PROTECTING CRITICAL INFRASTRUCTURE IN THE EU

CEPS TASK FORCE REPORT

CHAIR	**BERNHARD HÄMMERLI** President, Swiss Informatics Society
RAPPORTEUR	**ANDREA RENDA** Senior Research Fellow, CEPS

CENTRE FOR EUROPEAN POLICY STUDIES
BRUSSELS

The Centre for European Policy Studies (CEPS) is an independent policy research institute in Brussels. Its mission is to produce sound policy research leading to constructive solutions to the challenges facing Europe. As a research institute, CEPS takes no position on matters of policy. The views expressed are attributable only to the authors in a personal capacity and not to any institution with which they are associated.

This report is based on discussions in the CEPS Task Force on Critical Infrastructure Protection. The members of the Task Force participated in extensive debates in the course of several meetings and submitted comments on earlier drafts of this report. Its contents represent the general tone and direction of the discussion, but the report's recommendations do not necessarily reflect a full common position reached among all members of the Task Force. A list of participants appears in Annex 1 at the end of this report.

ISBN: 978-94-6138-070-8

Centre for European Policy Studies
Place du Congrès 1, B-1000 Brussels
Tel: (32.2) 229.39.11 Fax: (32.2) 219.41.51
E-mail: info@ceps.eu
Website: www.ceps.eu

CONTENTS

List of Figures

List of Tables

FOREWORD

The emerging challenge of Critical (information) Infrastructure Protection (C(I)IP) has been recognized by nearly all member states of the European Union, following the pioneering experience of the United States. More generally, politicians are increasingly aware of the threats presented by radical political movements and terrorist attacks. Responses to these facts have been in line with the available resources and possibilities of each country, so that the UK, Sweden, Switzerland, the Netherlands, Germany, France and Italy for example, are already quite advanced in translating the C(I)IP challenge into measures, whereas other member states are lagging behind but trying to accelerate their own internal policy process in the direction of a mature C(I)IP policy.

In the international arena of this policy domain, Europe is still in search of a role to play. The EU is supporting the C(I)IP community with research projects, a first pan-European exercise and a unit in the European Commission DG Information Society, which supports the policy process very pro-actively. The European Commission is entrusted with the task of promoting awareness of this important topic, facilitating cooperation between member states, fostering the exchange of know-how and coaching the MS in their efforts. For all these tasks, trust and confidence are crucial: these, however, are properties that only develop with time and mutual cooperation. Efficiency and quality are necessary to use the scarce resources available in the most cost-effective way. Only with due attention to the issues of trust and efficiency can we set up a stable partnership with the potential to contribute to better policy-making. In all of this, the EC can contribute significantly to the acceleration of the overall process by steering the direction of the much-needed cooperation.

Since the most important factors in the whole picture – trust and confidence – grow with time and experience and cannot be the result of mere top-down commands by EU institutions, upfront regulation is very unlikely to work: on the contrary, helping the development of a community and a successful partnership between national governments is much more likely to succeed. Fortunately, the Commission can count on the past experience of some national governments that have adopted a similar ‘facilitating’ approach. This way of handling such a complex task avoids fear, uncertainty and obstruction and also generates excitement and followers for the good of all parties. In addition, suppliers and service providers must become allies of the EC and the national governments in order to keep up the pace of the evolving C(I)IP process. Furthermore, economic incentives should be given to support C(I)IP and to address social responsibility, i.e. enhancing preparedness and resilience while overcoming the tendency to focus exclusively on maximum economic corporate benefit.

Against this background, we highly recommend approaching C(I)IP as though it were analogous to civil emergency planning. The EU must generate successful cooperation, just as President Barroso did in August 2005, by announcing support to the firefighters in Portugal and sending aircraft from other member states (Italy, Greece, France and Spain). Such actions create good will and excitement, and help resolve the situation.

