincial governors and sub-governors – responsible for defining and protecting these assets.[ii]

In terms of definition, at a local level, each province, under the authority of the provincial governor, has a Provincial Security Commission composed of local officials (either appointed by the central government or elected locally), that is responsible for defining critical infrastructure. These commissions are also responsible to take any necessary measures to protect already defined CIS within their area of jurisdiction and responsibility. Naturally, this may led to very different definitions of critical infrastructure as well as different outcomes in terms of implementing related security policies at the local level. In addition, when we take some other local bodies – such as small local municipalities, fire fighting bodies, regional environmental commissions, etc. – into account, the subject becomes more complicated.

Meanwhile, the main central body responsible for protecting critical infrastructure in Turkey is the Ministry of Interior. In rural areas, dams and refineries are protected by Gendarmerie General Command (GGC). In urban areas, or within the municipality boundaries, police forces take the responsibility. The Coast Guard, national intelligence bodies, Turkish Armed Forces, special border protection units, but rarely private security companies, also play some role. In sum, there is a fragmented security structure that occasionally results in coordination problems.

Among those entire sectors of critical infrastructure, critical energy infrastructure namely the pipelines probably are the most central one as far as the terrorist threat has taken into consideration in Turkey. The risk of a successful terrorist attack is high, especially for energy systems and facilities or installations located in certain geographic regions. An example from Turkey could help to understand the impact of single incident on the producers, consumers and the transit country. On 5 August 2008, an explosion occurred in the Turkish section of the Baku-Tbilisi-Ceyhan (BTC) oil pipeline.[iii] Pumping one million barrels per day (bpd) of Caspian crude to the Turkish port of Ceyhan on the Mediterranean Sea for export to Western markets, the pipeline is widely regarded as one of the most important alternative paths carrying Central Asian and Caspian gas to the international market. The blast, which occurred on a pipe gate valve near the eastern Anatolian town of Refahiye in Erzincan province, caused one percent of the international oil transportation to stop. The line remained closed for fifteen days. Officially, it was claimed that the explosion was a mechanical or technical failure, arising from a fault in the system that had been detected prior to the blast. However, the separatist Kurdistan Workers' Party (PKK) claimed responsibility for the blast. It is widely believed that was it was an act of PKK sabotage. If it was a terrorist attack, the asymmetrical nature of the incident rapidly becomes apparent. It would have cost the PKK around $500 to conduct the attack but in contrast, the material loss of the explosion to the owner is striking. Overall, it was estimated to be in the region of $1.68 billion (1 billion barrels a day at $120 a barrel spread over 14 days = $1.68 billion). When we add the other costs such as burned oil in the pipelines, firefighting and personnel costs, suspension of oil flow, repairs and so on, the overall bill was somewhere in the region of $2 billion. We can compare this amount with the 2008 budget of security organizations that are responsible for protecting the pipelines in Turkey. For instance, the 2008 budget of the Gendarmeries General Command was $2.5 billion and the 2008 budget of the General Police Forces was $4.5 billion.[iv]

It should be noted that, apart from the 2008 Erzincan-Refahiye blast, there has not been any serious incident against the BTC pipeline. Until then, almost 30 incidents of vandalism or attempts to steal oil had been reported, but the pipeline had essentially been successfully protected by the security forces. However, the intention to increase the number of pipelines running through Turkey makes the protection of pipelines and other related critical infrastructure a sensitive issue and there are more than 10 attacks to other pipelines, especially in the south-eastern regions. Problems of cooperation, lack of efficient communication between the responsible bodies and a lack of investment in the security structure for protecting the pipelines are the main issues confronting Turkish decision makers. In order to address these issues, there is now greater coordination between the GGC and the Ministries of Foreign Affairs, Energy and Interior Affairs. Security Coordination Meetings organized by these bodies, with the participation of representatives from the Turkish Armed Forces, Turkish Intelligence Service and BOTA , have been held regularly. By and large, this system works well. However, some problems continue to arise due to lack of coordination and timing. **CIP**

References

[i] "Critical Infrastructure Protection", Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical Infrastructure Protection in the fight against terrorism [COM(2004) 702 final – Not published in the Official Journal]. See, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm

[ii] For a detailed analysis see Mitat Çelikpala and M. Melih Ba demir, "Türkiye'de Petrol ve Do al Gaz Boru Hatlarının Güvenli i: Politikalar ve Öneriler", *Stratejik Ara tırmalar Dergisi*, Vol. 8, No.14, January 2010, p. 97-128.

[iii] The BTC is one of the longest oil pipelines (1.776 Km) in the world and runs through the territories of three countries, namely Azerbaijan, Georgia and Turkey. The BTC pipeline is operated by the Baku-Tbilisi-Ceyhan Pipeline Company (BTC Co.). It is a joint venture company consisting of 11 shareholders. The pipeline's construction phase took 12 years at a cost of more than 5 bln US$. It has a capacity of 1 million barrels per day; 1.2% of world's daily crude oil production flows through the BTC.

[iv] Mitat Çelikpala, "Protecting the Key National Utilities and Energy Infrastructure", James Ker-Lindsay and Alastair Cameron (Eds.), *Combating International Terrorism:Turkey's Added Value*, RUSI Occasional Paper, October 2009, p. 16-18. Hasan Alsancak,

Prof. Dr. Mitat Çelikpala
Chair of the Dept. of International Relations, Kadir Has University, Turkey

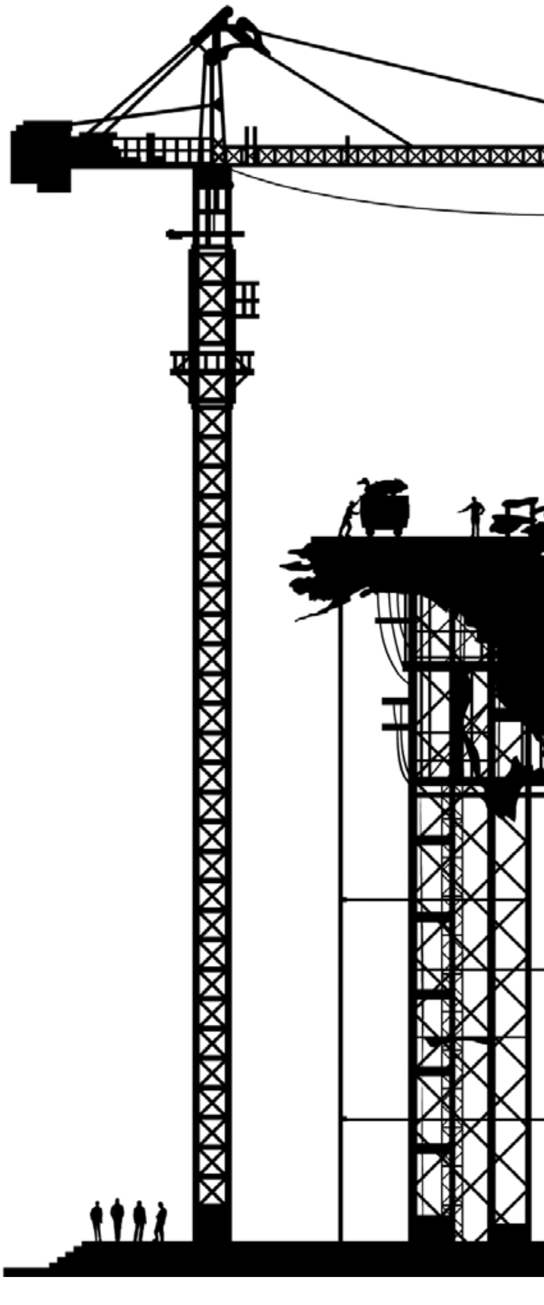
Specialization:
B.A. Middle East Technical University, Ankara Dept. of Public Administration and Political Science (1992)
M.A. Hacettepe University, Ankara Dept. of Public Administration and Political Science (1996)
Ph.D. Bilkent University, Ankara, Dept. of International Relations (2002)

Interests and Activity: Turkish Foreign Policy; Turkish Russian Relations; The Caucasus and Central Asia; Black Sea Region and Regional Security; Critical Infrastructure Protection for Turkey and Black Sea Region. He is lecturing at TOBB Economy and Technology University, at the Army War College, and at the Turkish National Security Academy. He is also the academic adviser to the National Security Academy, the Turkish Ministry of Foreign Affairs' Strategic Research Center, and the Turkish Armed Forces' Strategic Research Center (SAREM) in Ankara.

EOS activities in Critical Infrastructure Protection

By Luigi Rebuffi

Critical infrastructures are increasingly vital to our modern economies as citizens, businesses and governments all rely on an array of interlinked physical and information infrastructures for their daily operations.



Critical infrastructures are not only vulnerable to malicious attacks and other man-made malfunctions, technological failures, natural disasters and hazards, but also they are becoming increasingly interdependent, which means that the disruption or failure of one of them can result in cascading effects. Suffice to recall the November 2006 electricity black-out in Western Europe, the January 2009 Russia-Ukraine natural gas dispute leading to severe supply disruptions in the EU, and the April 2010 volcanic ash cloud crisis. This means that the failure to reach sufficient resilience standards in one country can have a detrimental effect on many others, in other words, an interconnected network is only as strong as its weakest link.

State of play in the EU

Being aware of these threats and challenges the EU and the Member States have identified critical infrastructure protection (CIP) as a key security priority, which has led to the development of all-hazard approaches in many countries. In recent years, the European Commission has also adopted a number of policy initiatives, namely the 2006 **European Programme for Critical Infrastructure Protection (EPCIP)** designed to raise critical infrastructure protection capability across all EU Member States and in all relevant sectors of economic activity. This framework contained a number of binding and non-binding measures including: financial support for projects related to CIP (CIPS Programme), a dedicated CIP information sharing network (CIWIN), an external dimension, and, as a key element, the **Directive 2008/114/EC on the identification and designation of European Critical Infrastructures** focusing in the transport and energy sectors, and introducing requirements on information exchange and basic security measures.

However, a number of outstanding problems remain: a) Member States have fragmented national policies with varying degrees of maturity and although all Member States have legally implemented the Directive, the sector-focused approach of the Directive represents a challenge as in practice the analysis of criticalities is follows a 'system' or 'service' approach; b) despite having raised CIP awareness and fostered European co-operation, the Directive has mainly encouraged the bilateral engagement of Member States and not established a European forum for decision-making; c) finally the lack of common methodologies for risk evaluation and risk reporting represents a serious gap. The implementation of a harmonised assessment methodology would require databases at EU level for threats, vulnerabilities, interdependencies and impact of critical infrastructures disruption that do not exist, in this regard, Member States have repeatedly asked for EU support.

EOS CIP activities

EOS has been very active in the field of CIP, developing a number of security projects under the Seventh Framework Programme of the European Commission addressing critical energy infrastructure, land transport, supply chain, civil aviation and cybersecurity. Several of EOS projects focus on energy and transport thus mirroring the sectors prioritised in the Directive 2008/114/EC, but are not limed to this scope also covering the undisputable link to cybersecurity. An overview of the work developed in these areas is presented below.

Energy

The **European Risk Assessment and Contingency planning Methodologies for interconnected energy networks (EURACOM)**, was a FP7 financed Coordination Action finalized in 2011 and led by EOS with the participation of members of several countries, including Transelectrica from Romania. Addressing the issue of protection and resilience of energy supply for European interconnected energy networks, the project's objective was to identify, together with European Critical Energy Infrastructures operators, a common and holistic approach (end-to-end energy supply chain) for risk assessment and risk management solutions.

By establishing links and coherent risk management procedures across energy sectors and EU countries, the project aimed at increasing the resilience of critical energy services across the whole energy infrastructure.

