Royal High Institute for Defence
Center for Security and Defence Studies

Critical Infrastructure Protection Policy in the EU: state of the art and evolution in the (near) future.

Sr. Capt. Bart Smedts

FOCUS PAPER 15

June 2010

Critical Infrastructure Protection management system developed by Lockhhed Martin (Credits : Lockheed Martin)

Abstract

Conventional attack, but evenly asymmetrical threat need resilient response: risk analysis and critical infrastructure protection are therefore key words in an environment threatened by asymmetrical proliferation. Starting from the existing EU framework, a comparison is drawn with some NATO approaches in critical infrastructure protection policy. Synergies could lead to improvements for better cooperation and interoperability between EU and NATO operations. The corollary will lead to the reinforcement of homeland security, hence national approach in its present context is analyzed. Finally, recommendations are formulated to reach an integrated approach between national, EU and NATO institutions in relation to risk analysis and protection of our critical infrastructure.

The views expressed are only those of the author.

Keywords: EU, Risk analysis, CIP, CIIP, synergy.

ABOUT THE AUTHOR

Bart Smedts is Sr. Capt. of the Belgian Air Force. He is currently fellow researcher at the Center for Security and Defence Studies of the Royal High Institute for Defence where he is in charge with proliferation issues.

TABLE OF CONTENTS

ABBREVIATIONS

ARECI	Availability and Robustness of Electronic Communications Infrastructures
ATU	Action Against Terrorism Unit
BELNIS	Belgian Network Information Security
BIPT	Belgisch Instituut voor Posterijen en Telefonie
CBRN(E)	Chemical Bacteriological Radiological Nuclear Explosives
CERT	Computer Emergency Response Team
CFSP	Common Foreign and Security Policy
CI²RCO	Critical Information Infrastructure Research Co-ordination
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CIVCOM	Committee for Civilian Aspects for Crisis Management
CIWIN	Critical Infrastructure Warning Information Network
CMPD	Crisis Management and Planning Directorate
CNO	Computer Network Operations
CORDIS	Community Research and Development Information Service
CPCC	Civil Planning and Conduct Capability
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
EADRCC	Euro-Atlantic Disaster Response Coördination Centre
EADRU	Euro-Atlantic Disaster Response Unit
EDA	European Defence Agency
EDHS	European Department of Homeland Security
EEAS	European External Action Service

EECMA	European Electronic Communications Market Authority
EGC	European Government CERTs group
EISAS	European Information Sharing and Alert System
ENISA	European Network and Information Security Agency
EP3R	European Public Private Partnership for Resilience
EPCIP	European Programme for Critical Infrastructure Protection
ESDP	European Security and Defence Policy
EUMC	European Union Military Committee
EUMS	European Union Military Staff
FCCU	Federal Computer Crime Unit
MIC	Civil Protection Monitoring and Information Centre
NCIRC	NATO Computer Incident Response Capability
ROE	Rules Of Engagement
SCADA	Supervisory Control and Data Acquisition

1. INTRODUCTION

In a previous study, "Weapons of mass destruction: legacy of the Cold War and threat to the future," recommendations were formulated in order to improve national emergency planning. One of the recommendations was aimed at proper risk assessment, an essential part in the evaluation of the resources to be deployed in CBRN(E) scenarios: since 9/11, we witnessed disruptive conventional attacks in London, Madrid, Mumbai and Islamabad to name but a few. Should we also underline the shift of the Afghan conflict to Pakistan, a nuclear weapon state which has not signed the Non Proliferation Treaty? The presence of sleeping Al Qaeda cells on European soil, increases the possibility for terrorist attacks. Therefore the threat is not always to be considered from outside existing borders but should also take into account "the enemy within". Risk analysis can help determine what this means or what improvements should be made to existing plans, or what infrastructure should be better protected. Future threats will materialize in proliferation, international terrorism, unequal distribution of wealth, spreading of organized crime and pandemics. This type of threat undergoes additional pressure from globalization with as direct consequences the growing energy demand, climate change, urbanization, demographic explosion and its sociological consequences as well as the present economic crisis. This study aims to shed some light on the consequences of aforementioned problems, hence risk analysis and critical infrastructure protection are key words in an environment of asymmetrical proliferation.

First, the framework will clearly be defined by the explanation of relevant definitions, for concepts like risk, threat and impact are often interchangeably used: this can result in unclear contextual documents which are useless. Once these foundations laid out, the methodology for the development of a

sound critical infrastructure protection planning can be detailed.

After these basic foundations, the EU-framework for critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP) will be explained. The dependency between these two frameworks will be detailed as well as their military dimension.

Finally, recommendations will be formulated which could improve homeland CIP and CIIP for expeditionary forces.

2. METHODOLOGY TO OBTAIN EFFECTIVE CIP

Even though the worst happened in some parts of the world, the reluctance to invest in measures to prevent incidents remains. One reason could be the assumption that such incidents would not take place a second time, or else financial considerations in time of financial crunch prevail. The fact is that in 2009, even in the US, the situation has not really improved much since 9/11, notwithstanding the creation of new national security departments such as The Homeland Security Council (HSC) and Department of Homeland Security (DHS). Cooperation with other departments is not clear yet between actors and the command during an incident is a perfect ambiguity. This was once more illustrated in the attempted bombing incident the December 26th, 2009 when a Nigerian listed terrorist failed to ignite its explosive charge in the final phase of a transatlantic flight from Amsterdam to Detroit: in Europe his explosives were not detected and he was even allowed to board.