This report is the result of a collective effort by all participants of the Task Force. Without their support, their willingness to contribute and to engage in discussion, this work would never have seen the light of day. Therefore, I would like to express my deepest gratitude to all those who supported the CEPS Task Force, and especially to CEPS itself, to the Rapporteur Andrea Renda, and to Staffan Jerneck, Anne-Marie Boudou and Christopher Napoli, who organised the Task Force meetings and facilitated the exchange of information between participants. On behalf of the whole Task Force, I hope that this report will contribute to a faster, stronger and better coordinated C(I)IP policy both in Europe and in individual member states.

The Chairman of the Task Force

PROTECTING CRITICAL INFRASTRUCTURE IN THE EU

CEPS TASK FORCE REPORT

MAIN POLICY RECOMMENDATIONS

1. **A thorough subsidiarity test should be performed for each economic sector.** The increasing interdependence between infrastructures and between countries, as well as the inter-links between physical infrastructure and the information infrastructure create a compelling argument for the coordination of CIP policy at international level. The European Commission should thus perform a thorough subsidiarity test to identify areas where joint action is more desirable, and areas that may remain under national competence in C(I)IP policy. The test should be run for each of the economic sectors involved.
2. **One single EU top-level agency.** The EU must adopt an all-hazards approach by empowering – in line with a consolidated trend in many countries – a single agency to deal with CIP and CIIP issues. The agency's mandate should include both preparedness and response coordination, including an EU hotline for emergency management and early warnings.
3. **Increase policy and operational focus on resilience and preparedness.** The need to protect critical infrastructures (CIs), including critical information infrastructure (CII), must be fully understood by policy-makers, as awareness of this policy issue leads to a paradigm shift in the way we think about infrastructure policy-making.
4. **Build a long-term CIP strategy for EU.** The EU needs a forward-looking well defined strategy, and strong political commitment. The strategy should include key pillars such as the development of best practices, education exercises and training, the promotion of R&D and fostering information-sharing between public and private operators and suppliers. The fact that suppliers are often global players, while public policy-makers act at a local level, makes the policy dialogue more difficult and international coordination even more important.

5. **Foster trust between information-sharing partners.** Public-private-partnership (PPPs) are a good way to facilitate trusted information-sharing among the key EU stakeholders; however, given the unique challenge posed by the need to coordinate the approach across the EU 27, it needs to be carefully planned and orchestrated. It needs time, clear rules, sector-specific arrangements and sharing units of limited size: this issue needs to be addressed upfront and carefully in order to ensure successful international and EU-level cooperation.
6. **Develop common approaches for C(I)I risk assessment based on the ongoing production of data and relevant information.** The EU should promote the development and adoption of common risk metrics and standardized approaches for risk identification, assessment and management in the field of CIP. This cannot be an EU-level effort only, since it requires, inter alia, the constant production of data and statistics at national level. Without the availability of reliable data, a meaningful and thorough approach to CIP is not feasible.
7. **Adopt a 'new approach' for industry-government cooperation.** The EU should adopt a flexible approach to CIP policy, by establishing, through primary legislation, only the general principles and main outcomes sought through EU CIP policy, and leaving it to the industry to devise the best technical measures that fulfil the desired levels of resilience.
8. **Integrate CIP into the EU policy-making processes.** Impacts on CI resilience should be introduced as a mandatory step in the Commission's Impact Assessment system, whenever the policy issue in hand potentially affects, even indirectly, the resilience or vulnerability of CIs.
9. **Develop policy validation methodologies.** Methodologies to stress-test existing policies should be developed through public funding of *ad hoc* research projects. In particular, these projects should look at how to test interdependencies between CIs and potential cascading effects triggered by failures of given infrastructures, based on models or simulation games.
10. **Establish indicators and criteria for success.** Criteria and indicators to assess the outcomes of national and EU-wide information-sharing initiatives are needed, in order to allow the tracking of progress towards common, coordinated goals in CIP policy.