Its main deliverable was the development of a holistic approach to risk assessment and contingency planning, in a format that can be used as a framework for implementation by the Energy sector operators, through the creation of a risk assessment and of a contingency planning approach to be implemented at operator level and recommendations on how risk assessment and contingency planning processes can be implemented and

EOS activities in Critical Infrastructure Protection

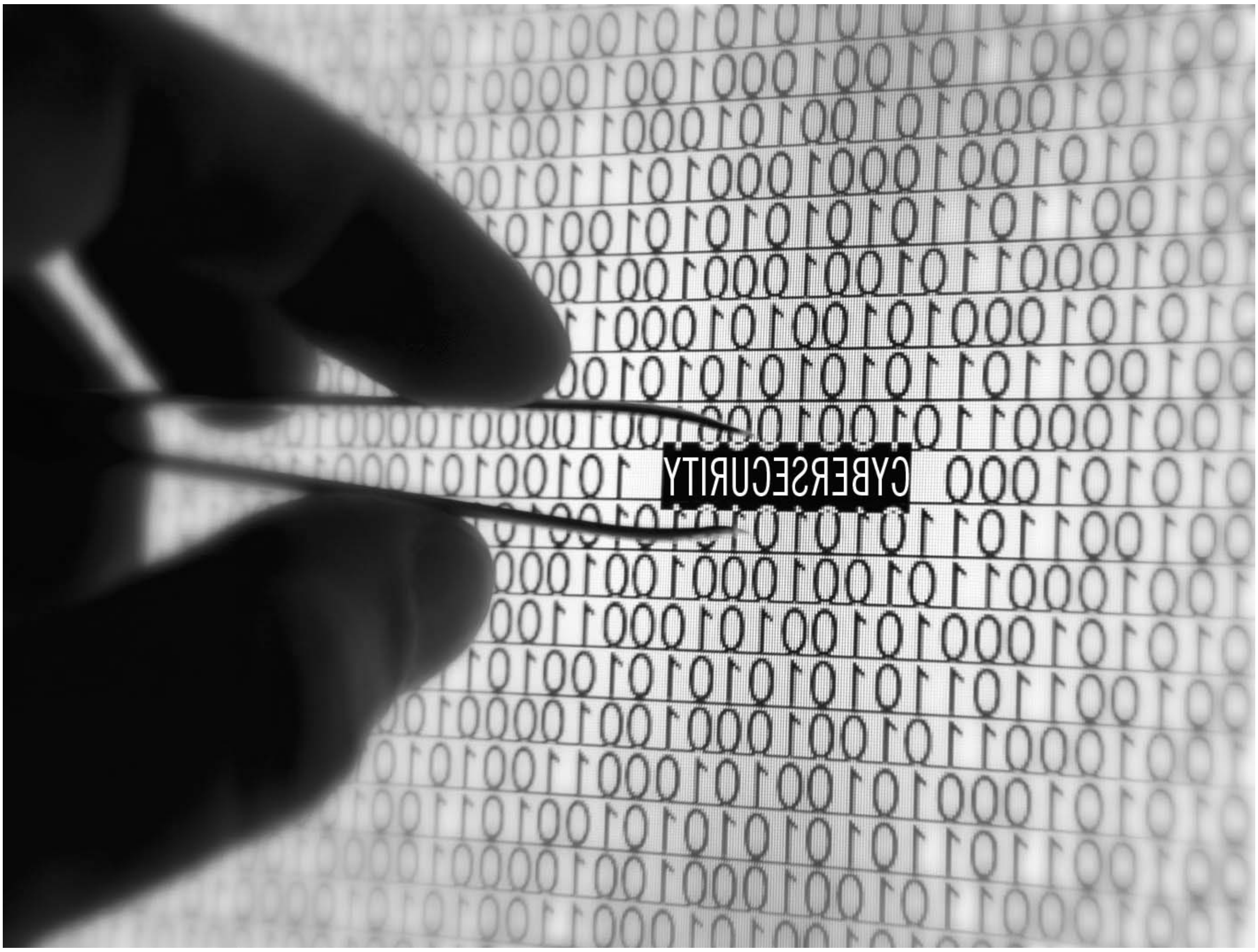
supported at a higher level of analysis. EURACOM methodology and procedure thus offered the basis for compatible assessment and management tools that can be easily adapted, thus contributing to the implementation of consistent European and national policies on the protection of critical energy infrastructures.

The results of EURACOM have been well received by Member States regulators, however we still see limited private public dialogue between the European Commission, the regulators, the operators and the security providers, likely due to concerns over the regulatory burden associated with risk assessment and contingency planning obligations.

Transport

Regarding **Land Transport** security and in line with the Commission activities in this sector - currently focusing on secure lorry parking, cyber-crime in transport networks, multimodal passenger terminals problematic and rail crime - EOS is part of the **Secured Urban Transportation – A European Demonstration (SECUR-ED)**. This four year (2011-2014) FP7 demonstration project aims to provide a toolkit to improve urban transport security in medium to large sized cities and includes the participation of all major stakeholders from across Europe. Based on best practices, SECUR-ED will integrate a consistent, interoperable mix of technologies and processes, covering all aspects; from risk assessment to complete training packages. SECUR-ED's rationale is to create a global European improvement in mass transportation security through the development of packaged modular solutions validated through flagship demonstrations in Madrid, Paris, Milan and Berlin (4 in total plus additional satellite demonstrations). Each city will play host to several distinct scenarios. These demonstrations will seek to validate the security enhancement packages, acting as the showcase for this unique European initiative.

On **Supply Chain** security, given that approximately 70% of all cargo is transported in intermodal shipping containers, container security associated with terrorist threats, illegal immigration, theft and smuggling is an important factor in the overall European cross border security and in the wider issues of optimization of supply chains. Following this need for monitoring and tracking of shipping containers EOS is also participating in **CONTAIN**, a FP7 project initiated in 2011, having as main goal to specify and demonstrate a European Shipping Containers Surveillance system which encompasses regulatory, policy and standardisation recommendations, new business models and advanced container security management capabilities. The project also focuses in demonstrating Secure Multimodal Corridor Design and Chain Monitoring & Control across



international and European corridors at Interporto Bologna, Rotterdam /Amsterdam and Valencia.

In the **Civil Aviation** field it has become clear in recent decades that the number of threats to aviation security has grown significantly, which has led to even more security regulations as the threats evolve. Security procedures have become exceedingly complex and invasive to passenger privacy, at the same time passenger and cargo traffic are expected to double in the next 15 years. It is thus clear that the current complex security system cannot be adapted to such a growth as it has already and will increasingly become a major market restraint. Therefore, the **Comprehensive European Approach to the Protection of Civil Aviation (COPRA)** FP7 project was initiated with the objective of developing requirements and recommendations for future research activities which could lead to a more resilient, flexible and comprehensive approach. To that aim COPRA brought together major air transport stakeholders, who identified and categorised 70 current, emerging and new threats to airports, aircrafts and auxiliary infrastructure, compiling more than 350 possible security measures to counter these threats. Over 50 conceptual ideas for overarching approaches to passenger, cargo and external security concepts were assessed according to the balance of security benefit, costs, impact on the aviation system and public acceptance and constraints. Using all of these results as a basis, the requirements for future research and development have been laid out in the COPRA Aviation Security Research Roadmap.

Cybersecurity

Cybersecurity is of growing influence regarding all critical infrastructures in Europe, impacting smart grids, air traffic management, the tracking of parcels and cargos, among many other critical societal services. The EU, Member States and the private sector have become increasingly aware that cyber threats pose important challenges not only to the security of their network information systems, but also to the integrity of their physical infrastructure, not to mention the risk of domino effects across entire networks and affecting multiple sectors of economic activity.

Voicing these growing concerns a number of activities have been recently launched in the EU, with a new Cybersecurity Strategy of the European Union and a proposal for a Network and Information Security Directive. Foreseeing the current and future importance of cybersecurity in the European market, EOS is developing several projects aiming to increase the capacity of industry to protect itself from cyber disruptions by European Cybersecurity Protection Alliance (**CYSPA**), and investing in the development of a cybersecurity research agenda for privacy and technology challenges (**CAPITAL**).

Way forward

A Commission **Communication on a new approach to the European Programme of Critical Infrastructure Protection** is expected in the summer of 2013. It presents the results of the comprehensive review process of the 2006 Programme and the Directive 2008/114/EC and proposes a new implementation of the EPCIP to better pursue the main policy objectives: improve the overall protection and resilience of EU critical infrastructures (CIs). This implementation will be gradual and composed of several building blocks addressing prevention, preparedness and response.

The initial work will focus on four selected EU CIs: Galileo, Eurocontrol, the European Electricity Transmission Grid and the European Gas Transmission Network. Activities will include a detailed assessment and analysis of processes and methodologies used by the four selected CIs, as well as a comprehensive overview of their criticalities and interdependencies. By comparing these, common concepts, including CIP risk assessment and risk management methodologies and preparedness measures, will be agreed on following discussions with selected stakeholders. In addition, the possible inclusion of required CIP expertise within the Union Civil Protection mechanism for long-term recovery of critical services will also be assessed.

The main objective is to develop and benchmark an EU approach for to be disseminated to other infrastructures and sectors of critical importance and, at a later stage, to regions where Member States are interested in cooperating with each other on a voluntary basis. An important spill-over-effect is expected, which would to make the EU better prepared for threats to CIs in Europe and improve overall resilience in case such disruptions occur.

EOS activities will contribute to support the new approach proposed in the Communication according to the interest of its members and the competence they will provide, in order to develop a harmonised and competitive security market for critical infrastructure protection. **CIP**

Dr. Luigi Rebuffi
CEO, of the European Organisation for Security (EOS)

Specialization:
B.Sc. in Nuclear Engineering at the "Politecnico di Milano" (1984)
PhD in Engineering at the Paris – Orsay University (1987) with a fellowship of the European Commission

Interests and Activity:
From 2003 to 2007 he was the Thales Director for European Affairs for Division Services and Division Security. He was responsible for the development of business and research activities with European Institutions of these Thales Divisions. Since 2007 he is the Deputy Director for Security of ASD – Aerospace and Defence Industry Association of Europe developing at European level common sectoral positions on security issues. Since 2003 he is the initiator and since 2007, the CEO, of the European Organisation for Security (EOS), gathering the most important European private security stakeholders and public NGOs from supply and demand side to develop and implement consistent European security solutions and services in a comprehensive approach.

Bulgaria: Protecting National Critical Infrastructures with the Contribution of the Ministry of Defense

By Todor Tagarev

The term "infrastructure" is used by the military since the 19th century. During the first decade of the Twenty first century, with the rise of international terrorism, its significance for the national and regional security sharply increased. Among the reasons for increased attention to critical infrastructure protection policy were the terrorist acts in New York and Washington (2001), Madrid (2004) and London (2005), as well as the development of major infrastructure projects for transportation of petroleum, gas and other energy and strategic resources.

The term 'critical infrastructure' was introduced in Bulgaria's legislation in 2005 with the 'Law on Crises Management,' and was later adjusted to reflect the EU definition in Directive 114/2008.[i]

The contribution of the Ministry of Defence of the Republic of Bulgaria and the Bulgarian Armed Forces to the protection of the national critical infrastructure is stipulated by the Disaster Protection Act, the Law on Defence and the Armed Forces, as well as in the Ordinance on the Procedure and Authorities Competent for Specification and Risk-Assessment of Critical Infrastructure Sites. This issue is also reflected in the National Security Strategy and the National Defence Strategy.

The National Security Strategy of Republic of Bulgaria [ii] in its article 102 stipulates that "The Republic of Bulgaria meets commitments deriving from the Directive [114] concerning the protection of European and national critical infrastructure and mandating the cooperation between public and private organizations on the basis of mutual interest and partners' expertise in order to guarantee the protection of public interests and needs by efficient allocation of funds, risks and benefits in the process.'

Article 145 of the National Security Strategy envisions contribution of the Bulgarian Armed Forces to the protection of the national critical infrastructure in the effort to prevent disasters and accidents, as well as to cope with their consequences.

The National Defence Strategy (NDS),[iii] in its Chapter VI 'Use of Armed Forces', elaborates further on this contribution. Article 67 states that 'In peacetime the Armed Forces participate in crisis response and disaster relief operations on the territory of the Republic of Bulgaria, and perform as well tasks for: control of air space, control of shipping and support to migration control; protection of the population in case of disasters, management of the consequences of disasters, emergencies and terrorist acts.'

Article 71 of NDS specifies the CIP tasks to be carried out by the Bulgarian Armed Forces: "... the Armed Forces perform tasks on providing protection and defence to critical infrastructures, strategic sites and activities and shall provide, if necessary, military units and resources to enhance physical protection measures, in implementation of their operational plans.'

In accordance with the White Paper on Defence and the Armed Forces of the Republic of Bulgaria [iv] and the Armed Forces` Development Plan,[v] the three Services of the Armed Forces perform tasks on critical infrastructure protection, respectively maritime infrastructure, and strategic sites on the territory of the country.

