ANALYTICAL SUPPORT TO CRITICAL INFRASTRUCTURE PROTECTION POLICY AND INVESTMENT DECISION-MAKING

Todor TAGAREV, Venelin GEORGIEV, and Petya IVANOVA

Abstract: Critical infrastructures are complex, interlinked socio-technical systems, with impact often crossing state borders. Their protection involves governments and business organisations, interacting in the application of a broad variety of measures to provide safety and security while investing a considerable amount of public and private resources. This paper examines the challenge of making respective policy and investment decisions transparent, and a sample of methods and tools used to facilitate decision making. It also calls for contributions to a knowledge portal on security and safety of critical infrastructures.

Keywords: CIP, security policy, interdependency, complex adaptive systems, CASoS, EU Directive 114/2008, ECI, CIP Meta-management, decision support, taxonomy, method, tool, knowledge management, knowledge portal.

Introduction

Advanced technologies allow businesses, and modern societies as a whole, to increase their efficiency in delivering goods and services. Transport networks, electrical grids, energy pipelines, and fibre optics connect countries, regions, communities, and individuals. This increasing interconnectedness creates opportunities, while on occasion introducing vulnerabilities. This dual nature of the very high degree of interconnectedness can be understood only when studied with appropriate methods. And the adequate understanding is the basis of making decisions – how to remedy vulnerabilities, what efforts are required to provide reasonable safety and security, where to focus public and private investments, how to manage these investments, and so on.

This paper provides description of the critical infrastructure protection (CIP) problem, with definition of goals and tasks, both from a theoretical perspective and in the practice of the European Union and individual nations. It provides an overall decision-making framework and lists of methods that support decision making. This paper provides evidence that critical infrastructures need to be studied as complex adaptive

systems, with application of appropriate tools while understanding the limitations of the analysis and, in particular, predictions that can be made regarding the consequences of one or another event.

Towards that purpose the following section examines critical infrastructures (CIs) as an object of research and presents possible frameworks for making decisions on their protection. Next, we examine the evolution of the European Union (EU) approach to critical infrastructure protection. The next two sections list main decision making tasks and samples of respective methods and tools for decision support. The concluding section calls for creating a knowledge portal on security and safety of critical infrastructures.

Decision making frameworks

This section looks into the challenge of defining "CIP policy," the nature of critical infrastructures as an object of analysis, requirements to the policy making and strategic management processes, potential decision-making frameworks, and the need to address uncertainty in devising and implementing a CIP policy.

Policy is defined as declaration of the senior executive leadership (e.g. of the EU or a member state) on the adopted course of action, intended to direct and guide future decisions and actions in regard to critical infrastructures. As a minimum, the policy needs to be adequate to the security, social, technological and economic environment, affordable and acceptable to the society. It also has to balance goals, ways, and means, with clear understanding of involved risks.

The basic policy decisions include defining the scope of 'critical infrastructures'; identifying (and informing stakeholders) on threats and hazards; defining capability requirements and priorities; assigning responsibilities; and providing public and/or private financing for CIP. The comprehensive approach to security can provide guidelines in considering CIP measures and capabilities, to cover options aimed at: prevention; protection; monitoring; early warning & detection; reaction; consequence management & recovery; resilience.

In considering possible decision making frameworks, one needs to account for the large number of actors, the increasing proliferation of mutual dependencies and feedback loops, the nonlinear nature of these dependencies and other features typical for complex adaptive systems.[1] It is increasingly understood that CIs are Complex Adaptive Systems of Systems (CASoS) with the characteristic inability to fully explain their behaviour, limitations on predictability, and phenomena of self-organisation.

Thus, the methods and tools used to facilitate decisions have account for these CI features and still provide for transparent decision making. Further, it is necessary to

provide for comprehensive treatment in policy making; assignment of responsibilities at the appropriate level and place; involvement of stakeholders; assessment of alternatives; measurement of results and performance; and adaptation to changing circumstances.

The respective decision making frameworks implement the all-hazards approach. Technically, one can use a *risk management framework* or a framework providing for *selection of a portfolio* of measures and capabilities for critical infrastructure protection. Another recent development involves implementation of adaptive/ dynamic approaches in a *CIP strategic management framework*.

Whichever decision framework is selected, one needs to address uncertainty. Scenario-based planning with design and selection of a set of scenarios—each one describing one or more events with significant negative impact on critical infrastructures—is considered state-of-the-art. To reflect deeper uncertainties our team explores the use of context scenarios, or 'alternative futures,' in a framework of *exploratory foresight*.[2]

The approach of the European Union

In highly interconnected societies, a disruption of critical infrastructures in one state can negatively impact the provision of essential services in other states. Therefore, in the beginning of the new millennium the European Union turned to defining a EU-wide policy and a programme of critical infrastructure protection. Building on the experience of EU and other nations in devising critical infrastructure protection policies, as well as demands for countering terrorist threats,[3] in November 2005 the European Commission adopted the so-called *Green Paper on a European Programme for Critical Infrastructure Protection*.[4] The purpose of this paper was to provide a basis for discussions on the EU CIP policy with a broad number of stakeholders and to solicit feedback on main policy options.

