Critical infrastructure protection at the European level

Bart Smedts[1]

Introduction

We have been forced to admit that there is no such thing as zero risk: the draconian measures implemented in the field of air transport security since 11 September 2001 could not prevent other attack attempts. Since then, the world has had to deal with the terrorist attacks of London, Madrid, Mumbai and Islamabad, to name but a few. Besides, the threat assessment must also take the "internal enemy" into account. Whether attacks or accidents, risk assessment can help determine the scale of the means to be deployed in order to reduce possible risks or to improve the protection plans of existing critical infrastructure. Potential threats can materialise in a very broad spectrum of fields such as proliferation, international terrorism, unequal wealth distribution, the spread of organised crime or pandemics. Furthermore, globalisation puts even more strain on existing threats, with the direct consequences that energy demand, climate change, urbanization, the current economic crisis as well as demographic growth and its socioeconomic consequences worsen. All those potential threats pose a security risk for our critical infrastructures, which are vulnerable to the effects of an attack[2].

[1] Bart Smedts is a research fellow at the Center for Security and Defence Studies (CSDS) of the Royal High Institute for Defence (RHID). The views expressed are only those of the author.

[2] B. Cornelis, *Federal Risk Inventory, Survey and Knowledge building*, SPIRAL, Liège, 2004.

Modelling and methodology

The interdependence of the different sectors adds to the difficulty of the problem. Yet Zimmerman[3] has shown the importance of this interdependence in the framework of securing networks (including information networks). The central question is to know how to best model the risk. Excessive digitization has almost become an obsession: digits are charged with providing a solution to each of our problems but we overlook the fact that they are subject to interpretation and that the obtained results remain just hypotheses. Some have looked for a solution in Farmer's diagram whereas others turned to Nash's equilibrium and game theory in order to optimise their defence strategy. Other analysts got all confused by the disparate use of those various models. Without going into too much detail, it should be however known that to each model corresponds a series of initial hypotheses. This entails constraints in the exploitation of the results to be interpreted. The bases of the definition of a risk can thus help find a solution to develop a useful methodology in order to work out a planning as far as the protection of critical infrastructure is concerned. Yet this is not a sufficient step: the reluctance to invest in corrective measures to prevent incidents is lingering. A reason for this may lie in the illusion that such incidents will not happen again in the short term. Parallel to this, financial considerations in times of financial crisis generally also get the upper hand. The fact is that today, even in the United States, the situation is quite similar to the one prevailing before the 11 September attacks. Despite the creation of new homeland security departments such as the Homeland Security Council (HSC) and the Department of Homeland Security (DHS), the role of various actors in interdepartmental cooperation is not clear yet. The command structure in the case of an incident remains ambiguous.

The situation is not better in Europe: the attempted attack on the Amsterdam-Detroit flight in December 2009 is the perfect illustration of this. A Nigerian known to antiterrorist services managed to board an aircraft and to set off the undetected explosive charge he was wearing. The different security measures of each check were not sufficient to detect the explosive device. The essential factors that could lead to an efficient methodology for risk assessment are lacking. As a consequence, lasting problems could arise at the national level. This is where the higher level, namely the supranational level, can step in. The

[3] R. Zimmerman, "Decision making and the Vulnerability of Interdependent Critical Infrastructure", CREATE Report 04-005, Homeland Security Center, p. 1-4, 2004.

EU could help identify the necessary capacities to counter a particular threat or to implement integrated means in an emergency plan.

A possible methodology includes:

- identifying essential infrastructures that are critical to the smooth functioning of society: determining a catalogue on the basis of established criteria and international definitions. The current list does not meet those requirements. An investigation might for example put new solutions forward to replace obsolete national lists.
- assessing the threat: the proactive identification of the elements of a critical infrastructure (CI) could be integrated in a strategic document which would also take into account the trends to be foreseen in the future. An analysis of the appropriate information and intelligence means is necessary at this stage.
- assessing vulnerability: determining the impact of an incident on a CI, taking into account the sensitivity of existing facilities in order to draw up a list of possible incidents.
- assessing the risk: it should be mentioned here that a catalogue of existing risks can be drawn up *a priori*. Depending on the definitions, this catalogue should comprise the distinction between each of those potential risks with regard to their cause, nature, potential target as well as an estimate of the impact.

Moreover, it should be understood that the various critical fields are interdependent. As such, a single incident can lie at the basis of disruptions in various fields in our society because of cascade effects that are not often taken into account in risk assessment.