Legal definition of 'critical infrastructure' is given in Article 15 of the Additional Provisions to the Disaster Protection Act,[vi] as follows: "'Critical infrastructure' shall be a system or parts thereof, which are essential for the performance of vital public functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would cause significant negative consequences for the Republic of Bulgaria as a result of the failure to retain those functions."[vii]

Similar definition is set forth by Article 18 of the Additional Provision to the Law on Defence and the Armed Forces,[viii] defining 'Critical infrastructure' as "the system of equipment, services and information systems, whose stopping, impaired functioning or destruction would have serious negative impact over the health and safety of the population, environment, national economy or over the effective functioning of the state governance."

Article 35(3) of the Law on Defence and Armed forces of the Republic of Bulgaria stipulates that "'The Ministry of Interior' bodies independently or jointly with the Ministry of Defence, the units directly subordinated to the Minister of Defence and the Bulgarian Armed Forces and other specialized bodies shall provide defence of strategic for the country activities and sites, as well as of those, declared as critical infrastructure." The Bulgarian Armed Forces are tasked to protect and defend critical infrastructure

N
E
W
1806 km
KUTAISI
GEORGIA
8900 km
OKA
DAEGU
KOREA
1921 km
GYUMRI
ARMENIA
7800 km
LUOYANG
CHINA
km
TURK
КОШИЦЕ
СЛОВАКИЯ
БЪРНО
ЧЕХИЯ
ПОЗНАН
ПОЛША
САНКТ-ПЕТЕРБУРГ
РУСИЯ
243
МАКЕДОНИЯ
324 km
GREECE

Bulgaria: Protecting National Critical Infrastructures with the Contribution of the Ministry of Defense

installations and for that purpose developed specific operational plans. These tasks are as follows:

- Building and maintaining a early warning system for potential risks and threats;
- providing support when necessary to other government organizations with assigning trained reaction forces/units within the framework of existing capabilities;
- supporting, when necessary, other governmental organizations and local authorities in preventing and overcoming the consequences of terrorist attacks.

Military units could possibly take part in the protection and defence of installations from the critical infrastructure outside the state territory and in the prevention and overcoming the consequences of terrorist attacks abroad in accordance with standing international agreements.

Critical infrastructure protection tasks are executed by units from different branches of the Armed Forces and in particular by the Duty Forces and units designated and trained for the support of other governmental organizations and local authorities to prevent and overcome the consequences of natural disasters.

The activities of the Duty Forces and assets (ships, helicopters, airplanes, GBAD, command, control, surveillance and early warning and alert system, etc.) basically include, but are not limited to surveillance and early warning and alert as well as reaction to prevent possible treats and to overcome the consequences therefrom.

The Duty Forces and assets execute their tasks on the state territory, the national airspace and the territorial sea in accordance with national legislation. It is possible to execute tasks on the territory of other countries with which Republic of Bulgaria has a standing agreement. One example is the "Memorandum of Understanding regarding the protection of the strategic facilities and facilities of special importance in the proximity of the common border against air terrorist attacks," signed in 2002 with the Republic of Romania. For developing critical infrastructure protection capabilities contribute also the bilateral agreements regarding air policing and cross-border operations, signed with neighbouring countries that are NATO members. The first agreement of this kind in South Eastern Europe, in force since 2012, is the one between Bulgaria and Romania. Under development are similar agreements with Greece and Turkey.

As required by the Disaster Protection Act, Ordinance on the Procedure and Authorities Competent for Specification and Risk-Assessment of Critical Infrastructure Sites was adopted in 2012.[ix] It determines the procedures and authorities competent for the specification of critical infrastructure sites in order to reduce risk of disasters and protect the population. Coordination and control of the overall process are assigned to the Minister of the Interior. Critical infrastructure sites and their location are determined by relevant Ministers, assisted by standing committees. Working groups for different sectors elaborate particular rules for identifying critical infrastructure sites and their location and prepare a list. The Ordinance sets forth the respective order, procedures and authorities competent to assess risk. The Minister of the Interior issues guidelines to the standing working groups to elaborate risk-assessment methodology. Control over facilities of strategic importance for national security is conducted by the State Agency "National Security."

In compliance with the Ordinance, a standing working group was formed to determine MOD critical infrastructure facilities.[x] The working group was tasked to develop Rules for Determination of Critical Infrastructure Facilities of the Ministry of Defence. A draft of these rules was elaborated and is currently under discussion. These Rules will lay down the basis for elaboration of a List of the Critical Infrastructure Facilities of the Ministry of Defence, to be followed by a Methodology for risk assessment for the facilities on the list. The two documents are to be finalized by the end of July 2013.

In addition, in compliance with the Regulation of the Council of Ministers # 181/2009, strategic sites and activities of the Ministry of Defence for the national security are determined by a ministerial order. They are considered national critical infrastructure.

In accordance with NATO commitments, an assessment of the national critical information infrastructure during Alliance operations in the region is forthcoming. It will utilize a methodology developed by NATO Allied Command Transformation and tested in Norway and the Netherlands.

The EU policy on critical infrastructure protection has been rapidly evolving since 2004 in the context of the fight against international terrorism, with the European Programme for Critical Infrastructure Protection (EPCIP) and a Critical Infrastructure Warning Information Network (CIWIN) already in place.

National requirements, NATO and EU commitments provide the following directions for the development of CIP capabilities:

Improvement of the coordination and cooperation among ministries and governmental agencies during the planning and execution of operations for Critical Infrastructure Protection by:

- standardization and optimization of the information exchange;
- achievement of common understanding of the situation, tasks, available capabilities, structure of acting entities and on-going processes;
- development of required capabilities of the Reaction Forces by:
- Task-tailored training;
- Coordination of training plans of different ministries and government agencies for joint capability development;
- Coordination of action plans;
- Constant improvement of the command and control system during crises of non-military nature.

Development of cyber-defence capabilities.

Development of the cooperation with neighbouring NATO and EU member countries in the area of critical infrastructure protection.

The processes for designation of critical infrastructures, derivation of capability requirements, bi-lateral cooperation and coordination within NATO and the EU in CIP capability development are still to mature. Structured exchange of information [xi] among both governments and academics may make the process more efficient to the benefit of allies and partners. **CIP**

References

[i] "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection," Official Journal L 345: 75-82.

[ii] Endorsed by the National Assembly on 25 February 2011.

[iii]Adopted by the Council of Ministers on 13.04.2011

[iv] Endorsed by the National Assembly on 28.10.2010

[v] Endorsed by the Council of Ministers, resolution 333, 29.12.2010

[vi].Prom. SG. 102/19 Dec 2006, last amend. SG. 80/14 Oct 2011

[vii] For further thoughts on the utility of defining 'vital' or 'essential' services and functions see Todor Tagarev, Venelin Georgiev and Valeri Ratchev, "A Taxonomy of Essential Services," *Radioelectronic and Computer Systems*, no. 58 (May 2012): 191-196, www.IT4Sec.org/node/3307.

[viii] In force from 12.05.2009. Prom.SG. 35/12 May 2009, last Amend. SG 33/ 27.04.2012

[ix] Adopted by the Council of Ministers `regulation 256/17.10. 2012 ., in force from 23.10.2012 . Promulgated SG 81/23.10.2012, amended and supplemented SG 19/ 26.02.2013

[x] by order of the Minister of Defence – 48/13.02.2013

[xi] See for example the proposals elaborated in Todor Tagarev, Venelin Georgiev and Petya Ivanova, "Analytical Support to Critical Infrastructure Protection Policy and Investment Decision-Making," *Information & Security: An International Journal* 28, no. 1 (2012): 13-20, http://dx.doi.org/10.11610/isij.2801.

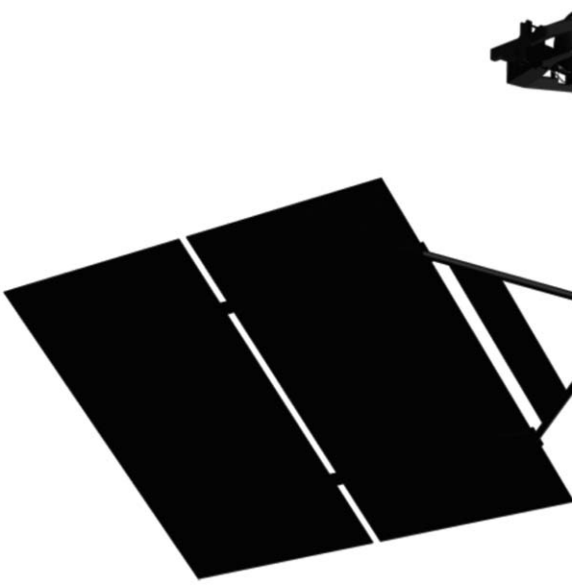
Dr. Eng. Todor Tagarev
Member of The Bulgarian Academy of Science
Senior Researcher at the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences and Head of its IT for Security Department
Director, Centre for Security and Defence Management
Editor in chief of "*Information & Security: An International Journal*"

Specialization:
M.Sc. in electrical engineering (1982), Air Force Academy, Bulgaria
Ph.D. (1989), Air Force Engineering Academy, Moscow
Defence policy and planning, security sector reform (primarily from organizational management perspective, with focus on planning, resource management, and process improvement)

Interests and Activity: Security and defence planner combining governmental experience with sound theoretical knowledge and background in cybernetics, complexity, and security studies; Specializing in security sector reform, primarily from organizational management perspective; Considerable expertise in leading and participating in national and international research teams. Currently involved in various projects on foresight based security policy making and planning.

Space Security, a Critical Component of the Future European Global Strategy

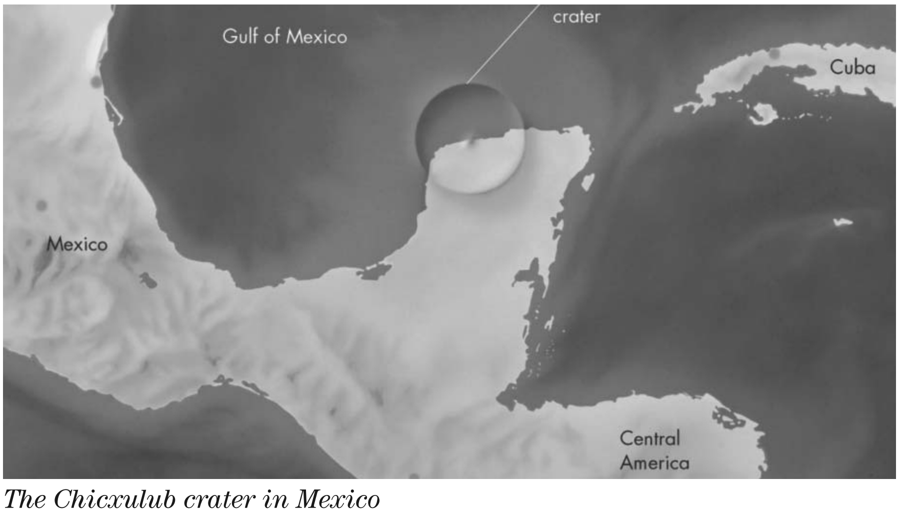
By Dr. Liviu Mureșan and Alexandru Georgescu



The importance of Space Security has been apparent for some time, with consecutive discoveries and recent events adding weight to the idea that the pursuit of Space Security should receive more attention and funding than it already has. On the one hand, space based systems have, in the last few decades, become a critical enabler for a wide spectrum of applications, not limited to communications, weather observations, command and control for numerous industries, as well as emergency and crisis management. At the same time, these systems, greatly clustered in low Earth orbits, are under threat from random collisions, in this increasingly crowded environment, with the debris of past human activity.