EXECUTIVE SUMMARY

The European Union and its member states face very unique challenges in critical infrastructure protection (CIP) policy. In the past few years, the European Commission has adopted a number of policy initiatives in this field, including Directives and Communications to promote the enhancement of preparedness, security and resilience. However, a number of outstanding problems remain. First, member states are at varying degrees of maturity with respect to the development of a comprehensive and effective CIP policy. Second, there are islands of cooperation across the EU member states but no overall concept of operations at the EU level. Third, partnerships and relationships are scattered across countries (each individual country has and will maintain unique relationships with private sector owner operators and global companies that enable them). Fourth, critical EU infrastructure is also scattered across many different countries.

Critical infrastructures (energy, communications, banking, transportation, public government services, etc.) are now more vital to industrialised economies. Citizens, businesses and governments all rely on an array of interlinked physical and information infrastructures to satisfy their needs and perform their daily operations. At the same time, these infrastructures are becoming increasingly interdependent, such that failure of one of them can often propagate and result in domino effects. Suffice it to recall the recent failures of the electricity grids in November 2006 in Western Europe, when a shutdown of a high-voltage line in Germany resulted in massive power failures in France and Italy, as well as in parts of Spain, Portugal, the Netherlands, Belgium and Austria, even extending as far as Morocco and affecting ten million customers in total. In addition, some of these infrastructures can also trigger cross-border effects, due to their inherently regional or global nature (as in the case of energy sources or the internet). This means that for some modern infrastructures, the failure to reach sufficient resilience standards in one country can have a detrimental effect on many others.

Infrastructures are becoming increasingly important in our economies, making risk issues as important as efficiency. This needs to be reflected in our economic policies

Recent episodes have highlighted the need for internationally coordinated CIP policy. But the current landscape is still very fragmented, also in the EU

Recent dramatic episodes, from 9/11 to the Madrid train bombings, the power cuts in North America in 2003, the April 2010 ash cloud, the Louisiana 2010 oil spill and the cyber-attacks in Estonia in 2007, have highlighted the need for a comprehensive, internationally coordinated policy for the protection of critical infrastructures. For the purposes of this report, we define critical infrastructure as infrastructure whose failure would result in substantial damage to society and/or the economy. The magnitude and heterogeneous causes of these events has led to the development of all-hazard approaches to policy in many countries, in order to account for both natural disasters and man-made attacks when conceiving prevention and remediation measures against the risk of infrastructure failure. With this in mind, several countries have put in place a policy for critical infrastructure protection (CIP) and also critical information infrastructure protection (CIIP). However, the landscape of these national policies is still very fragmented, and the same can be said for that of the EU, where the European Commission is still attempting to devise a more coordinated policy.

This report contains the opinions expressed by participants of the CEPS Task Force on Critical Infrastructure Protection as regards future policy directions in this topical and ever-more important field. There was agreement among Task Force participants that the EU can play a leading role in facilitating global cooperation. In particular, the European Public-Private Partnership for Resilience (EP3R) presents a key opportunity for Europe to engage the local and global industry players in guiding and reviewing important aspects of emerging cyber policy. This is likely to result in the application of effective policy levers, ensuring that emerging technologies are well addressed, and that there is alignment with other similar initiatives outside the EU. In this respect, Europe can also act as a model for the rest of the world.

The findings that emerged during Task Force meetings can be summarized as follows:

CIP policy features very peculiar economic problems, from externalities to rational ignorance and bounded rationality issues, all calling for public intervention

- *The need to protect critical infrastructure is real, and potentially determines a trade-off between (short-term) efficiency and resilience*, which must be addressed by policy-makers when making choices. The economics of CIP features important specificities, including the need to solve potential dilemmas identified in our report, such as the 'efficiency-security trade-off' and principal-agent problems. CIs often exhibit positive and negative externalities that lead to market failure. In addition, the CEPS Task Force debated the difficult role of liability and insurance, as well as behavioural problems related to rational ignorance and bounded rationality. All these issues call for a coordinated public-private action.