EU framework for critical infrastructure protection (CIP)

An attempt to define CI was made at the European level in 2005 through the publication of a Green Paper. In the framework of the European Programme for Critical Infrastructure Protection (EPCIP), 11 sectors with 37 related services were identified to be listed as CI. The proposal for the directive eventually retained 11 sectors and 29 sub-sectors. The directive itself only mentions 2 sectors (energy and transport) and 8 sub-sectors. Moreover, the initial responsibility for CIP remains national. Consequently, a distinction is introduced between national and European CI: the European dimension is considered

when the infrastructure becomes critical for more than one member state of the Union.

Besides those sectors, the EU is aware that the CI can geographically be located outside the EU territory. This highlights the importance of the oil and pipelines supplying the EU: the neighbouring facilities of the EU are essential to supply its economy. The destruction or sabotage of those infrastructures in potentially instable regions could have unprecedented consequences for the European Union. Gas supply cuts from Russia had serious repercussions in Europe. Furthermore, the economic and banking crisis has exposed the interconnection of the various sectors. Cooperation to reach lasting solutions is promoted through sector agreements.

The exchange of rapid information on potential threats and vulnerabilities plays a crucial role. As such, it was evident that a specific network became necessary: this task has been assigned to the CIWIN network[4] (Critical Infrastructure Warning Information Network). This network fulfils two functions. It is first and foremost an electronic forum for information exchange related to CIP. Moreover, it serves as a rapid alert functionality between member states to inform the Commission on common risks and threats. All member states signed a memorandum of understanding to contribute to operational participation in the network. The way in which this information must be secured is still being studied. The internal communication of the Commission is supported by the current ARGUS platform. The financial support for the initiatives relating to the EPCIP programme will be endorsed by the Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks" until 2013, as established by the Seventh Framework Programme of the EU. In view of this, the achievements of the EPCIP programme are part of a dynamic process. As announced in the annual reports, the framework has been established according to the timetable of the action plan[5]:

> "Within the competence of the European Community, the programme offers a comprehensive framework and contributes to the development of the European Programme for Critical Infrastructure Protection (EPCIP) as well as policy measures aiming at upholding, and/or guaranteeing security and public order during a crisis situation."

4 COM (2008) 676 final.
5 COM (2006) 786 final.

It should also be noted that, as far as civil protection is concerned, assistance can be requested through the MIC (Civil Protection Monitoring and Information Centre): a warning system of the European Commission which enables people to coordinate mutual assistance and cooperation between member states in the event of major emergencies.

At the Council level, a cooperation platform was created in 1987 under the name EUR-OPA: resolution 87/2 states that its activities lie within the crisis management of major natural or technological disasters. To this end, the cooperation between member states has materialised by the creation of a multidisciplinary framework for the development of projects aiming to raise public awareness and resilience. In order to set up a common work basis, the Commission published in 2009 a new document[6] summing up the necessity for a coherent and common approach for the:

- determination of conditions enabling a management policy for disaster prevention (based on accurate and scientifically proven information);
- consultation between the various actors and the policy for crisis management;
- exploitation of existing resources for disaster prevention;
- reinforcement of international cooperation as far as prevention is concerned.

This document most certainly provides a positive basis to rationalise existing resources and their use.

Dependence between CIP and the protection of critical information infrastructures

We have noticed that the legislative responsibilities for the management of CIP (CIIP) lie with the member states. Besides, we have to admit that all member states are not moving forward at the same pace and in the same manner to implement the directives. Consequently, it is of the utmost importance that European coordination should be reached in order to meet the objectives stated in the action plan. The interaction between the various sectors included in the EPCIP programme is clear: electricity, gas and oil have been classified in the energy sector. Electricity relies nevertheless strongly on oil and gas (or *vice*

6 COM (2009) 82 final.

versa). Furthermore, the monitoring and management systems of those infrastructures (Supervisory Control and Data Acquisition-SCADA) use computer networks. Those systems interact and are also subject to a wide range of sensitivities, such as previously mentioned. As far as transport is concerned, the EPCIP programme comprises the sub-sectors of road and railway transport, air traffic and shipping. It is obvious that the connections between those different sub-sectors are essential.

Dependencies can be of a physical or virtual nature: "cyber dependency" illustrates the importance of interfaces and data base connections. The importance of interaction and dependences is obvious: they are essential elements for the sensitivity assessment of the system as a whole. Not only are the various sectors or sub-sectors critical, but their mutual dependence is crucial for the scenarios in which cascade effects will prevail. In this field, research is being conducted, for example, in the case of sabotage or electrical network saturation[7].