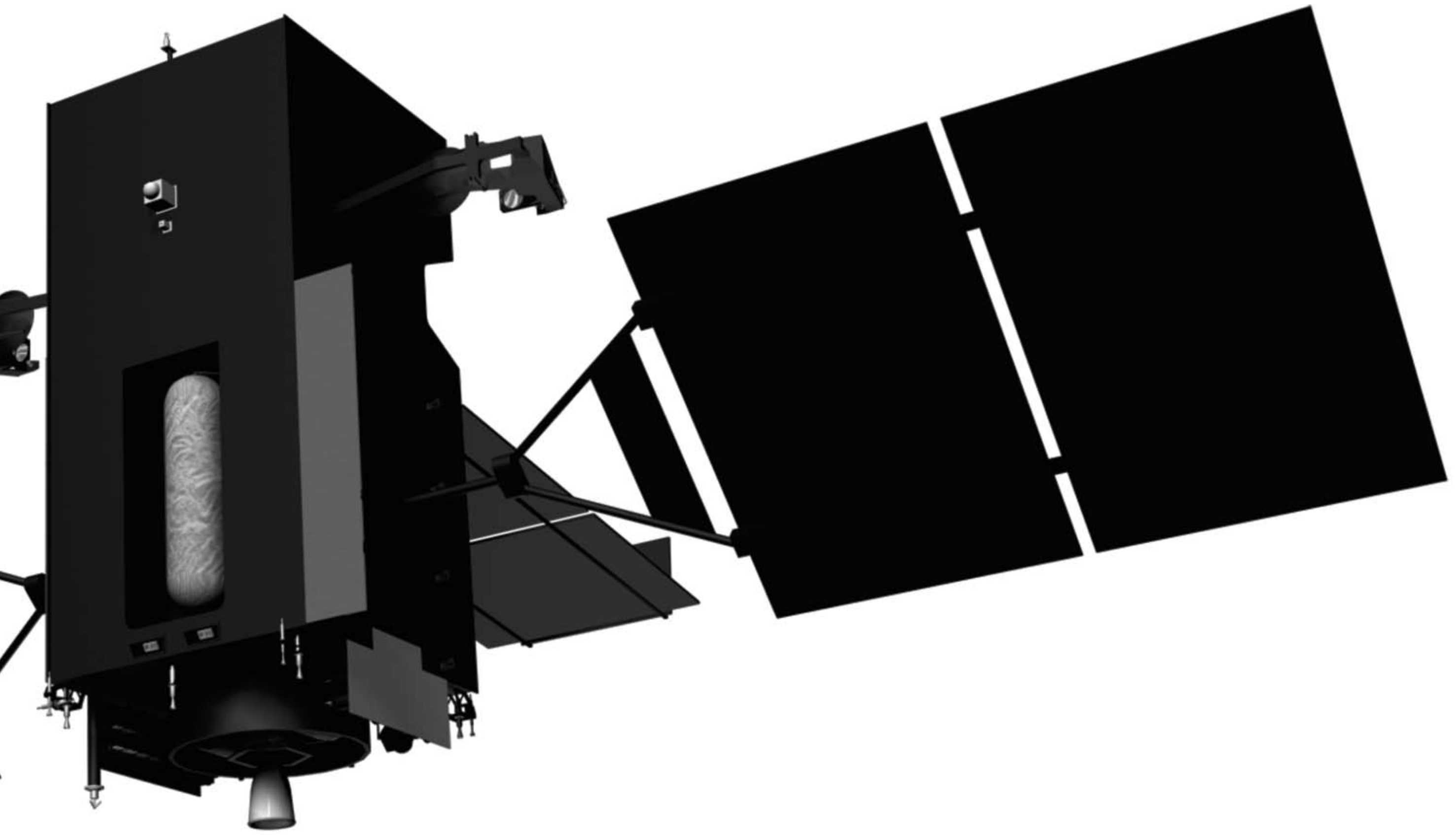
Their destruction or disruption would greatly impact business continuity and quality of life, leading to incalculable losses, especially in advanced societies which have formed a greater dependence on them, such as the European nations. Stewarding this "orbital commons" is a collective responsibility of the spacefaring nations and the myriad space stakeholders, and an area in which European initiatives may provide leadership, leading to soft power, prestige and extensive economic opportunities.

On the other hand, outer space is the originating environment of significant threats that we are just now beginning to understand. The meteorite impact in Chelyabinsk, Russia, along with the coincidental and much more serious near-hit, on the same day, of an asteroid that was the same caliber as the one that produced the Tunguska event in 1908 (which flattened 2,000 square kilometers of forest), highlight the urgency of documenting and dealing with the objects whose trajectory can transform them into kinetic warheads. In October 2014, there is a slim chance of witnessing, on Mars, the impact of a comet whose supposed physical characteristics would place the impact in the same range as the one that destroyed the dinosaurs at the end of the Cretaceous period and produced the Chicxulub crater in Mexico. The growth of our awareness of the potential dangers that traverse our planetary neighborhood has only added to the urgency of the requirement to act.

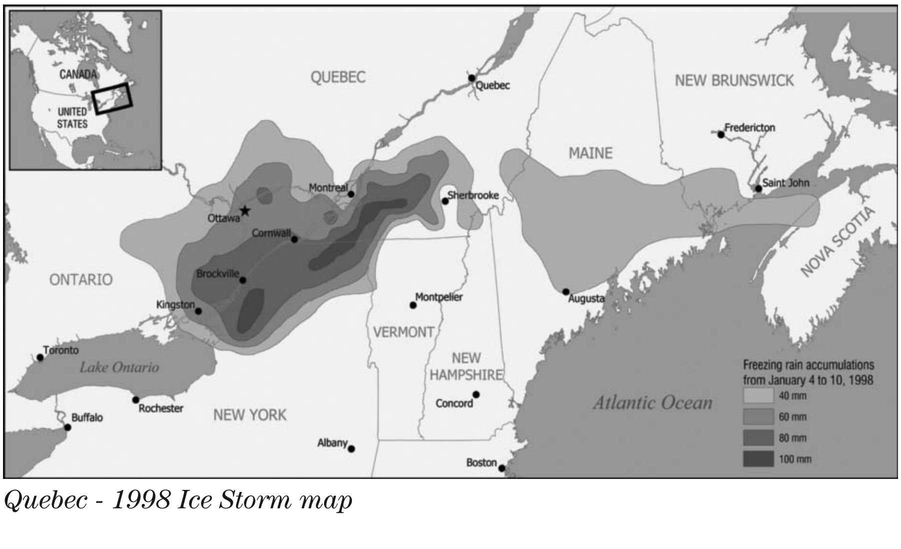


The Chicxulub crater in Mexico

There is also a more diffuse, but similarly dangerous threat, especially for advanced societies – that of "space weather", a term which describes the changes in radiation, magnetic fields, plasma and other space matter independent of Earth-based phenomena, and which are largely driven by Solar activity. The variations in this outer space ambience can lead to values which are high enough to damage not only space



based assets, but also infrastructures on the ground. These phenomena have been under observation since 1859, when the Carrington event, a 500 year peak of solar activity, caused equatorial auroras to appear, telegraph lines to short circuit and poles to catch on fire. Future events, in 1921 and 1960, disrupted radio communications. In 1989, millions of inhabitants of Quebec were left without electricity when a transformer was destroyed, and in 2003, the same thing happened in Sweden, at a lesser scale, along with grounded flights and one destroyed NASA satellite. Unlike statistically distant impact events, these phenomena take place on a cycle related to the Sun's internal processes, with a new high point predicted for the near future, and a certainty of new disruptions of business continuity and quality of life unless appropriate measures are taken.

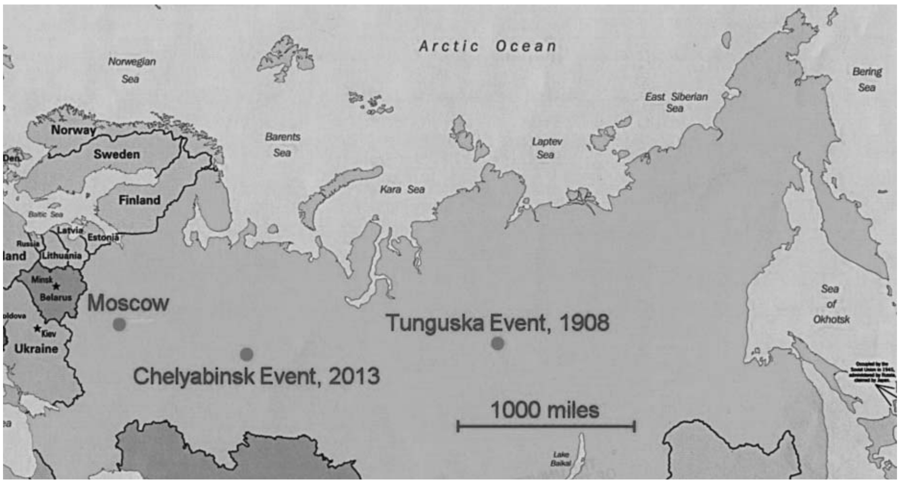


Quebec - 1998 Ice Storm map

These are some of the reasons why Space Security should become a priority focus for European security leaders and decision makers. At the same time, a future European Global Strategy could provide the optimal venue for making recommendations on the development of Space Security, in terms of scope and depth, as well as through a holistic approach towards issues of European interest with a global perspective.

For one, Space Security is indelibly linked to other areas, such as Critical Infrastructure Protection, scientific research and emergency and disaster management. It is, therefore, logical to address the issue as part of a common narrative relating to security on the one hand, and development and competitiveness on the other.

Secondly, the nature of space-based threats and of human interests in space (existing assets, industrial development and so on) means that Space Security features a high degree of interconnectedness between beneficiaries. A hypothetical European or national initiative cannot reason-



The russian map of the meteorite event

ably expect to exclude other countries from the security benefits it generates, just as the country in question will benefit from the initiatives of others. The opposite is also true – no European efforts in Space Security matters will truly be effective without similar efforts on behalf of other stakeholders, national and otherwise. The global nature of many space threats such as Near Earth Object impacts and "space weather" tends to compromise the effectiveness of solutions that remain at national or regional levels. Can a European or non-European detection program for possible future impacts filter its activity to only warn against threats to their own territories? Will the adoption of guidelines for limiting the amount of space debris that is created during normal human activity in space be as effective in the absence of cooperation with the developing spacefaring nations? Even the hardening of one's own space infrastructure against the harsh conditions of space does not immunize against threats to quality of life and business continuity, since there is also a demonstrable dependence, on the part of European citizens and companies, on infrastructure belonging to other actors. At the very least, due to globalization, the materialization of risks in other areas of the world will have an impact on European well-being and warrants inclusion into the security calculus.

Finally, the very developments associated with Space Security will, in addition to bolstering private investor confidence, create new opportunities

for growth and rising competitiveness, as new capabilities are developed and new efficiencies harnessed in the course of eliminating security gaps. Solutions developed as part of Space Security efforts can also become products with global markets, in addition to minimizing the considerable financial and human costs of a breakdown in the functioning of space critical infrastructures or of terrestrial infrastructures under the influence of space threats.

To that end, the Space Security portion of a future European Global Strategy can advance diverse solutions, with positive externalities and an awareness of various interdependences, such as:

- A consolidation of the various national and European space initiatives, with a greater emphasis on knowledge sharing and security research, under the umbrella of the European Space Agency, as utilizing an existing framework serves to reduce administrative costs.
- The implementation of an "S3: Smart Space Security" philosophy, wherein various groups begin to create specialized capabilities for research, development, risk governance and crisis resolution. In an era of increased budgetary awareness, this counts towards reducing costs, eliminating the duplication of efforts and achieving new competences. Similar to this is the "Smart Defence" and "pooling and sharing" policies promoted by NATO and EU, which have been well received and designed with many of the same restrictions and "value for money" requirements that Space Security will face.
- Working towards linking Space Security with national and European initiatives for Critical Infrastructure Protection, as implemented by public and private actors. Space Security provides a whole new dimension of risk awareness to these actors, by expounding on the new threats they face, but, also, the new tools for command, control and coordination which are at their disposal. An example of this would be the hardening of assets such as electricity grids, power plants, communication grids, server farms and others against the deleterious effects of increased solar flare activity. This would be a long-term endeavor, also from a global perspective, involving European, national, regional and local authorities, as well as the Critical Infrastructure Operators themselves and representatives of civil society.
- Pursuing a policy of "osmosis", through close cooperation with non-European stakeholders in Space Security who are acting in good faith. This means that international cooperation can serve to fill in the gaps that the various participants possess in terms of space awareness and security, enhancing the effectiveness of Space Security efforts for all. An important actor in this regard is the UN, which can serve as a main vehicle for the dissemination of good practices and technical standards for Space Security purposes, through its United Nations Committee on the Peaceful Uses of Outer Space. At the same time, cooperation can highlight the overlooked issues which present important inherent opportunities for security and growth. For instance, the latest UN initiative, coming on the heels of the publicized meteorite events in Russia, relates to the detection, deflection, possible destruction in extreme cases of such threats, and mitigation of consequences in case of inevitable Earth impact. However, there is no corresponding attention given to research into the best means for population evacuation, damage reduction, resumption of normal activity and support for the affected governments to implement all of the above. This presents itself as an opportunity for the European Space Agency and other European institutions to fill in this important gap.