European security shows not so much difference with the one in the US: at different stages, security measures are failing. Essential elements that could lead to an effective methodology of risk assessment are lacking. The consequence can induce lasting problems at national levels alongside a lack of concrete planning of all necessary means to obtain effective and working risk management. The methodology once developed or

convened internationally, could deliver a blueprint for all incidents of interest to be handled in the future. Further it could help to identify capacities needed to counter a specific threat, where to put them in operation and how to get them integrated into an effective Emergency Plan with adequate command and control at the national and supranational (EU) level. These elements can only be resolved as a result of extensive research on clear and undisputed definitions of threat, risk and impact: 9 years after the ravaging events in the US, these basic cornerstones of risk management are not yet clearly put in place, or at least not similarly understood by different member states in the EU on the one hand and between transatlantic partners on the other hand. All kinds of reasons can be cited for this: one is undoubtedly the price tag attached to R&T of detection equipment and uniformity of procedures. It is still much more expensive to rely on disaster relief than to be able to fall back on proactive risk analysis and management. A possible sequence of steps includes:

- Identification of critical infrastructure (CI): determining a catalog based on established international criteria and definitions. The current list does not meet those requirements. A review may for example offer new solutions for the outdated national list of criteria: cyber infrastructure is to be considered as a vital part of CI.

- Threat Analysis: proactive identification of CI elements could be integrated in a strategic document including trends to be expected in the future. Adequate information analysis from intelligence resources is required at this point.

- Vulnerability Analysis: determining the impact of an incident on CI, taking into account the sensitivity of the existing facilities for a list of possible occurring incidents.

- Risk: one should mention here that a catalog of existing risks can be performed a priori. According to the definitions, this catalog should encompass the distinction

between each potential risk in relation to their possible cause, nature, target and type of impact. Different models can be applied for risk classification in order to obtain priority listings. It is however crucial to understand that the obtained priorities are snapshot results and should be considered in dynamic evolution: depending on the identified trends and threats previous priorities should be reassessed. Asymmetric proliferation will also adapt to the countermeasures that were put in place: an imminent or ongoing cyber attack could be the forerunner for an imminent conventional or CBRN(E) threat. Moreover, it has to be understood that different critical domains are interdependent. Hence, a single incident can be the cause for disruption in different domains of our society due to cascade effects which are not often considered in risk assessments.

As it is obvious that Information Infrastructure is part of the CI, specific measures must also be developed in the context of CIIP. One must acknowledge that CIIP should be realized in a comprehensive approach with regard to CIP. The definitions lead out, measures which could lead to the protection of critical infrastructure can be defined as follows:

- Provide means for preventive action including exercise and training (prevention, training and exercise).
- Provide immediate response to early signals (mitigating).
- Provide the capacity for rapid detection of an ongoing incident (detection and early warning).
- Coping with the consequences during the incident and display resilience competence (respond).
- Recovery to normal as soon as possible (recovery).
- Learning lessons from the events and feed-back to appropriate actors (lessons learned).

As definitions are agreed upon, work becomes easier. At least we can expect inconsistencies and discrepancies to be eliminated from policies and doctrines. That is the reason why the present situation in the EU regarding CIP and CIIP was further considered in detail: possible synergy with NATO way of thinking could improve operational readiness.

3. EU-FRAMEWORK FOR CRITICAL INFRASTRUCTURE PROTECTION (CIP)

Besides the terrorist attacks on the WTC towers and subways in London and Madrid, the tropical storm Katrina has shown that natural disasters can seriously damage existing infrastructure. Natural or man-made disasters could be the cause for the disruption of every day life. But even political decisions can have similar effects: the disruptions of gas supply from Russia to East-Europe during the winter of 2008-2009 illustrate this. The energy sector seems to be an essential issue that should be considered under the umbrella of critical infrastructure protection. One must also understand the importance of the interconnection between the various sectors: due to globalization, the vulnerability resulting from interconnections between different economic sectors increases. As a result, networks are to be considered as a whole instead of focusing on separate sectors such as energy, information exchange, communication, food and transport: cascading effects due to failure in one sector, are certainly not inconceivable. An additional difficulty is caused as a result of the liberalization of the market economy and privatization. National governments are no longer in full control over all sectors that are essential to society: private partners hold the greatest share of major companies controlling the above mentioned sectors and services. This allows for national or supra-national interests to be disregarded as they conflict with commercial interests of private companies.

As mentioned above, the capacity to protect CI, is highly dependent on the basis of definitions on risk, followed by the

process of defining CI, cataloging of CI and finally selecting the measures that can reduce risks. This leads us to the conclusion that, as far as CI is concerned, different selection criteria are applied depending on the country of origin. More general approaches have been given and refer either to the importance for the systematic functioning of society or even the symbolic value of a facility/infrastructure. Another approach is based on whether the "critical" aspect is due to the objective of the infrastructure or the impact that its failure would cause to society. The practical interpretation of a list of CI depends on a unique methodology, as set out at the end of the first paragraph. This leads us to the challenge to determine whether a national or regional infrastructure can be described as "critical". In the latter case, centralized action is required. One should not forget that a final "list" may contain sensitive information not only because of the fact that the CI itself is exposed, but also because of the fact that such a list may contain sensitive security information surrounding CI. The regular review of the list (including new risks) is an essential part of the procedure to protect CI.