- *There is no way to organise a meaningful CIP policy without involving the private sector*, as CIs in Europe are mostly owned by private players, many of which are worldwide operating companies.
- *The key foundations of a CIP policy are a widely communicated vision and a forward-looking strategy, coupled with strong political commitment*. The key pillars are then the identification of gaps in the development of standards and best practices, strengthening education and training for the development of new professional skills in the CIP domain, the promotion and support of R&D for the development of improved CI protection technologies and methods, and information-sharing. Operationally, the key phases of the CIP cycle are often identified as follows: i) analysis and assessment; ii) remediation; and (iii) indications and warnings, before the adverse event occurs. In addition, they include iv) mitigation; v) incident response; and (vi) reconstitution, after the event (or succession of events) has occurred. Trust is a key dimension in any information-sharing exercise and should be addressed by CIP policy, knowing that building trust needs time, clear rules, sector-specific arrangements and limited group size.

- *At national level, CIP policy: i) focused on resilience and an all-hazards approach; ii) is centralised in a limited number of bodies; and iii) is inclusive of the cyber-dimension*. The role of critical information infrastructure and its relevance for CIP policy is on the increase, also leading to more interplay between cyber-security and CIP policy. The increasing reliance of physical Critical Infrastructures on ICT and the increasing importance of the internet and associated services to society and the economy gradually change the threat landscape. Increasingly, local CIs are affected by global cyber threats. In addition, our understanding of the causes of failure of (or attack to) infrastructure is still limited, in particular when it comes to infrastructure interdependency and cross-country effects. Finally, greater risk seems to be arising from unexpected and highly unpredictable causes (the so-called 'black swans' problem), which creates significant challenges, and may require even greater efforts in securing efficient mitigation and response.

There are structural biases between attack and defence in CIP: this calls for information-sharing and the promotion of common standards and metrics

- *There is a clear need for establishing a more holistic approach, a common taxonomy, metrics and a common risk management framework for CIP-related risks and threats*. Standardisation in this domain – also relying on existing standards from ISO, NIST and ANSI, for example, – would significantly improve the circulation of best practices and the development of a mature insurance market. Moreover, the production of data at national and sectoral level is crucial for the development of guidance on risk management and CIP for public and private authorities. Furthermore, in the area of security standards, where extensive work was already carried out by standard bodies as well as specific sectors like defence, health, and finance: recent surveys demonstrate that a comprehensive vision of security is still lacking, and technical standards do not often interact sufficiently with sector-specific models.
- *Different sectors have different needs when it comes to CIP policy*. For example, coupling national public-private-partnerships (PPPs) with a global partnership and intelligence centre in the financial sector would provide a compelling mechanism to increase the resilience of the financial infrastructure. However, global action is hampered by the heterogeneity of potential participants, as well as conflicting interests, diverging knowledge bases and high transaction costs. For

example, in the energy sector, security of supply, climate and environmental concerns and the need to secure the affordability of energy for residential and business customers form a peculiar 'trilemma' that must be solved by carefully accounting for all the interests and incentives at stake. In the IT sector, the impact of quickly evolving and emerging technologies must be assessed on the resilience of critical services and dependent critical infrastructures.

Against this background, EU member states are still pursuing fragmented C(I)IP policies, and there is still a significant lack of cooperation between national governments and EU institutions in setting up a coordinated emergency response to potential threats. In other words, the higher degree of risk to which we expose our daily activities is not mirrored by an increased response potential of EU institutions. Yet member states are indeed interdependent: even if the internet backbone is not evenly spread over the EU27, several critical infrastructures are cross-border infrastructures, and for those the weakest links – i.e. the countries with a weaker emergency response potential – affect the vulnerability of all countries. For example, if 26 out of 27 countries have sufficiently strong policies to protect the internet backbone or challenge the spread of malware, this is not enough to guarantee the resilience of the internet network in the EU. It takes no more than one country to disrupt the whole system and expose it to threats.

With this in mind, the policy recommendations of the CEPS Task Force are aimed at the future directions that EU policy should take as regards critical infrastructure protection. There was agreement among Task Force participants that the EU can play a leading role in facilitating global cooperation. In particular, the European Public-Private Partnership for Resilience (EP3R) presents a key opportunity for Europe to engage the local and global industry players in guiding and reviewing important aspects of emerging cyber policy. This is likely to result in the application of effective policy levers, ensuring that emerging technologies are well addressed, and ensuring alignment with other similar initiatives outside the EU. In this respect, Europe can also act as a model for the rest of the world.