Annex 2 to the Green paper provided an indicative list of sectors that may be considered as potential European critical infrastructure. The list included 11 sectors (with a total of 37 sub-sectors) including:

1. Energy
2. Information and communication technologies (ICT)
3. Water
4. Food
5. Health
6. Financial
7. Public & Legal Order and Safety
8. Civil administration

9. Transport
10. Chemical and nuclear industry
11. Space and Research.

In October 2008 it was proposed to establish a Critical Infrastructure Warning Information Network (CIWIN).[5] The CIWIN would provide EU countries with a secure information, communication and alert system for exchanging CIP related information. Further, it would facilitate cooperation between EU countries through exchange on threats, vulnerabilities and strategies for improving CI protection.

In December 2008 the Council approved Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.[6] It provides a common approach for assessing CIs and sets up a procedure for identifying and designating European critical infrastructures (ECIs), with the purpose of improving them to better protect citizens' needs. The Directive defines 'Critical infrastructure' as

> an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

The Directive also formalises the criteria to be used in assessing criticality, including:

- Casualties criterion (assessed in terms of the potential number of fatalities or injuries)
- Economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects)
- Public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

Compared to the 2005 Green paper, it limits the scope to two sectors, with the following sub-sectors:

- Energy:
  1. Electricity: Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity
  2. Oil: Oil production, refining, treatment, storage and transmission by pipelines
  3. Gas: Gas production, refining, treatment, storage and transmission by pipelines; LNG terminals
- Transport:

4. Road transport
5. Rail transport
6. Air transport
7. Inland waterways transport
8. Ocean and short-sea shipping and ports.

While the current focus is on the implementation of Directive 114 requirements across the European Union, experts continue to discuss the eventual broadening of the scope of CI sectors it covers. Number one candidate for expanding the scope is the ICT infrastructure, including the future internet. Of particular interest is to provide an understanding of the interdependencies among ICT infrastructures and other CI sectors. In our view, any decision to include new sectors of CI would be based on perceptions and readiness of the EU and member states' leadership to commit the necessary political, administrative and financial resources.

Decision making tasks

The implementation of the decision making framework in a transparent manner requires that all stakeholders from public and private organisations have a clear understanding why certain measures have to be implemented. Ideally, the parties involved (e.g., auditors) could also track the decision making logic. Towards that purpose, in an earlier work we developed an integrated decision making framework and a process.[7] On that basis we developed a taxonomy of seven groups of decision making tasks with the respective sub-tasks as follows:

A. Assess and represent threats

- Identify, characterise, and evaluate threats and hazards;
- Describe their realization through plausible scenarios; select a set of scenarios to be used for policy making and planning purposes;
- Represent deeper uncertainty.

B. Assess vulnerabilities

- Identify sectors, sub-sectors and assets of critical infrastructure;
- Assess vulnerability of individual assets;
- Analyse sensitivity.

C. Study and understand interdependencies

- Assess interdependencies among assets, subsystems, and infrastructures;
- Identify interdependencies that would potentially lead to cascading effects.

D. Assess negative impact

- Design criteria and measures;

- Analyse each scenario;
- Select a course of action;
- Define impact per scenario;
- Aggregate impact assessment (accounting for hypotheses of simultaneous realisation of two or more scenarios).

E. Formulate policy for critical infrastructure protection (CIP Policy)

- Decide on the scope of the term "critical infrastructure," accounting for perceptions, readiness to commit, etc.;
- Formulate and decide on goals and objectives;
- Devise a strategy;
- Assign responsibilities;
- Allocate resources.

F. Decide on CIP investments

- Derive capability requirements;
- Explore investment alternatives:
    - Evaluate options;
    - Analyse forms of providing protection measures and capabilities, e.g. applicable forms of public private partnerships;
    - Assess investment project risk;
- Decide on investments.

G. Strategic Management [8]

- Analyse and improve management processes;
- Analyse novel approaches, concepts, and strategies;
- Devise and introduce standards for CI safety and security;
- Provide integrity, transparency, and accountability.

Sample of decision support methods and tools

There are numerous methods and tools that are or could be used in supporting CIP decision making. This section provides just a sample of methods for analytical support of CIP investment decision making, serving to evaluate investment alternatives in terms of economic feasibility, assess investment project risk, and study investment forms. The economic feasibility of investment alternatives cane be assessed using static or dynamic methods. Among the static methods are the method of payback period; method of annual rate of return on capital; method of the number of revolutions of the invested capital; method of relative profit; method of comparing the analytical

profit. Among the dynamic methods are the method of net present value; method of the net future value; method of internal rate of return on invested capital; method of the modified internal rate of return on capital; the cost–benefit method; annuity method; and the method of discounting payback period.