An attempt to define CI at European level was established in 2005 by the publication of a Green Paper. In the context of the European Program for the Protection of Critical Infrastructure (EPCIP) 11 sectors with 37 related services were identified to be framed as CI's. The proposed Directive held 11 sectors and 29 subsectors. The EU Council, published a directive on December 8, 2008 in which only 2 sectors and 8 sub-sectors remain (energy and transport). Furthermore, the initial responsibility for the protection of CI remains a national responsibility. Important is the distinction made between national and European CI: the European dimension is being considered when an infrastructure becomes critical for more than one Member State of the Union.

Besides these sectors, the EU is aware that CI may be located outside the EU: this has explicitly underlined the importance of crude oil and gas pipelines supplying the EU. The plants or

pipelines bordering the EU are essential for the economy and every day life. Destruction or sabotage of these facilities located in countries bordering the EU, possibly in politically unstable regions, could have unprecedented consequences for the EU: this was precisely illustrated by the failure of the supply of gas from Russia. The interconnection of contemporary economy was demonstrated by the economic crunch. Cooperation to obtain lasting solutions is encouraged in these issues through sector agreements.

Given the exchange of information about threats and vulnerabilities plays a crucial role, it became clear that a specific network was necessary: this task was assigned to the Critical Infrastructure Warning Information Network (CIWIN)[1]. The network has two functions. First it is an electronic forum for exchange of information on the protection of CI. In addition, it is a rapid alert system for the delivery of early warnings for member states to inform the Commission in relation to acute risks and threats for all. All Member States have signed a Memorandum of Understanding for contribution to the operational participation to this network. CIWIN is a network that effectively supports exchange of information between EU Member States. The manner it has to be safeguarded is still under consideration. The internal communication of the Commission is supported by the existing ARGUS-platform[2]. The financial support for initiatives regarding the EPCIP program will be provided by the "Specific Program for Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" (CIPS) until 2013, under the terms of the Seventh Framework Program of the EU. In this respect, the achievements of the EPCIP program are part

[1] COM (2008) 676 final.

[2] An internal network for rapid dissemination of information between directorates and services of the Commission. Rationalization of the early warning networks of the EU is a requirement which could improve the coherence of the ICT-network.

of a dynamic process. As announced in the annual statements, the context has been defined as follows[3]:

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

Additional tools for the creation of an extensive EPCIP framework were provided by consultation of expert groups, exchange of information and identification of dependencies. It should also be mentioned that, in terms of civil security, assistance may be requested by the MIC (Civil Protection Monitoring and Information Center): a warning system from the European Commission that allows to coordinate faster mutual aid and coordination between Member States in case of serious emergencies.

At Council level, a cooperation platform was created in 1987 by the Ministers of the Council of Europe under the name EUR-OPA: the wording of the resolution 87/2, locates its activities in the crisis of major disasters of natural or technological origin. To this end the cooperation of the Member States was requested to encourage a multidisciplinary framework for the development of projects increasing awareness and resilience of the population. In order to create a common working basis, the Commission issued a new document in 2009 summarizing the need for a coherent and common approach by:

- Determining the conditions that allow a management policy for disaster prevention (based on accurate and scientifically based information).

[3] http://ec.europa.eu/justice_home/funding/cips/printer/funding_cips_en.htm accessed July 13, 2009. The agenda was initialy determined by the EPCIP Action Plan as outlined in appendix of COM(2006)786 final.

- Actors and politics consult together for disaster management.
- Exploit existing resources in favor of disaster prevention.
- Strengthening international cooperation in terms of prevention.

This document explains undeniably a positive basis for a rationalization of existing resources and their use.

Since 2000, the EU Council created new permanent structure for operational management of the civilian aspects of ESDP operations, namely the Civil Planning and Conduct Capability (CPCC). It is under the political and strategic control of the Political and Security Committee and its military arm the EU Military Committee (EUMC). The CPCC Director can rely on the capabilities of the Military Staff (EUMS) regarding civilian planning, capacity and available expertise (through the Civil / Military Cell) for operational planning and execution of the civilian aspects of crisis management operations. In 2009, civilian and defence directorates were merged in the Council Secretariat with the Civ-Mil Cell to form the Crisis Management and Planning Directorate (CMPD). As an example of some CPCC initiated operations, we can mention EUPM (Bosnia and Herzegovina), EULEX (Kosovo), EUPOL (RD Congo), EU SSR (Guinea Bissau), EUBAM Rafah (Palestine), EUPOL COPPS (Palestine), EUJUST LEX (Iraq) and EUPOL (Afghanistan). This organization has also a role to play in the aforementioned area of disaster prevention and disaster management of CIP. It is striking to realize that CIP responsibilities appear to be scattered over different levels of responsibility. Gya described the capacity and capability domain in 2008[4]:

[4] GYA, G., JACQUEMET, O., « ESDP and EU-mission update. », in ISIS European Security Review, ISIS, N°39, July 2008.

> *"Also required, is a stronger EU liaison between the CPCC (the Civilian Planning and Conduct Capability - directly responsible to the SG/HR Javier Solana) and DGE IX (civilian crisis management DG of the Council General Secretariat under DGE IX) – particularly vis-à-vis training and concepts."*

For clarification of this statement we should refer to the original document which states[5]:

> *"The EUMC will provide guidance, through DGEUMS, on the military activities undertaken by the EUMS within the framework of civilian crisis management. Contributions by the EUMS for civilian aspects of crisis management remain under the functional responsibility of DGE IX for all activities (planning, Fact-Finding Missions, etc.) up to and including the development of the CMC and, where appropriate, CSO/PSOs. Once a decision to launch a mission is taken, these contributions come under the functional responsibility of DCPCC. Reporting on these activities to the CIVCOM will be conducted in accordance with established procedures on civilian aspects of crisis management."*

Instead of clarification, the scattering of responsibilities becomes confirmed: it is clear that a rationalization of the operational information and responsibilities should be imposed here.