In particular, we recommend the following actions at the EU level:

- The European Commission should perform a thorough subsidiarity test to clearly identify areas where acting jointly is more desirable, and areas that may remain under national competence in C(I)IP policy. The test should focus on available policy options in each sector and for the overall governance of the system, including the creation of a European institute for the coordination of CIP and CIIP in Europe, or the creation of an EU early-warning centre.

- The EU must adopt an all-hazards approach by empowering – in line with a consolidated trend in many countries – a single agency to deal with CIP and CIIP issues; and launching an EU number for emergency management and early warnings, operated by the same agency.
- The EU should promote the development and adoption of common risk metrics and standards for risk identification, assessment and management in the field of CIP. This will enable a broader choice of incentives to improve CIP, will contribute to the greater availability of data and possibly also to a more mature insurance market.
- The EU should adopt a flexible approach to CIP policy, by establishing through primary legislation only the general principles and main outcomes sought through EU CIP policy, and leaving it to the industry to devise the best technical measures that fulfil the desired levels of resilience.
- Impacts on CI resilience should be introduced as a mandatory step in the Commission’s Impact Assessment system, whenever the policy issue at hand potentially affects, even if indirectly, the resilience or vulnerability of CIs.
- Methodologies to test existing policies with respect to CIP goals should be developed through public funding of *ad hoc* research projects. In particular, these projects should look at how to model interdependencies between CIs and potential cascading effects triggered by failures of given infrastructures based on models or simulation games.
- Models of interdependency between CIs and potential cascading effects triggered by failures of given infrastructures have already been researched to a certain degree. However, a more detailed analysis should be performed, including a technology assessment of new and upcoming technologies.
- Clear goals and success indicators to assess the outcomes of national and EU-wide information-sharing initiatives are needed, in order to enable progress tracking towards common, coordinated goals in CIP policy.

1. INTRODUCTION: A PARADIGM SHIFT?

In recent decades, our lives have become increasingly dependent on a number of pieces of infrastructure, ranging from physical assets – such as roads or the electricity grid – to the networked environment –such as financial services, or the internet.[1] We perform many activities and satisfy many of our primary needs thanks to these types of infrastructure: relying on critical infrastructure allows us to act more economically and efficiently. This also means, however, that the disruption of infrastructure may damage our economies substantially and lead to natural disasters and loss of human life. Suffice it to recall the recent failures of the electricity grids in November 2006 in Western Europe, when a shutdown of a high-voltage line in Germany resulted in massive power failures in France and Italy, as well as in parts of Spain, Portugal, the Netherlands, Belgium and Austria, and even extended as far as Morocco, affecting ten million customers in total.[2] Similar major blackouts, with even more severe consequences occurred in the summer of 2003 in the United States, Canada and in Italy, for various reasons.[3] Recently, the explosion at the Deepwater Horizon oil platform in the Gulf of Mexico on 20 April 2010, resulted in the massive, ongoing leak of underground oil.[4] Likewise, air travel disruptions caused

[1] See, inter alia, Ivo Bouwmans, Margot P.C. Weijnen and Adrian Gheorghe, *Infrastructures at Risk*, in A.V. Gheorghe, M. Masera, M Weijnen and De L. Vries (2006), "Critical Infrastructures at Risk", Springer Netherlands, (2006), pp. 19-36.

[2] Laprie *et al.* (2008), *Modelling Interdependencies between the Electricity and Information Infrastructures:* http://arxiv.org/ftp/arxiv/papers/0809/0809.4107.pdf

[3] Idem, quoting US-Canada, "Power System Outage Task Force — Final Report on the 14 August 2003 Blackout in the United States and Canada: Causes and Recommendations," (2004). And P. Pourbeik, P. S. Kundur and C. W. Taylor, "The Anatomy of a Power Grid Blackout," IEEE Power & Energy Magazine, September/October issue, pp. 22-29, (2006).