The development of a future European Global Strategy will, necessarily, highlight even more opportunities for synergistic development of different European interests, beyond security and growth or security and international cooperation. Within this framework of intersecting knowledge applied to priorities, Space Security serves as both a source of fresh perspectives and a component which adds weight and novelty to the final result. **CIP**

Dr. Liviu Mureșan
Executive President of the EURISC Foundation – European Institute for Risk, Security and Communication Management
Executive President of ARPIC – Romanian Association for the Promotion of the Protection of Critical Infrastructures and Services

Specialization:
B.A. in in Economics, Academy of Economic Studies, Bucharest, Romania (1969)
Ph.D. in Economics, Academy of Economic Studies, Bucharest, Romania (1978)
Further training at the Defence College NATO GFO (Rome), the Institut des Hautes Etudes de Defense Nationale (Paris) and the Center for Civil–Military Relations (Monterey)

Interests and Activity: Strategic issues, critical infrastructure protection, energy security, security sector reform, crisis situation management, security and defense, security culture, foreign policy and diplomacy, political issues, information and communication. He held several positions in the Romanian governmental structures: Senior Adviser to the Prime Minister, Senior Adviser to the Romanian Government, Senior Adviser to the Interior Minister, High Representative of the Romanian Government of the Anti–Corruption Initiative of the Pact of Stability (SPAI) and of the Combating Organized Crime Initiative (SPOC). He was Director of the Romanian Agency for setting up the regional Center for Combating Transborder Organized Crime, and as the Deputy Director of the National Defence College he was the first civilian appointed in command position in the Romanian Army (1993–1994). He was a member of the Romanian Parliament, leader of the Majority (1990–1991). He is Executive President of the Euro–Atlantic Council Romania – Casa NATO, EURODEFENCE Romania and member of Security and Defence Agenda (Brussels). He chaired the 11th Working Group of the ESRIF – European Security Research and Innovation Forum, and, more recently, an active contributor to the European Global Strategy project.

Energy Security in Romania through an EU and NATO lens

By Adrian Vâlciu

Through their nature, critical infrastructures are essential for economic prosperity, national security and quality of life. Therefore, both at national and European levels, their continued functioning is a priority and the source of significant preoccupations, so much so that critical infrastructure protection efforts are an essential component of a society's sustainable development.

Current geopolitical and geostrategic trends and perspectives expound on the notion of "national security" as an integrator of economic, ITC, diplomatic, environmental and other components. Critical infrastructures are, generally, vulnerable to disruptions by external and internal factors and are at risk of being destroyed or rendered unfunctional.

Given the growing vulnerability of infrastructures, and the fact that disruptions can have multiple points of origin – whether human, natural or technological – governments and competent institutions are awarding ever greater attention to the complex task of ensuring their security. This explains why grids/public systems (governmental, military etc), as well as their private counterparts are protected through physical, legal and informational means agains actions and inactions which may threaten their security and functional status.

With regards to the energy sector, especially the electricity subsector, we can safely confirm the existence of a wide range of threats. We should also remark on the fact that the most recent systemic failure in the Romanian energy system took place on May 10th 1977, so the national system has a track record of uninterrupted viability, security and operational safety for the past 35 years.

The complexity of the international context, being characterized by armed conflict and a rising tide of international terrorism, has led to a new perspective for approaching the concept of security. In the not so distant past, the security of a system was conflated, mostly, to coincide with the operational security and safety.

The events on September 11th 2001, however, led to a separation of the two areas. Technical capabilities that ensure the safety of a system's functioning are complemented by security measures that shield the operational framework and its objective oriented design from disruptive elements originating outside the system.

Electricity systems are especially vulnerable to terrorist attacks, either physical or originating in cyberspace, since they were never designed for such a category of threats. Terrorist attacks are differentiated by the type of objectives they pursue. The following types of attacks can take place on energy systems:

- Direct attacks, where the energy system is the prime target and the disruption of supply to consumers is a secondary concern;
- Through system usage, some parts of the energy infrastructure are converted into weaponry against the population (for instance, an attack on a nuclear power plant);
- Attacks through the system, wherein consumers are denied the fulfillment of their energy requirements (or a certain category of consumers, such as military units or residential areas etc.).

The current organization of the Romanian energy system is based on European Directive 72/2009 regarding common norms for the internal electricity market and 73/2009 regarding common norms for the internal natural gas market. As a distributed infrastructure, the Romanian electricity system presently features a complex structure, in which diverse production, transportation and distribution entities cooperate on the basis of contractual relations.

This situation can lead to dysfunctions in the handling of crisis situations, such as terrorist attacks and emergency situations, as well as to incoherence regarding the drafting of collective plans for rapid recovery in the aftermath of such events. Though unitary in its technical functioning, the electricity system's contractual mode of functioning generates sector interdependencies that may be a source of added vulnerability.

For instance, extreme weather phenomena are an increasingly common threat that we need to factor into our daily lives. There is a well substantiated need to reconsider the threat posed to us by extreme weather phenomena, because their severity often exceeds the design limitations of existing systems. Since the reassessment of the functional demands and pressures on systems is not handled in a coherent and unified manner, it is virtually impossible to exhaustively assess the risk of malfunction, in case of major disturbances, all throughout the production-transportation-distribution chain of electricity.

The European approach towards designing general norms for the functioning of electricity systems emphasizes the role of the system and transportation operators, who are designated as technical authorities who can spearhead greater technical uniformity and raise the interoperability of various European systems. As part of ENTSO-E (European Network of Transmission System Operators for Electricity), the security of electricity systems is based on the following premises:

There are a multitude of physical and informational resources that must satisfy the security demands of the system, at local and global level;

There is a widespread pattern of physical distribution for system components;

There is a relative autonomy throughout the components of the system;

There is a transparency of the system structure with regards to the operational demands placed on it;

There is a unified and global vision regarding the system.

The priority actions for the next period are the drafting of specific methodologies for the risk analyses, as well as in support of the coherent and unified assessment of physical and cybernetic vulnerabilities. The Romanian experience has been a valued addition to the various Working Groups, given the security achievements in relation to the national energy system.

A new heading for the development of critical infrastructure protection efforts at European level is the cooperation between European structures and NATO. At ENTSO-E level, a number of working sessions were organized for the purpose of debating issues regarding the security of critical information systems (SCADA). Within the discussions, Romania presented the results of its bilateral cooperation with NATO structures specialized in industrial systems. This collaboration took the form of various activities: the organization, in 2008, of a NATO seminar on critical infrastructures in the area of natural gas, the outlining of the general security requirements of critical energy infrastructures, the Romanian project for instructing civilian experts from NATO in critical infrastructure protection, the assessment of the readiness level of electricity transporters for protection against cyberattacks.

The new paradigm of energy security demands a dialogue between critical infrastructure protection providers and actors. The breadth of the problem under advisement means that the framework of debate needs to include state and private entities, academia, civil society and critical infrastructure experts from various sectors whose specific competences can promote the creation of a viable Romanian model for critical infrastructure protection at the national level. **CIP**

Ing. Adrian Vilciu
Manager, Department for Critical Infrastructure and Systems, Transelectrica
NATO civil expert for critical infrastructure protection

Specialization:
Power Energy at Bucharest Polytechnic Institute (1992)

Interests and Activity: Physical security, Information Security, Cyber Security, Security Management, Critical infrastructure protection, Security Risk assessment, Risk management, Continuity Management; Standardization for alarm systems, information security, societal security, risk assessment;
Contribution to security related national legislation.

IRAQ THE RESILIENT POWER
From critical infrastructure protection to business continuity and quality of life

By Liviu MUREȘAN PhD , Alexandru GEORGESCU M.Sc
EURISC FOUNDATION – European Institute for Risk, Security and Communication Management, Romania

With its tremendous endowment with natural resources as development capital, Iraq seeks to move beyond simply extracting and exporting its subterranean wealth. Iraq must develop its considerable human potential and create an advanced economy that is not held hostage to international oil prices and in which the greatest number of people may create added value and share in this prosperity. The stakes for Iraqi society are very high – development brings with it social harmony and political stability, with significant positive effects on all citizens.

At the foundation of these ambitions, one finds a complex system of critical infrastructures, which ensure that the society and the economy have the material basis on which to exist and to develop. The more advanced a nation is, the more infrastructure it has, the more infrastructure it needs to build and the more infrastructures become critical to its very survival. These critical infrastructures range from pipelines and other industrial assets, to healthcare, water supply, food supply and, finally, education, communication and financial capabilities. Removing any one of these from the equation makes it impossible for a society to maintain its standard of life and develop economically. In the end, Iraq will only be as safe and as prosperous as its infrastructure will allow.

The notion of critical infrastructure protection (CIP) addresses the numerous vulnerabilities that such a complex system will generate. These vulnerabilities can be triggered either intentionally or through simple attrition, either alone or in a chained event, and can have devastating consequences. At the very least, they impact investor and citizen confidence and the uncertainty of safety makes it harder to plan for the future.

A significant interest was expressed in the content of this paper and what such a project would mean both for the Iraqi security establishment, and for Iraqi-Romanian relations. Fruitful discussions followed, in which the two sides identified the key fields in which the research and documentation side of this project would provide the most added value and tailored a list of complementary activities, such as expert meetings and training courses. Apart from the merits of the project itself, there is also the symbolism of the resumption of close cooperation in research between Romania and Iraq, which would provide a base for a future increase in trade, investment and common academic pursuits. For Romania, such a project, with all of its components, represents a cutting edge product with which it can present itself to the world and an opportunity for further development within this field, where it already occupies a significant position.

Introduction

With the retreat of the last contingents of foreign militaries, the development of Iraq enters a new chapter, in which the promises of oil wealth to fuel further economic expansion and human development come alongside a great deal of risks. This transition to modernity and self-sustainability is crucial to the Iraqi people, since it is an opportunity to reduce their economic vulnerability and lay the foundation for their healthy growth and development. In order to promote growth, foreign investment and its own people's confidence in themselves, the Iraqi government has to work towards creating the kind of environment that is conducive to economic expansion and emancipation for its people and its companies. Part of that task is establishing the framework that will serve to identify and counteract the wide variety of threats that can disrupt societal development. To that end, just as it would in every other domain under its purview, the **Iraqi government must create institutions, procedures, strategies and high-tech infrastructure** which, when manned by specialists, would reduce the Iraqi society's exposure to potential losses and disruptions.

Due to high energy prices and Iraq's positive outlook in terms of natural resources, it may be tempting to forget about the one resource Iraq does not have in abundance – time. As the "Arab Spring" has proven, there are many long-standing tensions within the populations of the area with regards to the distribution of energy wealth, and **any government project must have a sense of urgency and provide results as quickly as possible**. This should not be interpreted as an argument in favor of massive transfers of wealth to local authorities or private citizens. True durable development comes from capacity building that enables local, regional and national authorities to conceptualize, develop and implement programs that lead to the emancipation of other valuable Iraqi resources, such as its people.

It is an inescapable fact of modern life that there is an increasingly large number of things that can go bad, but the assimilation of that fact is crucial for Iraq given its special circumstances. Nonetheless, the fact that it is now beginning **to build its early warning capacities, risk governance and critical infrastructure protection systems is to its advantage**, since it has the opportunity to implement the latest mechanisms and philosophies, while countries with already established and extensive systems find it hard to evolve to face the threats of the new millennium.

A very good analogy can be found in the world of computing. A computer has many components and we can associate some with the government, others with civil society, with infrastructure, and with the private sector. In the Iraqi case, the individual component analogy is apt because the greatest investors in Iraq are the large energy companies, and they provide the impetus for initial economic growth and investment. But the components cannot act alone, they need machine code to be able to work in unison and perform their tasks. This involves having a developed legislation, as programming language, and a set of institutions, bureaucracies, courts, procedures and a political mechanism as the operating system itself. Without it, the computer is useless. In the absence of pertinent and helpful state involvement, economic ventures become riskier, costlier and more uncertain. Individual components may act out alone – companies may build their own schools, their own security, their own roads and power plants, their own port facilities so that they may function, but their productivity and efficiency is nowhere near their potential.

That is why, without exception, **the rest of the world has come to rely on the state to provide the basic infrastructure and stable environment** that lets companies focus on what they're good at and enrich the whole of society.