---

[5] Doc 7235/08 van 18 maart 2008 (COUNCIL DECISION amending Decision 2001/80/CFSP on the establishment of the Military Staff of the European Union), p.11.

4. EU-FRAMEWORK FOR CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP)

In anticipation of the year 2000, fears for the millennium bug -a global paralysis of information networks- emerged. It soon became clear that the information, the carriers and vectors, could seriously be disrupted due to a simple software bug as illustrated by the fact that customers are unable to use their credit cards as the year 2010 is not recognized in some payment systems. As illustrated, CIIP therefore refers to the protection of these two hatches: information and hardware containing and processing that information. One must bear in mind that some aspects are fundamentally different from CIP. In principle, any citizen is a customer of the information network. Therefore he also constitutes the weak link: not everyone is thoroughly informed about security problems of information networks. The protection in this field seems therefore very difficult, given the entire world can access the network. Compared to CIP the safety problem seems much more difficult to ensure as private companies own the infrastructure and provide the services which have to be protected. A repeated information campaign for the benefit of the users would certainly help to improve the awareness of the level of network insecurity. An additional distinguishing feature compared to CIP is the absence of boundaries: the success of the information network is also its weakness. National boundaries are completely irrelevant, so one can not speak about one or other infrastructure to be important for one or more Member States. This sector is particularly vulnerable to cascade effects. Therefore, particular attention should be given to protection on a supranational level.

Cyber attacks on Estonia's network began in April 2007 and have shown that a coordinated attack on a nation's network initiated by private individuals or governmental agencies could be able to paralyze daily functioning of society. The consequences have awakened many people and have made them understand the risk of coordinated attacks on the cyber

network in conjunction with a physical threat. The difficulty in this field can be found in the diversity of national approaches to CIIP; some trust largely on the resilience of the private sector (Switzerland, Great Britain), while others held the main reactive role in the hands of national institutions, including through deployment of military experts (Sweden, France, USA). The example of Estonia was an important test case: it is now clear that an early warning chain is required at the supranational level. Further attention is focused on a criminal approach to cyber security: the G8 agreed to set up a network to coordinate the denial to Internet for terrorist activities or cyber crime purposes. The legal basis for this action is contained in the regulation of the Ministerial Council of the Organization for Security and Cooperation in Europe (OSCE)[6]: cooperation by the Action Against Terrorism Unit (ATU) is promoted based on the existing G8 24/7 Computer Crime Network, which can also act as a central organ for detecting unauthorized network abuse and cyber terrorism. Each State has a point of contact in this group: Belgium has entrusted this task to the Federal Police.

The EU has also coordinated a number of initiatives to combat cyber attacks. To this respect, the thrust of the moves aimed at coordinating national initiatives, to harmonize national legislation with statutory provision for data protection and privacy (though the latter also works in favor of organized crime). Furthermore, a European Network for Information Security (ENISA) was established: although it has no powers in the fight against cyber attacks, the agency works as expertise platform. The finding that there was no cross-border cooperation in the field of network and information security has led to a closer cooperation between Member States. To this aim ENISA was empowered by the European Commission to fulfill the role as a centre of excellence[7]: it collects and analyzes data on security incidents in Europe. Risk assessment and risk

---

[6] OVSE MC Decision 7/06.

[7] COM (2007) 861 final, p.18.

management are performed to promote the capacity to improve safety risks, while exchange of information and cooperation between actors in information security are stimulated, in particular through partnerships between the private and public sectors.
Follow-up of standardization for products and services focused on network and information society is one more task of ENISA: it allows for interoperability of networks and information platforms where Member States guarantee the safety of technical requirements.

Initially appointed on March 14, 2004 for a period of five years[8], the mandate was extended until March 13, 2011. In order to ratify the decisions of 2007 on the framework laws of the telecommunications sector, the European Electronic Communications Market Authority (EECMA) would endorse the tasks attributed to ENISA[9]. Under the Sixth Framework Program (6FP), the EU made progress in the field of research on this topic. The CI²RCO project provided the agenda[10]:

> *"The Agenda is structured around the following eight groups of R&D topics:*
>
> 1. *Holistic system security.*
> 2. *Risk management & vulnerability analysis.*
> 3. *Prevention & detection.*
> 4. *Incident response & recovery.*
> 5. *Survivability of systems.*
> 6. *Polices and Legal environment.*
> 7. *Fundamental research and development.*
> 8. *Non-technological issues which compromise CIIP."*

---

[8] Regulation (EC) N°460/2004.

[9] COM (2007) 699.

[10] Critical Information Infrasructure Research Co-ordination (CI²RCO) project Research running from March 1, 2005 till February 28, 2007. Critical Information Infrastructure. The CI²RCO project: Towards a European Research Agenda. The CI²RCO consortium, 2007, p.13.