Military dimension of CI(I)P in the EU

The military aspect of CIP is by no means insignificant. At the national level, the intervention of armed forces is planned in the framework of support to the nation in order to overcome the saturation of the logistic capacities of public services. As regards security, the respective laws differ: in Belgium, exceptional measures allowed the support of Defence to the police during the attacks of the *Cellules Communistes Combattantes* (Communist Combatant Cells) in 1985. France has been planning a similar intervention since 1978, when the plan "*Vigipirate*" was launched. Other countries do not constitutionally allow military troops to intervene on the national territory.

At the European level, military structures have been developed in the framework of the European Security and Defence Policy (ESDP). The EU military structure, which carries out the ESDP and which has been renamed Common Security and Defence Policy (CSDP) after the ratification of the Lisbon Treaty, falls within the scope of the tasks of the "second pillar" of the organisation. Considering the separation of competences between Council and Commission, having an insight into the state of play in the activities in the CIP field is

7 V. Rosato, "Modelling interdependent infrastructures using interacting dynamic models", Int.J.Critical Infrastructures, Vol. 4, No.1/2, p. 63-79, 2008.

rather complex. Either at the national level, which recommends appealing to European aid through the MIC, or at the Union's level, for the deployment of troops in the framework of an EU military operation, critical infrastructure protection is planned in both cases. The supreme military body, whose task is to assign missions within the Council of the EU, is the EU Military Committee (EUMC). The EU Military Staff (EUMS) will implement the Committee's decisions while activating military capacities available within the EU. In addition, the EUMS remains the source of military expertise, under the authority of the EUMC. In the light of the dispersal of expertise among member states, the coordination of the protection through the Committee and the Military Staff is essential.

In the preceding section, we have noted that the critical infrastructures often depend on computer networks. Quite obviously, armed forces cannot develop secured networks on their own, except if they are isolated and possess an independent exploitation network: an alternative would be to offer secured integration of military and civil networks, at least for a defensive action. However, this approach is fundamentally different from the one adopted in NATO, which focuses even more on cyber defence. Whereas offensive operations for CIIP are, as far as we know, not yet mentioned in NATO doctrine, they will be one of the points receiving specific attention in the near future. In EU doctrine, this option is already planned, though some aspects of task distribution within the EU still remain under discussion. The roles hitherto shared among the CI(I)P domains have been the subject of fierce debate. So, a seminar on the role of cyber security within the CSDP was concluded with these words: "At the Union level sizeable efforts to address cyber threats are already taken under the First and Third Pillars. The central question at the seminar was whether to address the cyber threat under the Second Pillar too and to seek a more comprehensive cross-pillar approach." [8]

Conclusion

Sovereign states do not have the possibility to ensure critical infrastructure protection autonomously: at present, the interdependence of sectors and globalisation offers an opportunity for markets. At the same time, new threats involving

[8] General Secretariat of the Council of the EU and the EU Institute for Security Studies, "Cyber Security: What Role for CFSP?", Seminar held in Brussels on 4 February 2009. Institute Report IESUE/SEM(09)04, 10 March 2009, p. 4.

inter-state risks are part of the side effects that we should be able to face. Hence the supranational level needs to get organised: either NATO or the European Union will have to define measures to be taken and synergies to be developed in order to promote communication as well as information exchange to implement common early warning systems. Interoperability should be promoted both in civil and military systems in order to protect the proper functioning of the institutions and to ensure the protection of infrastructures and services, including that of energy resources. Cooperation between NATO and the EU should make it possible to become complementary in the implementation of measures to improve resilience at all times.

Bibliography

G.B. Asheim, *Behavioral game theory*, Lectures in game theory, Oslo University, 2009.

B. Bennett, *Understanding, Assessing, and Responding to Terrorism. Protecting Critical Infrastructure and Personnel*, John Wiley & Sons, London, 2007.

V.M. Bier, Game theoretic Risk Analysis of Security Threats, Springer, New-York, 2009.

B. Cornelis, *Federal Risk Inventory, Survey and Knowledge building*, SPIRAL, Liège, 2004.

V. Rosato, "Modelling interdependent infrastructures using interacting dynamic models", Int.J.Critical Infrastructures, Vol. 4, No.1/2, p. 63-79, 2008.

R. Zimmerman, "Decision making and the Vulnerability of Interdependent Critical Infrastructure", CREATE Report 04-005, Homeland Security Center, p. 1-4, 2004.

EUR-OPA major hazards agreement. Comparative analysis of the Interministerial Management of Major Hazards: Belgium, France, Russia, Bulgaria. Council of Europe, AP/CAT (2005) 30, Strasbourg, 21 June 2005.