[4] See Los Angeles Times, *Gulf Oil Spill: Katrina on Obama Administrations' mind, 2* May 2010, by Paul Harris, at http://latimesblogs.latimes.com/greenspace/2010/05/katrina-on-obama-administrations-mind-in-oil-spill-response.html.

by the eruption of Iceland's Eyjafjallajökull volcano cost nearly $5 billion in global GDP, according to a report from Oxford Economics.[5]

Against this background, several governments around the world have concluded that infrastructures that are considered to be 'critical' are increasingly vulnerable and interdependent with other critical infrastructures. The relevance of some infrastructures for the continuity of government, for business operations and for the supply of basic services to citizens has become so high that a disruption of any of these fundamental assets can cause considerable damage. And the risk is significant. For example, the World Economic Forum estimated in 2008 that there is a 10-20% probability of a major breakdown of the critical information infrastructure in the next ten years, with a potential global economic cost of approximately $250 billion.[6] The macroeconomic costs of a major disruption to Switzerland, for example, with an annual GDP of CHF 482 billion, are estimated to be CHF 6 billion, i.e. 1.2% of GDP.[7]

Examples are manifold, and increasingly include threats from the internet world – as was seen in the now famous cyber-attack on Estonia in 2007. To give an idea of the magnitude of current exposure to threats of cyber-attacks, a recent study estimated that the cost of 24 hours of downtime as a result of a cyber-attack on critical infrastructure averages at US$ 6 million per day, with the peak being reached in the oil and gas sector ($8.4 million) and the lowest average amount in the water and sewage sector. The estimated cost of cyber-attacks was thought to be US$ 1.75 billion yearly – but this estimate does not take into account the opportunity cost borne by businesses that experience denials of service. According to an OECD report on "Malicious software", the estimated annual loss to US businesses caused by malware is USD 67.2 billion.[8] Currently, no such

[5] See the Oxford Economics report, *The Economic Impact of Air Travel Restrictions due to Volcanic Ash,* available online at http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/aktuell.parsys.87229.DownloadFile.tmp/economicimpactsofvolcanoinisland2010.pdf.

[6] See *Global Risks 2008. A Global Risk Network Report,* available online at http://www.weforum.org/pdf/globalrisk/report2008.pdf.

[7] The US Business Roundtable in 2007 suggested that the economic costs of a month-long internet disruption to the US alone could be more than $200 billion.

[8] See OECD, *Malicious software (Malware): A Security Threat to the Internet Economy,* Ministerial Background Report, DSTI/ICCP/REG(2007)5/FINAL, at: http://www.oecd.org/dataoecd/53/34/40724457.pdf. The estimate however

estimates are available for the EU or for the majority of EU member states. This lack of data makes it more difficult to both frame the issues and provide a deeper analysis of the challenges faced by the EU.

An important development highlighted by many governments and field experts is that critical infrastructures have become increasingly mutually dependent.[9] This means than a denial of service in, say, the energy sector can have immediate repercussions for many other infrastructures, from the financial services networks to the internet, gas and transportation networks, generating a cascading effect that ultimately harms society exponentially. For example, the Canadian government reported that:

> … during the 1998 Ice Storm, large segments of rural and urban communities were in the dark and without heat. Traffic and street lights were out. Banking and government services were interrupted. The disruption in one sector – electricity – affected a score of others, interrupting the delivery of important services upon which Canadians depend.[10]

comes from the US Government Accountability Office, United States Government Accountability Office (2007), *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, available online at: http://www.gao.gov/new.items/d07705.pdf.

[9] More precisely, infrastructures can either be independent, dependent, or mutually dependent. An independent infrastructure is one that in principle is isolated from the risks associated with other infrastructures. A dependent infrastructure is one that relies on another infrastructure (but not vice versa). Last, mutually dependent infrastructures depend on each other, with a successful attack to either resulting in damage to both. The growing interdependence of infrastructures has been confirmed by many Task Force participants. As an example, in a survey completed in 2008 by Secure Computing, when asked about the interconnection of control networks and corporate networks, over 60% of the 199 respondents said their networks were already interconnected and 98% said that interconnection increased their security risks. See Nicholson (2008), at http://www.securecomputing.com/pdf/IDCEnergyCybersecurity.pdf.