In the special circumstances of Iraq, the "**stabilization of instability**" becomes even more important, as it struggles to build and develop from the ground up. As it develops, all infrastructure becomes critical, not just oil and gas pipelines – there is a transportation infrastructure (roads and railroads), educational infrastructure, a healthcare infrastructure; all of it must be built and safeguarded against increasingly challenging and diverse threats. **Infrastructure may be tangible or intangible, but all of it is important**. There is also a fiscal infrastructure which provides the government with legitimate and transparent revenues, as well as economic development information. Finally, there is even a social transfer infrastructure, which sees money go towards public and social services to enable the economic emancipation of the population, which, alongside education, would lead to the growth of a modern and diverse developing economy. Without such development, even if the large companies thrive and the government becomes flush with energy money, Iraq can find itself trapped in the middle-income, resource rich, high inequality trap. As seen in recent events in the area, a population with no stake in their society is a hotbed of unrest that is only quelled by government hand-outs, which are in turn dependent on volatile energy prices, an untenable and risky position.

Even without such tensions, the **unique characteristics of the Iraqi security environment call for an innovative and modern approach** towards sustainable development and critical infrastructure protection capabilities. The Iraqi leadership needs to be informed, it needs to have the mechanisms and tools for decision making as well as those pertaining to the implementation of those decisions. Finally, it needs to be able to measure the results in a meaningful way and use that information to predict future issues. Without this, even if nothing catastrophic were ever to happen, Iraqi economic development would be at risk from uncertainty and lack of confidence in its stability.

The following proposal is an outline for a comprehensive, flexible and entirely customizable approach to satisfying those very needs and giving the Iraqi people the tools to effectively guide their development and manage a wide range of risks. The **ultimate goal of this project would be to design and create the kind of stable, predictable environment in which crises are swiftly dealt with, with minimum disruption and economic losses**. The purpose is the continued betterment of Iraq and, as Iraqi economic emancipation continues, the importance of the capabilities this project aims to create can only increase, since the more people have, the more they stand to lose. In this respect, the initial investment into the accumulation of organizational capacity will pay handsome dividends and should be regarded, alongside fixed capital accumulation, technological improvement and human resources development, as one of the pillars of a vision for a prosperous and stable future Iraq.

Critical Infrastructure Protection Strategy for Iraq and Drafting of Legislation

An important component of the project proposal is the contribution to the elaboration of the basic documents on which the **Iraqi government will base its efforts and philosophy for critical infrastructure protection, risk governance and crisis response**. These docu-

Iraq - The Resilient Power

ments embody not only the applicable international experience in the realm of security, but also a unique Iraqi perspective on such matters. They will also ensure future relevance of these strategies and visions, as they will be drafted in accordance with the vision that Iraqi citizens have of how their society will evolve and their own perception of their strengths and weaknesses.

Strategic thinking is essential to all countries, especially those who, like Iraq, are in a process of modernization and democratization. Despite its importance, many countries would treat this important document as a "to do" list and not an overarching vision of their security environment, their preparedness or their roadmap to the future.

A new area of security with great potential for Iraq is related to the protection and development of critical infrastructures in the widest possible sense, meaning not only pipelines and roads, but also cyber infrastructure, health, crisis response and the provision of basic necessities. For this, a **Critical Infrastructure Protection Strategy for Iraq** shall be elaborated, with the latest in scientific advances in the field of technical and security studies of critical infrastructures, including the nascent field of **infranomics** – the interplay between a system of critical infrastructures and engineering, economic, political and social sciences, considering the inter-relationships among infrastructures and stakeholders. The goal of infranomics is to support decision making in view of achieving a set of goals, at multiple levels. The next generation of Iraqi infrastructure will be built on top of the existing one, leading to a compounding of complexity, as the interactions of a multiplicity of actors lead to constant evolution of this system-of-systems. As such, a multi-disciplinarian approach is required to perform adequate analysis and decision-making and infranomics has the potential to group all needed knowledge. Moreover, this Critical Infrastructure Protection Strategy for Iraq would implement novel management concepts, such as "agile security". Derived from the field of project management, especially that of software, **"agile security" stresses the benefits that can be derived from a flexible security framework and apparatus**. "Agile security" uses expert human resources to ensure constant incremental improvements to the security capabilities based on responsiveness to changes in circumstances or in goals.

The resulting Strategy for Critical Infrastructure Protection will serve as a roadmap and reference point for all Iraqi efforts in this field. It will point out vulnerabilities in Iraqi infrastructures, prioritizes them and gives clear indications regarding the manner in which they will be resolved. It will also represent a valuable and organic addition to the established documents of strategic thinking, such as the National Development Plan for Years 2010-2014. Its emphasis on maintaining quality of life and business continuity is even more important, as disruptions cause heavier losses the more developed a society is. **In the end, Iraqi society will only be as prosperous, efficient and secure as its infrastructure will allow.**

The close cooperation between foreign experts and their Iraqi counterparts will not only lead to the creation of pertinent and high quality strategies, procedures and other documents, but will also **foster a transfer of know-how** which will subsequently allow the institutions put in place through this project to provide the intellectual backbone for future Iraqi security philosophy.

The next phase in establishing the framework for security and risk resilience is to insert some of the basic precepts into new legislative projects. International experts would work closely with Iraqi counterparts and stakeholders to create drafts of laws pertaining to adequate responses to emergency situations, the organization of the necessary institutions and the provision of continued support for the protection of critical infrastructures and recognition of their immense importance as the foundation for future Iraqi prosperity. These drafts would then be submitted to the Iraqi legislative body for debate and fine-tuning, with the purpose of, eventually, being adopted and provide the legislative basis for future Iraqi efforts in the field.

Institution building

While strategies and legislation eventually become outdated and lose their relevance, a comprehensive approach to critical security capacity building calls for the establishment of an institutional framework to support the goals of such an initiative. The first and obvious roles of these institutions would be to allow the Iraqi government to train its own specialists in the field and **allow continuity of security expertise** without the need for large outside input.

A first example would be the setting up of an **Advisory Council on Critical Infrastructure Protection to the NSA**, with a mandate to analyze the way in which Iraq develops and expends its wealth, be it human, mineral or energetic and make specific recommendations with regards to threats and new developments in the field. This overview would lead to a better implementation of the precepts of the applicable national strategies, as opposed to the inefficiencies which arise when the control functions are too compartmentalized. The Advisory Council would be a focus for the best in Iraqi Security expertize, trained abroad or at home, and would consist, primarily, of security experts and members of Academia, acting as the first resort for information on critical infrastructures.

By establishing **Critical Infrastructure Protection** officers, reserve cadres and even departments in central administration, local administration, state companies, private companies and even universities, internal training could take place, as well as development of indigenous manuals and teaching materials and, in time, original research and innovation in the field of security. Moreover, as is accepted practice in many other countries, a professional **Association for the Protection of Critical Services and Infrastructures** could be formed that would enable periodic testing, the dispersion of new information and the promotion of good practices and professionalism in what is still a young field of activity in the rest of the world. The established entities could not only provide training, but also certification, allowing for the imposition of demanding standards in the field, which is a critical way of reducing uncertainty in the competence and skills of the members. Licensing and certification are critical to all modern governments, and it will give the Iraqi government a way to gauge the quality of its experts and the result

of its investment, as well as promoting the establishment of a professional class of infrastructure security experts, embedded in central and local government, as well as critical companies.

Another important function of institutions would be that of research, enabling the Iraqi security establishment to develop high quality studies and innovations on its own. Given the threats that face Iraq, it is a fertile ground for research and the institute would be the first step towards developing a complex, modern, and thoroughly **Iraqi school of thought on the matter of critical infrastructure protection**. It would also be the future source for pertinent information for the Iraqi government, compiling and sharing know-how with other such institutions from all over the world. By establishing a Virtual Library for Critical Infrastructure Protection, it could maintain a wealth of knowledge on the matter and create fast transfer networks. This means that, within a short time-span, total synchronization with libraries from the US, Europe and Asia would be achieved. This academic base, along with its own research arm, would represent the foundation for the initiation of all new Iraqi security initiatives.

Embedding knowledge, creating experts

As mentioned before, the proper development of human capital is a key issue for our vision of Iraqi security and prosperity. The transfer of knowledge and core competences to our Iraqi counterparts is crucial to the success of this project, as the complexities of today's security environment calls for a **multi-disciplinarian training, creative problem solving and a great deal of lateral thinking**. With this in mind, one of the goals of this project will be to equip the Iraqi people with a class of security experts who will be able to make good use of the instruments at their disposal to safeguard Iraq's continued development.

The training programs and continued assistance initiative would not only offer a theoretical basis for the Iraqi experts, but would also expose them to actual working security systems, the kind they will be asked to design and create in Iraq.

Therefore, the purpose is not just one of professional education, but also of **embedding knowledge** within the Iraqi security establishment which will limit future dependence on outside training. This role of multiplication, with the "**train the trainers**" concept at its core, gives the project great added value, that will be felt for years to come, in contrast with classic training programs, which engender a dependence on continued access to the original educator.

Ultimately, the purpose of this part of the proposal, as well as any other training program that the project would require, is **to create a new class of elites**, to complement the existing elites in Iraq, the ones who assumed the responsibility of transition and modernization. It is in keeping with Iraq's new phase of transition and momentous transformation that a group of specialists in their fields should be created to support the further development of Iraqi society and afford it the same **level of resilience and robustness** that any modern state offers its people. The reform of the security sector would contribute to the efficiency of the security systems being put in place, as well as continuing the top-down modernization that will lead Iraq on the path towards growth, new standards of living and stability.

This is in line with the entire vision of critical infrastructure protection in Iraq – to create not only the function and the mechanisms, but also the capacity for a self-perpetuating base of

Iraq - The Resilient Power

knowledge that would become a **permanent asset to a professional Iraqi security establishment**.

Decision rooms (demonstrative versions)

Critical Infrastructure Protection relies heavily on **Emergency and Crisis Management** as the tool with which business continuity and quality of life can be maintained in the event of a risk materializing. An adequate safeguard against the myriad threats that can impact human activity requires a proactive authority to identify these threats, to gather extensive data on them, to formulate an adequate response and, finally, to implement it. There is no avoiding the fact that this lengthy chain of response entails its own risks – information may be lost or distorted, it may be misinterpreted, the wrong decisions may be taken or the implementation may suffer at every step of the process. This has been a serious problem in any day and age, but the growing complexity of modern state development has meant that the general and specific threats working against it multiply and evolve on a daily basis. This ecosystem of predators generates staggering amounts of information, and the trend is that of exponential growth. In a simpler past, the competent authorities would compartmentalize these processes and divide them into discreet threats for easier comprehension and response, but this lead to inefficiency, as the relevance of a piece of information cannot be decided in the absence of a general overview. Moreover, **risks today are interconnected**, and prone to cascading, even while the relevant authorities remain oblivious to warning signs that happen beyond their limited domain. For instance, inequality may breed resentment, which boils over into agitation, which may paralyze social services or result in intentional economic disruption (cyber-attacks are one very accessible avenue). This leads to economic losses, a lowering of trust in the state and the economy and a chilling effect on future economic growth.

While the tools for gathering information and dispensing an adequate response have improved greatly, the organizational framework has not kept pace and is more of a hindrance in proper threat and crisis management. **That is why a fundamental redesign of the framework around the capabilities of the new tools is vital**. Iraq has the enviable opportunity of leaping ahead of other states by directly applying the latest concepts and ideas at the national level, while other countries are hobbled by bureaucratic rigidity and traditionalism.

The Decision Rooms Demo concept is an integrated platform based on the latest technical advances in simulation, supervision and data mining. It streamlines the collection of relevant data and allows the rapid digestion of huge amounts of information of a technical, financial and human nature. **The leadership may run different scenarios to predict possible outcomes and, based on this information with substantial added-value, can make an informed solution**. They can then track its implementation, intervene quickly to fix any shortcomings and competently analyses the results and derive valuable experience from it. Above all, the flexibility and centralized nature of the system is what matters in an increasingly complex and challenging security environment.

Of course, the leadership does not have to wait for the actual crisis to take shape. Decision Rooms are also an instrument for improving overall preparedness, by running highly diverse scenarios with great realism, enabling the users to identify areas of heightened risk and plan accordingly. As such, the Decision Room becomes an **invaluable instrument for policy formulation and decision making**.