The project was intended to catch up with the transatlantic initiatives under the direction of a consortium led by Germany, France, Italy, Switzerland and Netherlands. Note that items 1 and 8 specifically focus on inter-dependency of different sectors, which is essential if cascading effects should be controlled. Since the EU Council published its strategy for a secure information community in Europe[11], initiatives in the framework of an extensive R&D plan were revised. As appeared in the March 2007 report of the ARECI study[12] the weak links in the communication infrastructure remain: unlike the traditional approach based on an existing threat, existing weaknesses are defined in order to obtain a robust network, regardless the type of threat that is susceptible to attack our infrastructure. This knowledge allows for improvements that should be able to resist any type of attack.

In the context of the eEurope 2005 Action Plan, an interim report was issued to the Commission that concluded the technical evolution in terms of ICT activity extended by far the national borders. Furthermore, we are well aware of the fragmentation between Member States in terms of capacity in the field of ICT. The need exists at European level to develop initiatives to promote competitiveness, even if this gap between the frontrunners and the rest of the group has to be closed. A "country profile" made one aware that the lack of ICT capacity and a discrepancy between the Member States exists. Therefore, the existing capacity gap should be solved in a coherent safety policy.

With the aim to protect Europe against massive cyber attacks, the European Commission defined an action plan that comprises[13]:

---

[11] 2007/C 68/01.

[12] Availability and Robustness of Electronic Communications Infrastructures.

[13] COM (2009) 149 final, pp.8-11.

Preparedness and prevention	Baseline of capabilities and services for pan-European cooperation	target: end of 2010 for agreeing on minimum standards; end of 2011 for establishing well functioning National/Governmental CERTs in all Member States[14].
	European Public Private Partnership for Resilience (EP3R)	target: end of 2009 for a roadmap and plan for EP3R; mid of 2010 for establishing EP3R; end of 2010 for EP3R to produce the first results[15].
	European Forum for information sharing between Member States	target: end of 2009 for launching the Forum; end of 2010 for delivering the first results.
Detection and response	European Information Sharing and Alert System (EISAS)	target: end of 2010 to complete the prototyping projects; end of 2010 for the roadmap towards a European system
Mitigation and recovery	National contingency planning exercises	target: end of 2010 for running at least one national level exercise in every Member State[16].
	Pan-European exercises on large-scale network security incidents	target: end of 2010 for the design and run of the first pan-European exercise; end of 2010 for pan-European participation in international exercises[17].
	Reinforced cooperation between National/Governmental CERTs	target: end of 2010 for doubling the number of national bodies participating in EGC: end of 2010 for ENISA to develop reference materials to support pan-European cooperation[18].
International cooperation	European priorities on long term Internet resilience and stability	target: end of 2010 for EU priorities in critical Internet components and issues.

[14] At the time of redaction, a European Government CERTs group comprises delegations from Finland, France, Germany, Hungary, The Netherlands, Norway, Sweden, Spain en the United Kingdom (see http://www.egc-group.org/). Belgium has activated a national and a military CERT in september 2009, but due to the lack of clear definitions, the national CERT lags behind as compared to other Member States' CERTs. In the foresight of the Beijing 2008 Olympic games, cyberexercises were organized by the Asia Pacific Computer Emergency Response Team (APCERT- zie http://www.apcert.org/ accessed July 10, 2008).

[15] In this framework "private public partnership" are nationally promoted by the Federal Computer Crime Unit (FCCU) to compensate for the lack of an operational CERT at that time.

[16] We stress the importance to have an operational CERT or CSIRT to take part in exercises.

[17] Also in this area, Europe is lagging as compared to efforts performed outside its' boundaries: Australia published a report of their second national exercise "Cyber Storm II" in 2008.

[18] On August 4, 2009 a notification could be found on the imminent creation of a national Belgian CERT http://belsec.skynetblogs.be/post/7190683/a-real-cert-in-belgium-to-be-established (accessed August 18, 2009)..

	Principles and guidelines for Internet resilience and stability(European level)	target: end of 2009 for a European roadmap towards principles and guidelines for Internet resilience and stability; end of 2010 for agreeing on the first draft of such principles and guidelines.
	Principles and guidelines for Internet resilience and stability (global level)	target: beginning of 2010 for a roadmap for international cooperation on principles and guidelines for security and resilience; end of 2010 for the first draft of internationally recognized principles and guidelines to be discussed with third countries and in relevant for a including the Internet Governance Forum.
	Global exercises on recovery and mitigation of large scale Internet incidents	target: end of 2010 for the Commission to propose a framework and a roadmap to support the European involvement and participation in global exercises on recovery and mitigation of large-scale Internet incidents.
Criteria for European Critical Infrastructures in the ICT sector	ICT sector specific criteria	target: first half of 2010 for the Commission to define the criteria for the European critical infrastructures for the ICT sector.

From this action plan it appears that ICT is considered to be an essential element in the European CI. The immediate consequence is that the ICT sector should be included again in the EPCIP program. If one reads the accompanying document on this action plan[19], one comes to the conclusion that an impact study is subject to voluntary implementation, with no legally binding framework (for example by a binding regulation). The reason for this can be found in the diversity of different national approaches with regard to information security, the operational responsibility of the private sector and the temporary lack of exchange of information between public and private sectors. Ongoing studies were published in 2009 under the framework of the EU strategy of research on CIIP. Framework Program 7 (Studies on EU Policy Initiative on Communication and Critical Information Infrastructure Protection)[20] includes more than 90

[19] SEC(2009) 400 dated March 30, 2009.