In the analysis of forms of investment, one can distinguish classical forms of public-private partnership (PPP) and forms of CIP Network Management. A selection of traditional PPP forms includes using/maintaining facilities—public property—by private partners; design and construction of public facilities by private partners; financing projects by the public and engagement of a private partner for designing, building and providing use of facilities for a specified period of time; financing and construction of extensions to existing publicly-owned facilities by private partners; construction and use of facilities by the private partner with the subsequent transfer of ownership; temporary privatisation of publicly owned facilities; hiring a private partner to lease or purchase, develop and use facilities, public property.

The introduction of novel forms of CIP Network Management, or CIP Meta-management, requires studies in support of the adoption of regulations allowing private sector companies to join temporarily their efforts with state agencies with security responsibilities, support for the operation of networks, e.g. through consulting, the adoption of appropriate social and economic regulations, the financing of networks via grants, guaranteed loans, concessions, licenses, taxes, insurance, etc.

Conclusion: Towards a CIP knowledge portal

The formulation of CIP policy and its implementation cannot be efficient without relevant analytical support. The respective decisions, however, are very diverse. This paper aimed at providing a framework for discussing decision support requirements and to structure the information on relevant methods and tools.

We have started arranging available information on CIP on the security and defence management portal at www.defencemanagement.org. Recognising that it is not in the powers of a single organisation to maintain an adequate knowledge portal, we invite all interested parties to submit relevant information on methods, tools and accumulated experience.

Notes:

[1] See for example the studies of the U.S. National Infrastructure Simulation and Analysis Center (NISAC) at Sandia National Laboratories and Chloe Griot, "Modelling and simulation for critical infrastructure interdependency assessment: a meta-review for model characterisation," *International Journal of Critical Infrastructures* 6:4 (2010): 363-79.

[2] For further information see the work of the authors within the EU FP7 research project FOCUS, <www.focusproject.eu>.

[3] See Communication from the Commission to the Council and the European Parliament of 20 October 2004: *Preparedness and consequence management in the fight against terrorism*, COM(2004) 701 final, Official Journal C 52, 2 March 2005, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0701:FIN:EN:PDF>; and *Prevention, preparedness and response to terrorist attacks*, COM(2004) 698 final, Official Journal C 14, 20 January 2005, <http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33219_en.htm>.

[4] *Green Paper of 17 November 2005 on a European programme for critical infrastructure protection*, COM(2005) 576 final, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF>.

[5] *Proposal for a Council Decision of 27 October 2008 on a Critical Infrastructure Warning Information Network (CIWIN)*, COM(2008) 676 final, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0676:FIN:EN:PDF>.

[6] *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, 23 December 2008, 75–82, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>.

[7] See Figure 1 and the accompanying deliberations in Todor Tagarev and Nickolay Pavlov, "Planning Measures and Capabilities for Protection of Critical Infrastructures," *Information & Security: An International Journal* 22 (2007): 38-48, <www.procon.bg/?q=node/472>.

[8] Strategic management is defined as aligning and maintaining the balance among goals, strategy, capabilities, and risk in changing environment. See Stephan de Spiegeleire, Paul van Hooft, Chas Culpepper, and René Willems, *Closing the Loop. Towards Strategic Defence Management* (The Hague Centre for Strategic Studies, April 2009); Todor Tagarev, Strategic Defence Management: From Core Processes to Organizational Structures, *IT4Sec Reports* 71 (2010), <www.IT4sec.org/node/2445>.

TODOR TAGAREV, PhD, Associate Professor, is Head of the IT for Security Department and the Centre for Security and Defence Management at the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences. He is a 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. *E-mail*: tagarev@gmail.com.

VENELIN GEORGIEV is Associate Professor at the Centre for Security and Defence Management in the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences. He graduated from the Bulgarian Air Force Academy in 1987 and received a PhD degree in management from the "G.S. Rakovski" Defence and Staff College. His main research interests include defence resource management, defence acquisition and risk management, innovation and investment management, controlling, and economic analysis. *E-mail*: georgiev@defencemanagement.org.

Petya IVANOVA is CEO of Procon Ltd. She led datamining projects of Information Services AD, and served as senior scientist at BiosGroup at the Honeywell Technology Center – Europe and the Institute for Information Theory and Automation of the Czech Academy of Sciences. She has published widely in international journals on bioengineering, soft computing, decision support systems, and scenario-based foresight. *E-mail*: petya@procon.bg.