The concept is not just a collection of hardware and software. Integral to the concept and design of this "**system of systems**" is the human component, which will be developed with training and assistance to create the level of expertise necessary to take full advantage of what the system has to offer. In connection with the institutional framework mentioned in an earlier part of this proposal, the capabilities of the war room as a **nexus of Iraqi security efforts** allow for the creation of new tools with which to gauge the Iraqi security environment. For instance, a **security index** may be calculated on a regular basis and used as a measure of success or a starting point for system reform. A vulnerability index of Iraq could be used to identify trouble spots and have preventive and preemptive measures in place. While the impact of war room operations has already been detailed, the availability of vast amounts of **data and mining** capabilities to generate such relevant informational products is a boon for the research arm of the Iraqi security community, allowing them to think and analyze in the long term, or develop new tools. For instance, it would be possible to create a weighted perception of risk within the security community itself, by gauging what every agent thinks about every other agent's domain and noticing the differential between self-described and outwardly measured vulnerability. This indicator could be an early warning for mass biases in the security community which can be very dangerous, as actual crises have shown.

By **using Decision Rooms in conjunction with a developed cadre of experts**, leaders and officers, the requirements of "agile security" can be met. The resulting adaptability to changes in the security environment or the expressed goals of the stakeholders becomes a powerful advantage in the maintenance of relevant security capabilities, both now and in the future.

The system is even more relevant to the Iraqi people – as evidenced by the example of many other dynamic economies, **cities are the drivers for all growth**. They are where companies base themselves, where the greatest number of jobs is created, where the best services and products are found, where universities innovate and develop human potential. They are a magnet for rural populations and outside investors and provide the most return on investment in infrastructure and public services. As such, they are the most vulnerable to major and minor disruptions. An example of a Decision Room is the City Security and Resilience Room (SERES) Demo, which focuses on urban security issues.

SERES is predicated on **ensuring continuity of life and business even through the most severe events**, as this continuity offers the assurances that investors and economic agents need to develop. As such, SERES tracks and plans for an exhaustive list of city vulnerabilities, setting in place a system of identifying and coping with risks to the critical infrastructure on which a city depends. The focus is on hard infrastructure components, their protection and improvement, investment prioritization and impact assessment. Factors such as traffic and transport management, natural hazards, major disruptions such as blackouts, emergency services, water, food security, environmental security and waste management, terrorist and organized crime threats, population shift phenomena, large scale social unrest, essential supply services and emergency and response services are important in assessing, predicting and achieving the improvement in the quality of life in cities. An even greater attention is paid to vulnerabilities to cyber-attacks which have the potential to cripple an entire country and have become more and more common, potent, disruptive and easy to perform.

As a concept of smart resource overview and management, security and critical infrastructure protection, Decision Rooms, coupled with the implementation of "agile security", provide the necessary instruments with the latest advances for only a **fraction of the costs** associated with classic systems and with a tighter focus on ensuring prevention of crises, control over them and limiting their damage. The technical solutions on which Decision Rooms are predicated (such as electronic visualization) as well as the solutions relating to management and governance (including "agile security"), may be extended to other branches of government, lowering costs and waste associated with inefficient communication.

Finally, Decision Rooms themselves are scalable. The concept works just as well when applied to a subsection of what the original concept was meant to accommodate. One variant is to restrict the variety of factors under its supervision, while enlarging the geographic area of control. Such a concept, in the realm of energy, is called the Energy Security Decision Room and it is a specialized product aimed at governments and energy companies. It allows rapid identification of issues, coordination of repair efforts, control of energy distribution along its grid, maximizing efficiency and minimizing losses. In keeping with all Decision Room variants, **its main functions are still to train, simulate and command**.

These examples of security applications which are intensive in technology and expertise provide a vision for the future of a modern society which, conscious of its vulnerability and security environment, chooses to adequately safeguard itself. The high added value of these investments make them worthwhile, as they are a stepping stone towards creating a stable environment that engenders growth, confidence and human development.

Conclusions

The proposal outlined is based on **an integral approach towards the idea of security**. It builds on the notable work done before it, such as Iraq National Security Strategy 2007-2010, National Development Strategy 2005-2007, UN Iraq Assistance Strategy 2008-2010, National Development Plan for the Years 2010-2014 and UN Development Assistance Framework for Iraq 2011-2014 and others. As Iraq starts living up to its potential, numerous obstacles will need to be overcome in a period of crisis and under time pressure or they will keep it from reaching that potential, or its citizens from enjoying its fruits. This holistic approach is predicated on a simple thought experiment – if you were to find the greatest risk facing Iraq, for instance a resurgence of violence, and eliminate it, you would be left with another great risk, and another and so on. By the time the list of threats has been shortened, one realizes that a list only exists as a snapshot of a moment in time, and new threats emerge daily, some of a new type, and some of a new origin. To deal with them, by "**thinking the unthinkable**", a society needs to become resilient, not in the sense of unwieldy and inflexible, but well organized, well conceptualized and, above all, aware of what it is facing. It needs to have the foresight to maximize prevention and the strength to resist the inevitable "**black swan**" event and "**feral futures**" that risk derailing its advancement. It should shrug off such incidents with minimal losses and disruptions, ensuring a continuity of normal life that belies the increasingly complex and threatening security environment in which the Iraqi citizens live.

The vulnerability to existing and future threats can be addressed through the development, in parallel, of key pillars of security – writing and implementing strategy, risk and resilience governance, the development of an institutional framework for the production and transmission of knowledge and the training of a class of experts in the nascent field of critical infrastructure protection through the transfer of know-how. The pinnacle of this program is the transfer of expertise from "war gaming" to "serious gaming", resulting in the "war room" concept, which integrates the latest in technology with an organizational structure that makes data mining, fast decision making and accurate implementation possible.

The project has, as a defining characteristic, the adaptability to the expressed needs of the Iraqi authorities. It is capable of scaling with the resources devoted to it, but, at every turn, it provides good value and long term viability for Iraq. By using infranomics, a new multi-disciplinarian concept that focuses on "systems of systems", and agile security, which stresses adaptability and responsiveness, **a new vision of Iraq emerges**, one where human potential meets human risks, and a web of infrastructure dependence leads to greater efficiencies and development. **CIP**

A first draft of this article was first published in the "GeoPolitica" Romanian magazine. The material was the result of research undertaken by members of the international team of the EURISC Foundation, with the invaluable cooperation of the Iraqi Embassy in Bucharest.

Alexandru Georgescu M.Sc.
Research Fellow, EURISC Foundation
Editor of International Section, "Economistul" Weekly Magazine

Specialization:
International Business Relations, Academy of Economic Studies, Bucharest (2009)
Master in Geopolitics and International Relations, Academy of Economic Studies, Bucharest (2011)

Interests and Activity: critical infrastructure protection, non military risks, space security, international relations, international organizations

The Albanian Experience in Critical Infrastructure Protection

by Dr. Arian Starova

Despite the overall progress during the past twenty years, Albania is still a country with a small economy and, of course it has a modest critical infrastructure as compared to other developed countries. What might be called critical infrastructure in Albania comprises the energy resources like numerous small and big hydropower plants and the corresponding interconnection electric grid, oil resources and refineries, medical service structures allover the country, road infrastructure, water resources and pipelines, oil and gas pipelines, banking and finance services, food supply services, cyber connection networks, as well as other services whose damage might upset the normal life of the society.

In the critical infrastructure area, the electricity production based on hydropower represents about 90 percent of the overall electricity production. Albania is now considering the possibility of creating a large number of new hydropower plants, given its enormous potential of hydropower resources, but also the renovation of some existent power plants. A new development which is expected to add to the existing critical infra-

structure of Albania is the recent agreement for the construction of the Trans Adriatic Pipeline (TAP) coming from Azerbaijan and going through Turkey, Greece and Albania across the Adriatic Sea into Italy. Other energy resources are being considered such as the wind-power, gas and solar power and related projects are being studied.

Critical infrastructure of Albania and trends of its further development

During the last ten years, an outstanding progress has also been achieved in the area of information technology. Internet connection service has tremendously widespread in the recent years in the government, many private businesses, services and schools. After the Albanian government turned the information technology into a priority of the National Strategy for Development and established the National Agency for Information Society, this progress has further accelerated. Today in Albania there are electronic business registration, electronic National Civil Register, electronic taxes system, electronic procurement and tender procedures, electronic licensing procedures, 550 post offices offering free Internet access throughout the country, automation of many government databases, biometric passports, identity cards, electronic judiciary procedures, electronic management of the borders, etc. Also in the defense sector, the digitalization process is fast advancing in the field of guarding, protection and security, management of human resources, surveillance of air and maritime space, etc. Since the years 2010, the Albanian Ministry of Defence established the Inter-institutional Maritime Operational Center (IMOC) which offers airspace and maritime surveillance and bears responsibility in time of civil emergencies or with regard to illegal activities or trafficking.

Albania is ranked 85 among 159 countries according to Information and Communication Technology (ICT) Development Index (IDI) and 85 among 179 countries according to e-Government Development Index (e-GDI) for the year 2010 according to the **United Nations** International Telecommunication Union (ITU). During the period 2006-2011, Albania ranked second among ten world's most improved countries in the Networked readiness Index (NRI) according to the World Economic Forum.

Some of the on-going ICT projects are the construction of various digitalized systems in the cadastre, health service, archives, Parliament, social insurance, judiciary, Government, government data centre, government backup centre, etc.

There is also an institutional structure for the information and communication technology in Albania, such as the Ministry for Innovation and ICT, National Agency for Information Society, National Authority on Electronic Signature, Agency on Research and Innovation Technology, Electronic and Postal Communication Authority, National Council on Radio Television.

Further investments in Information and Communication Technology will naturally expand and also interconnect the components of the critical infrastructure in Albania which also naturally and step by step will increasingly raise its vulnerability and place its protection among the highest priorities.

Protection of the critical infrastructure

Like in all the other countries, there always was a certain protection for the critical infrastructure in Albania carried out by different government institutions. However, along with the development of the critical infrastructure and the diversification of the security environment, a need for higher attention to the protection and security of this specific infrastructure also emerged. This became more important for Albania after its accession to NATO in view of its new allied responsibilities. NATO's operability and success as an Alliance in support of peace and security is so much relying on secure energy systems and cyberspace of its member countries.

Not only various terrorist attacks could be thought about and ranked among the threats to the critical infrastructure, but also various natural events linked with disasters resulting from various environment and climate changes. The very awareness of critical infrastructure protection is so closely linked as well with the present increasing constraints of the global energy resources and growing vulnerability of the global cyber space and energy infrastructure. Additionally, the substantial and fast expansion of cyber space in Albania which is resulting in an increasingly interconnection between private and state businesses and services constitutes another essential reason for that protection. Due to some natural disasters and minor cyber-attacks, Albania has also gathered some modest experience in the area of critical infrastructure protection.

The growing state awareness with regard to the critical infrastructure led to the taking of a number of measures such as the approval by the Parliament of specific laws and the establishment of government structures to more specifically deal with the critical infrastructure protection, such as the following laws, "On Electronic Communications", "On Digital Signature", "On Cyber Crime", "On the Protection of Personal Data", "On Electronic Commerce", "On Electronic

The Albanian Experience in Critical Infrastructure Protection

Document", etc. Albania was made party of and ratified in the year 2002 the "Convention on Cyber-crime" and, later in the year 2004, it ratified the "Additional Protocol to the Convention on Cyber-crime". In compliance with this Convention, there were made also amendments to the "Criminal Code "and to the "Code of Criminal Procedure".

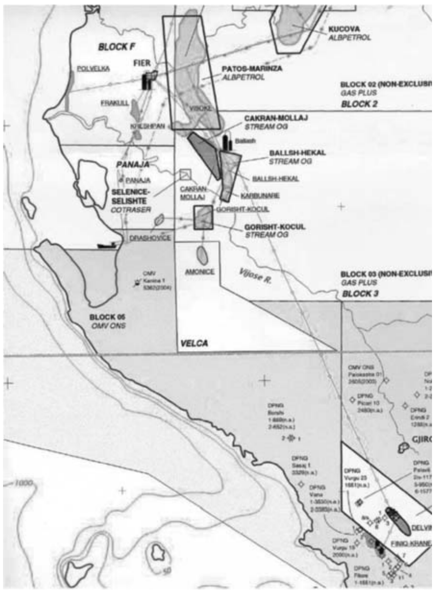
Albania has approved a Strategy for Information Society (2008-2013) adopted by the Government based on the "E-Europe Action Plan" which contains measures for the creation of specialized police structures for cyber-crime, for increasing the awareness of various interest groups like students, families, financial institutions, IT associations, for the development and implementation of Codes of Ethics that encourage cooperation between various structures, etc.