[20] Het EU FP7 2007-2013.

research projects, funded through the Seventh Framework Program to assess the future evolution of the Internet and its spin-off applications in security issues[21].

5. DEPENDENCY BETWEEN CIP AND CIIP

We have stated that the EU leaves legislative responsibilities and management of CIP as well as CIIP to the Member States. Consequently, we must admit that not all Member States are progressing at the same pace or in the same way in their efforts to implement directives. Therefore, it is important that efforts should be coordinated in order to achieve the objectives laid out in the action plan. The interaction between different sectors included in the EPCIP program is clear: electricity, gas and oil facilities were put in the energy sector. Electricity however is highly dependent on oil and gas production (or vice versa). Moreover, the control and management systems of infrastructure (Supervisory Control and Data Acquisition-SCADA) are performed over ICT networks. These systems evenly interact with each other and are also subject to a wide range of sensitivities, as previously mentioned. Concerning transport, the second sector of the EPCIP program holding rail, air and sea transportation, it is obvious that communications are essential in these subsectors! Dependencies may be physical in nature (e.g. the output of a production line used in one other). Cyber Dependence can illustrate the importance of interfaces and database connections. Geographical dependence may relate to roads or bridges that are common routes for different CI. The importance of the interaction and dependencies is clear: these are an essential element for the assessment of the sensitivity of the complete system. Not only the individual sectors or subsectors are critical. Not only scenarios that involve individual sectors are at risk! The mutual dependence of the different sectors is important for scenarios

[21] TSELENTIS, G., et al., Towards The Future Internet. A European Research Perspective. IOS Press, 2009.

where cascade effects will prevail. This particular issue was also taken into account by the EU under the "6th framework program" umbrella. Project number 004547 has led to the work entitled" ICT Security & Dependability Research beyond 2010: Final strategy". In launching the "7th Framework Program", the research priorities for the future are as follows[22]:

- Empowerment of stakeholders.
- Europe-specific Security & Dependability.
- Infrastructure robustness and availability.
- Interoperability.
- Processes for developing Secure & Dependable systems.
- Security and Dependability Preservation.
- User-centric security and dependability standardization.
- Security and dependability of Service Oriented Architectures.
- Technologies for security.

In the same context research into complex networks and inter-dependency or disruption of connected networks was performed by ENEA[23]. One of the results can be found on the ENEA Internet site: it is a tool for its analysis to test the sensitivity and the interdependence of complex network structures (Network Analysis Tool[24]). Other research, among others, on the dependency of electricity and communication

---

[22] SecurIST ICT Security & Dependability Research beyond 2010: Final strategy. Deliverable 3.3 of the 6th framework programme. Project 004547, January 2007, p.37.

[23] Ente per le Nuove technologie, l'Energia e l'Ambiente (Italian National Agency for New Technologies).

[24] http://irriis.nat.ylichron.it/ accessed July 8, 2009.

networks, was formed by Rosato et al.[25]. This type of research is crucial in the process of risk analysis through the findings on interdependencies: it can deliver insight into the different causes and processes involved resulting in cascade effects on different sectors of CI.

6. MILITARY DIMENSION OF CI(I)P IN THE EU

Given the separation of competence over the three pillars of the EU, it is not an easy task to get a comprehensive view on the state of the art concerning activities and doctrines in the CI(I)P domain. The military structure of the EU, which executes the European Security and Defense Policy (ESDP) fits in the second pillar of the organization. In the lead field, national representation is performed by the ambassadors within the Political and Security Committee (PSC)[26] in order to determine to the European Security and Defense Policy.

The highest military body in the EU Council is materialized by the EU Military Committee (EUMC)[27] . Military representatives of the Member States can also assist the Chairman of PSC for specific military matters. The Military Staff of the EU (European Union Military Staff-EUMS)[28] stands for the connection between the EUMC and the available military capabilities within the EU. Moreover it is the source of military expertise for the benefit of the organization of the EU under the supervision of the EUMC[29]. Important to know is that all requirements and doctrines related to CIIP are produced by the Department

---

[25] ROSATO, V., ISSACHAROFF, L., TIRITICCO, F., MELONI, S., DE PORCELLINIS, S., SETOLA, R., «Modelling interdependent infrastructures using interacting dynamic models.» *Int.J.Critical Infrastructures, Vol 4, Nos.1/2,* pp.63-79, 2008.

[26] Council decision of January 22, 2001 (2001/78/CFSP).

[27] Council decision of January 22, 2001 (2001/79/CFSP).

[28] Council decision of May 10, 2005 (2005/395/CFSP amending Decision 2001/80/CFSP).

[29] Doc 7235/08 dated March 18, 2008 (COUNCIL DECISION amending Decision 2001/80/CFSP on the establishment of the Military Staff of the European Union), p.11

Requirements of the CIS Section in the EUMS. After ratification of the Lisbon Treaty, the Common Security and Defence Policy (CSDP) was set up and in this framework the EU Military Committee submitted the conceptual analysis of Computer Network Operations (CNO) to the European Defence Agency (EDA). As this did not fit into the role of EDA, the CNO concept was elaborated by the CIS-department of the EUMS. The CNO concept however goes far beyond what is known as cyber defence: it includes defense against attack, but also offensive operations. The available expertise is scattered over the Member States, hence the organization of a workshop on June 4th, 2009: questions were addressed about the available technology, the involvement of every nation and the circumstances under which the available capacity should be used. Clearly, the military can not build secure networks by themselves, except when isolated with an independent operational network: an alternative would be to provide a secure integration of military and civilian networks, at least for defensive action. In September 2009 a concept for Computer Network Operations was still drafted. The approach however is fundamentally different from the NATO approach which is still focusing on cyber defence. While offensive CIIP operations are, to our knowledge not yet mentioned in NATO doctrines, in the future it will be one of the points that will get special attention though.

It should be mentioned that in the third EU pillar (Freedom, Security and Justice), fight against terrorism is focusing on CIP (EPCIP), hence partly on CIIP because ICT is a major element in CIP concerns. A rationalization of the operation within the CIP/CIIP domain might benefit from an integrated and coherent approach. As the Lisbon Treaty came into force, the pressing need to rationalize, to resolve the distribution of competences between the different pillars becomes a possible way to join inter-pillar forces in the EU. This should benefit the coordination and efficiency. The coherence in foreign policy should be crystallized in the European External Action Service (EEAS): where the military role of the EU was to be found in the

second pillar, in the case of CI(I)P shared powers are scattered over the third and the first pillar. It would be appropriate to centralize all efforts. The hitherto diversified roles in the same CI(I)P areas was subject to discussion. Thus, it was also one of the considerations that were made during a seminar on the role of cyber security within Common Foreign and Security Policy (CFSP) EU[30]:

> "*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 more comprehensive cross-pillar approach*."

In many ways the NATO organization is more structured: whether it fits in military operations involving the protection of CI or support to civil emergency planning. The necessary resources are provided or can be used according to their availability. The problem is still acute for military cooperation in national emergency planning of Member states. In many cases, the capacity has been filled in on request on an ad hoc basis and in all cases supports the organization by the capacity of Member States. The organization of CIIP in the context of the concept of the NATO cyber defense is remarkable: the organization chart is clear and the contact points are fixed. The responsibilities are clearly defined in a "defense" concept. Other activities may obtain a mandate of the NAC under the conditions listed in Art. 4 of the Washington Treaty. It is striking that, in the quest for synergy between the two organizations, a flagrant lack of information exchange appears between the two organizations themselves. This in itself is no surprise when one considers the divided responsibilities among

---

[30] 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.

the various directorates of the EU. This was indeed one of the frustrations of the former Secretary General of NATO Jaap De Hoop Scheffer. His successor, Anders Fogh Rasmussen, is already working to create ties with the EU: under the new strategic concept of NATO, and new trends emerging as asymmetrical forms of threats, protection of CI and CII will clearly stand on the agenda.

7. RECOMMENDATIONS

In this part we want to formulate some policy recommendations for possible support to the approach slopes of CIP/CIIP rationalization. We may find that their implementation will much rely on the existence of a long term vision, call it a strategic plan or a concept: in order to cope with the threats emerging from new trends, nations and international bodies have to establish the framework within which the policies will lead to tangible results that go beyond vague terms or dispersed capabilities.

In a context of credit crunch and war efforts in many places of the world, it will be difficult to establish priorities. However, reduced efforts in the field of tactical and strategic security on our own territory, based on budgetary considerations are a dangerous choice to make: security is an essential part of society whether we need to ensure it several thousand kilometers from here or in the capital of Europe. The loss of service in any field whatsoever will compromise the essential foundations of our society: an immediate impact on our daily lives is not excluded. We find that protecting our national critical infrastructure against asymmetric threat needs coordination and rationalization: the task of a supranational body may be even more burdensome. Therefore a National cyber defence agency should have the legal basis for coordination of all cyber-related information and action into one federal body. Unlike the Belgian Network for Information Security forum (BELNIS), where interdepartmental actors meet and (some) information is exchanged, a recognized body could

improve the coordination of action to protect against cyber attacks. National agencies, extending their work beyond the CERT-responsibilities, could be the point of contact to NATO and the EU on the one hand, and favor the national coordination on the other hand. The ratification of the Lisbon Treaty and the new Administration in the U.S. create a new opportunity to work in the right direction to implement new strategies and optimize cooperation in this field.

Therefore, new equipment should be submitted to internationally agreed certification standards in order to ensure interoperability and national compatibility. This implies that operators themselves, whether it is at EU or national level, should obtain security clearances before accessing sensitive information and infrastructure. We already mentioned the urgent need to rationalize early warning systems and communications between the different EU-pillars. This is a critical item in the view of direct communication with the EU Military Staff and operational headquarters: military information networks and communications can not be isolated and should therefore be resilient to cyber attacks. Expeditionary forces are more and more relying on network enabled information exchange. Protection of CI(I) is crucial for the successful completion of the missions. This is one more reason to protect the information flow in order to rely on exact information. Interoperability should therefore be a priority for EU operations, as is the case for NATO-led operations. Concerning UN-operations a lot of effort has to be put in the field of interoperability.

An international body at EU level, coordinating the emerging threats and risks for the benefit of the Member States could improve the resilience for the benefit of CIP and CIIP. Furthermore, it could benefit from national analyses for direct exploitation and dissemination in order to coordinate international help and prepare to restrict the effects of cross-border consequences of natural or man-made disasters. The Christmas bombing attempt of the transatlantic flight to Detroit,

illustrates that security demands ever lasting effort and optimal coordination. A European Department of Homeland Security, could perform this task when manned by different security experts (police, customs, military, civilian security, cyber experts, intelligence agencies, etc). Such a body could also be empowered for the protection of critical energy infrastructure and the protection of supply of resources. The NATO Strategic Concept being reviewed, supply of resources will for sure be a topic to be discussed. The review at NATO level, should be an opportunity to revise the EU strategy in a comparable manner in order to enable coordinated action in case of disruption. Besides differences in policy, definitions should be standardized in the view of compatibility of Rules of Engagement. Definitions and policy should therefore encompass the rationale of CI(I)P cascade effect consequences. A holistic approach of all CI(I)P related issues, should therefore be based on thorough R&T efforts with tangible return on investment: application in military operations and in daily life.