Among the structures that have been established in Albania for the protection of critical infrastructure, it could be mentioned, the Unit against Cyber-crime by the State Police, Computer Emergency Response Team (CERT), "National Cybersecurity Agency" (ALCITR) under the authority of the Prime Minister, "Government Data Centre" for hosting the government official systems, cyber-defense capability in the Ministry of Defense, etc. These agencies play a significant role for cyber defense by developing procedures and regulations related to the protection of cyber-security systems such as the regulations on the use of the Internet and electronic mail, official web sites, requirements for servers, regulations for the activity of telecommunication operators, mass media, etc.

Recently, USAID launched a Cyber-Security Program in Albania, an initiative that helped to build governmental capacities for the prevention and response to cyber-security incidents.

On some infrastructure protection concerns of the future

Considering the current level of development of the Albanian critical infrastructure and its protection and some expected trends of the future development, the following topics could be necessary.



As is expected a fast grow of the energy sector and its respective infrastructure in Albania, it is very necessary to develop a document of "National Strategy for Energy Security" which foresees establishing of a "National Agency for Energy Security" and the enactment of specific laws. The Albanian plans for the gasification of the country, as a result of the construction of TAP, make this issue more imperative.

Albania must consider the cyber-space as a national asset which deserves a growing attention and protection as a one undivided whole. Hence, special investments must be made for improving the technology of its protection and counter-response, improvement of its operational structures, training of experts, compilation and improvement of related laws and procedures, etc. In the same spirit, a close partnership between the Government and the private enterprises is very important in cyber-protection.

Albania must extend the cooperation beyond the borders of its country what relies in the very essence of the cyber-space. Special focus should be placed upon the cooperation in its region and with the specialized international organizations.

Considering the long-term nature of the scarcity of energy resources and in a more general framework of international cooperation, most of the countries are increasingly viewing upon it as clear issue of energy security. It is a problem of discovery of new energy resources. Hence, Albania must coordinate its research efforts and the existing energy resources not only for energy supplies, but also for building a common clear road map for the diversification of the energy resources, possibly in view of a common energy network including all European and which is complementary and inter-dependent for all. In this general respect, Albania should establish a specific Ministry of Energy Resources. The needs of Albania for energy will be for sure increasing alongside with its ambitions to turn itself into a developed country.

Energy security and cyber protection, eventually, are new issues for Albania. This is the main reason why there is a serious need in Albania for further developing awareness among various groups of interests and expert discussions on these topics. **CIP**

Dr. Arian Starova
Deputy Minister of Defence at the Ministry of Defence of the Republic of Albania

Specialization:
Law degree and PhD in Philosophy from the University of Tirana

Interests and Activity: From 2001 until his current posting, Arian Starova was a member of the Albanian Parliament but held several other senior positions during this period. From July 2002, he served as President of the Atlantic Council of Albania, and in 2005 was appointed President of the Liberal Democratic Party. From 2005 until 2009, Arian Starova served both as Vice President of the Atlantic Treaty Association (ATA) and Secretary of the Parliamentary Commission on Foreign Affairs. Within the last eight years, Starova has held memberships on the Advisory Board of the Szeged Center for Security Policy (Hungary), the European Strategy Forum (Ponte de Lima, Portugal), and as a member of the Board of Trustees of the Balkan Mosaic Foundation. He has also served previously as Minister of Foreign Affairs of Albania as well as several different senior faculty positions at the Faculty of Political Sciences of the University of Tirana.

Italian Association of Critical Infrastructures Experts – AIIC

The non-profit scientific association AIIC (Italian Association of Experts on Critical Infrastructures) was born to create and sustain an interdisciplinary culture to the developing of strategies, methodologies and technologies able to adequately govern the critical infrastructures, especially in crisis scenarios resulting from both natural catastrophes or anthropic malicious behavior.

The AIIC aims at exchanging experiences and knowledge related to the critical infrastructures to create an interdisciplinary and inter-sectoral shared approach among experts of different fields.

To this purpose it affiliates academics, researchers, and experts of the different critical infrastructures. The concert of the various perspectives allows a global, deeper vision of the problem and it enables the Association to support public Institutions and private Enterprises in the governance of this complex "system of systems". The main support provided by AIIC is throughout dissemination of knowledge among their affiliated and the organization of special events covering different aspects of CI(I)P.

Along with its dissemination activity, the AIIC patronizes or is co-sponsor of some international events.

AIIC constitute in Italy a focal point for all CI(I)P expertise and a valid entry point to these expertise for the rest of the world.

For any further information, please visit:

www.infrastrutturecritiche.it

ARPIC - AIIC signing protocol

Romanian Association for the Protection of Critical Infrastructures and Related Services – ARPIC

Romanian Special Register of Association
Registration Number: 64/2011
Tax Identification Number / Unique
Registration Code: 29012550 / 2011
Bank Account:
RO91RZBR0000060015802554, Raiffeisen
Bank, S 1, Bucharest, Romania

As Non-Governmental, with non patrimonial status, autonomous and apolitical organization, the aim of The Romanian Association for the Protection of Critical Infrastructures and Related Services – ARPIC, is to bring together specialists from different fields, so as to contribute to the understanding and harmonization of specific norms and operating procedures on the protection of critical infrastructures and related services, in Romania, as well as at regional, European and international levels.

The above mentioned main purpose will be achieved through the member`s joint effort and will consist in:

- Promotion of contacts and cooperation between professional organizations and specialists with activities in the field of interest of the Association;
- Cooperation between the public sector, business community and the civil society representatives in the critical infrastructures protection management;
- Promotion of national experience and dissemination of valuable international experience regarding CIP and CIIP management;
- Participation with specialists in scientific and research projects with national and European partners;
- Developing and organizing educational programs, training and consultancy in the field of risk management and vulnerabilities, prevention, safety, physical and information security, resilience and recovery of national and European critical infrastructures;
- Publishing of a scientific character, of training and information papers in the field of critical infrastructure protection;
- Formation and consolidation of required preparedness level of the specialists, managers and liaison officers for the protection of critical infrastructures
- Editing periodically “The European Journal of Critical Services and Infrastructure Protection”.

Contact Address: 101, Dr. Iacob Felix Str., Bl.19, Entrance A, Ap. 33, District 1,
Post Code 011036, PO Box 2-101, Bucharest, Romania
Phone/Fax: 0040 212122102; E-mail: office@arpic.org

www.arpic.org

ARPIC Participacion to: The First NATO, EU and Shanghai Cooperation Organization Think Tank Meeting

On September 24-25, 2013, in Bucharest, the EURISC Foundation, in partnership with the German Marshall Fund's Bucharest office, organized, the first meeting of international think tanks from NATO, EU and Shanghai Cooperation Organization Member States. Romanian and international experts were brought together to discuss various issues under this novel format.

The choice of Bucharest as host for this world premiere event reflect Romania's strategic position as a "bridge between West and East", further underlined by the new geopolitical and geostrategic reality of the Black Sea as a "border area" between NATO, EU and the SCO.

One of the starting points of the event is the insufficient use of the think tanks' significant endowments in the new security environment, specifically their analysis and security policy formulation capacities. Another is the dialogue deficit between the three great organizations, especially NATO and the SCO. Therefore, the event organized at the National Military Circle in Bucharest aimed to rectify some of these issues through a focus on exploring new opportunities for dialogue and cooperation. A wide variety of issues were touched upon, ranging from fighting terrorism and transnational organized crime, to the security of access to resources such as energy and water, the protection of critical infrastructures and the security environment in Afghanistan and its wider region after 2014.

The first NATO, EU and SCO Think Tank Meeting should be viewed as a starting point in the process of deepening the cooperation between them, as well as providing a basis for partnerships between state and non-state actors.

As was evidenced during the event, there is ample opportunity for cooperation between NATO and the SCO, which is undergoing significant institutional construction efforts. For instance, the two organizations may "shake hands over the Pacific" for the purpose of combating piracy and for securing the flow of resources, energy and products through areas which are, already, the most heavily used trade routes in the world.

On its second day, the event took the form of a reflection group, hosted by SELEC, the Southeast European Law Enforcement Center, which, since its founding, in 2001, has dedicated itself to fighting trans-border crime phenomena in South-Eastern Europe.

The participating experts originated in ten countries, not only from Europe, the United States, China, but also from Iran and Afghanistan. Among the Romanian research institutions accounted for during the event were EURISC-IRSI (the Romanian Institute for International Studies), the GMF (German Marshall Fund's Bucharest office), ISPAIM (the Institute for Political Sciences in Defense and Military History), the Conflict Analysis and Early Warning Center, the European Institute of Romania, the Black Sea Foundation and others. The international institutions represented were CEPS (Center for European Policy Studies), ECFR (European Council for Foreign Relations), SWP (Stiftung Wissenschaft und Politik), EURODEFENSE, the Center for Understanding Change (Washington), Old Dominion University (Norfolk, Virginia, USA) and George Washington University (USA), CICIR (the China Institutes for Contemporary International Relations in Beijing), the SCO Studies Center of the Shanghai Academy for Social Sciences, RIAC (the Russian Council on International Relations in Moscow), Far Eastern Federal University (Vladivostok, Russian Federation), IPIS (the Institute for Political and International Studies, in Tehran), SAM (the Strategic Studies Center under the Presidency of the Republic of Azerbaijan) and CSEES (the South Eastern European Studies Center in Sofia, Bulgaria).

The event also benefitted from the presence of the Ambassador of the Russian Federation to Romania, H.E. Oleg Malginov, of the US Chargé d'Affaires, Duane Butcher, of the Ambassador of the Islamic Republic of Iran, H.E. Bahador Aminian Jazi, as well as other members of the Diplomatic Corps in Bucharest. Among the representatives of the Romanian authorities taking part on the event were Valeriu Zgonea, President of the Chamber of Deputies, Iulian Fota, National Security Adviser to the President, Mihai Dobre and Radu Podgoreanu, Secretaries of State in the Ministry of Foreign Affairs, Sorin Encuțescu, State Councilor and Adviser to the Prime Minister on National Security and the Coordination of the Protection of Critical Infrastructures. The event also had, as a special guest, Ambassador Viorel Isticioaia-Budura, Director of the Asia-Pacific Department within the European External Action Service (the European Commission). **CIP**

Security Liaison Officer
EU Project Ref. No. : HOME/2012/CIPS/AG/4000003747
With the support of the
"Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme"
European Commission – Directorate – General Home Affairs

What is the Security Liaison Officer Project?

Within Critical Infrastructure organizations in the EU community, this question remains an extremely fluid concept. Through identification of the static standards amongst Security Managers who operate within European Critical Infrastructures and subsequently performing gap analysis, thisresearch aims to identify a framework for the Security Liaison Officer (SLO) position as mandated by Article 6 of the EU Directive 2008/114/EC.

The establishment of a common profile for the SLO position will provide a comparable professional standard for Security Managers currently operating within the European Critical Infrastructure (and National Critical Infrastructure) arena.

Specifically, **The Security Liaison Officer Project** aims to identify:

Who is the SLO? Which are his/her competences, rules, background? Which should be his/her position inside the organization?

What roles and responsibilities should the SLO position entail (before, during and after crisis scenarios)?

Should International Standards, certificates and training courses be prerequisites for filling a SLO slot?

Basic Facts
Start date: June 2013; Duration: 12 Months
Co Funder Entity: European Commission (DG HOME/2012/CIPS/AG/4000003747)
Partners:
University Campus Bio-Medico of Rome
Romanian Association for the Protection of Critical Infrastructures and Related Services - ARPIC
Associate Partners:
Italian Association of Critical Infrastructure Experts – AIIC
The Italian Association of Continuity Managers – BCManager
Italian ASIS Division (Chapter 211) of ASIS International – proeminent organization for security professionals
National Company "Transelectrica" S.A. – the Romanian Transmission and System Operator (TSO) which plays a key role in critical infrastructure protection on the energy sector.

For more information, news, results and documents, please visit: **www.slo project.eu**

SECURITY LIAISON OFFICER (SLO)
Identifying a Framework for the Protection of Critical Infrastructures

coperta 3