A long term vision at national level is the cornerstone for the targeted ambitions. This also applies to the EU: as NATO's strategic concept is subject to revision, the EU should also work towards a strategic vision that fits into a complementary framework of cooperation, with clear agreement on respective responsibilities, without duplication of duties and continuous engagement for optimal interoperability. The recommended rationalization of communication channels is also related: redefining the position of supranational institutions becomes therefore necessary. Duplication of efforts and dilution of resources can therefore be avoided. Pooling of capacity is one of the possible slopes. Once the strategic vision of NATO laid out, the implications for its partners and the EU will urgently be needed.

8. CONCLUSION

In the medium to long term we will see new emerging trends. Asymmetric threats can potentially lead to "strategic shocks",

events that have a disruptive nature on the proper functioning of society. From these new trends, the definitions allow for proper risk assessment in a specific context of asymmetric threats. From this general approach, a method can be followed for decision making in policy support: examples show that many pitfalls inhibit proper conclusion. Following the outline of the applicable definitions regarding concepts as risk, threat and impact, and the chosen methodology, both at national and supranational level, adjustments should be imposed on definitions and methods: the interpretation of the CI(I)P concept has a different meaning in different institutions, which has consequences for the identification of critical infrastructure, let alone the employability of those measures would be provided for their protection.

As opportunities for synergies between the EU and NATO were examined, a defect appears to exist in the definitions, information exchange, capabilities and objectives of the two organizations. We have mentioned in this context that it was one of the frustrations of the former Secretary General of NATO Jaap De Hoop Scheffer. His successor, Anders Fogh Rasmussen, is already working to retie the bonds with the EU: under the new strategic concept of NATO, and the new trends materializing in emerging asymmetrical threat, CIP and CIIP will remain on the agenda. Energy security is one of these examples, but even for this issue, the EU has a clearly different interpretation than NATO.

The national approach to CIP/CIIP is based on a national interpretation of the European EPCIP directive: a comprehensive policy will have to establish the framework within which tangible results can be obtained. Therefore legislation must go beyond vague texts or listings of available means. More than other countries, Belgium is economically dependent on trade, service, innovation, logistics and transport. As a result, our country has much to gain from a good approach to CIP/CIIP issues: infrastructure, the information network and related R&T need permanent rational innovation

and security. Moreover, these services, when available, will comfort the confidence of the public vis-à-vis the national Institutions: the elimination of such services or infrastructure, would have a serious psychological impact on the population in addition to the physical dismantling of society. The translation of the European EPCIP directive to national law is therefore a great opportunity for all national partners, both public services and private companies. Particular attention should be given to certification of personnel and equipment, both for the protection of critical infrastructure in Belgium as for troops operating abroad. Military operations abroad are equally dependent on critical infrastructure, although other means of protection are used: preservation of supply and communication lines is essential to the success of operations for expeditionary forces.

Scientific studies were not discussed: numerous studies are ongoing, especially in the CIIP domain. The result of studies may contribute to appropriate legislation. In this context of military-civilian interaction, appeal may be made to the experience of "network centric capabilities" in operational areas: it can both enhance communication, but also promote "situation awareness". The growing importance of private partners deserves evenly more attention. Further research in these areas and the applicability in the field of stakeholders is needed.

The expectations of the Copenhagen Climate Conference (December 2009) were dulled. Migration flows, due to climate change, are one of the risks leading to armed conflict. The decision making process of this UN conference has made clear that the position of the EU was not considered to be at the same level as emerging powers (China, India, South Africa, Brazil) or the United States. The EU will therefore only be able to expect support if the aforementioned parties find themselves insured in their interest. The Climate Conference has demonstrated that hitherto neither the EU, nor the UN have a role to play in global governance. It is therefore essential that both at political and at military level, the organization of CIP/CIIP in the EU is

effectively tackled: the EU must be able to rely on her own resources. Besides the economic impact, CIP and CIIP also have security implications: an asymmetric enemy will always try to circumvent the strength of his opponent. Unlike national economic interests, and due to the globalization, security problems could also have serious consequences on the other side of the world. Therefore the optimization of security of our society remains essential. One can however assume that support in this context would only be delivered if tangible return on investment may be expected.

Map

The Royal High Institute for Defence (RHID)

The aim of the RHID is to provide analysis on international trends in various fields as such as political, military, technological, socio-economical and ideological issues. The RHID has the objective to become a think tank and a center of excellence in security and strategy.

Contact

Royal High Institute for Defence
Renaissance Av. 30
1000 Brussels
Website: http://www.mil.be/rdc
Email: irsd.conferences@mil.be
Phone: +3227426995

Access

Our offices are situated in the center of Brussels, near the Jubilee Park and the European institutions.

Subway : lines 1A et 1B (stations “Schuman” or “Merode”)

Bus (STIB) : line 63 (bus stop “Gueux”) – line 61 (bus stop “de Jamblinne de Meux”)