[10] Public Safety Canada, February 2008.

Box 1. Interdependence and resilience during 9/11

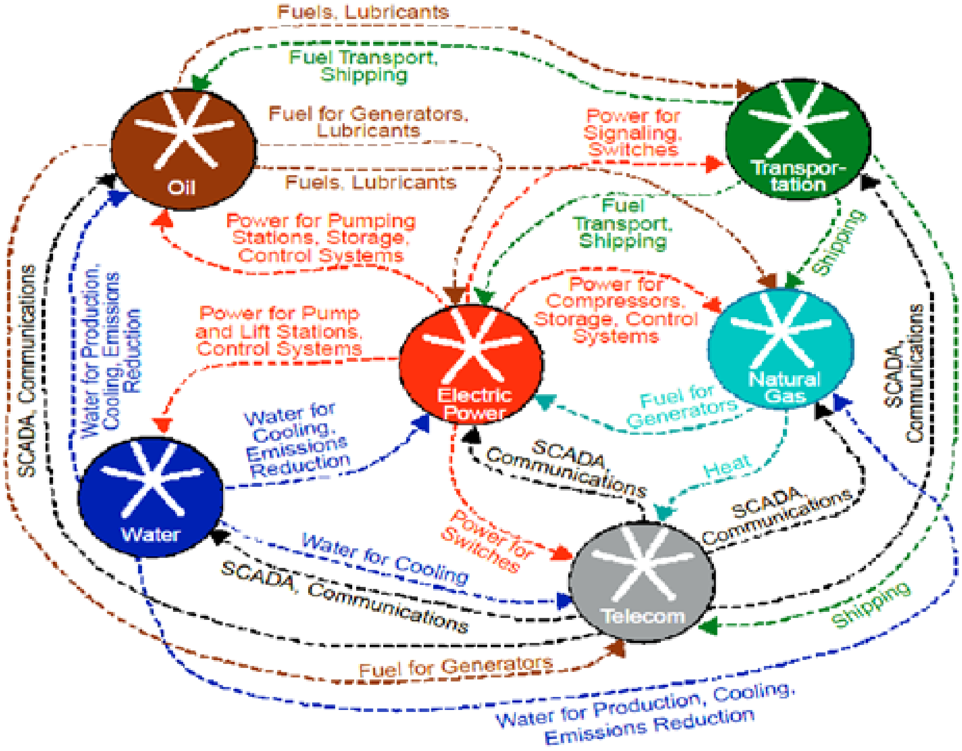
Cukier et al. (2005) offer an interesting reading of what happened on September 11, 2001:[1]

> *"After the second plane crashed into the South Tower at 9:02 am, telephone calls increased up to ten times the normal traffic volume – so much congestion that only a handful could get through. Major news Web sites – CNN, the BBC, The New York Times and others – were so clogged with traffic they became temporarily unreachable. By 9:39 am many radio stations in the city went dark (most broadcasters had transmitters on the towers). When the first tower collapsed at 10:05 am, and then the second at 10:28 am, they destroyed a vast amount of telecom infrastructure in the vicinity, complicating communications even more.*
>
> *To be sure, in many instances the systems proved resilient. For instance, network technicians struggling to repair systems coordinated their activities using mobile text messages since their cell phones couldn't handle calls. And as many noted afterwards, the internet worked when the phone system didn't. Indeed, at 9.54 pm the Federal Emergency Management Agency alerted all stations to prepare in case primary communications methods failed – and did this, ironically, by email.*
>
> *But here is the nub: as bad as all this sounds, the actual event did not do too much damage to the information infrastructure – yet subsequent problems with other networks began to cause havoc. For instance, a fire at a building on the periphery of the World Trade Center knocked out a power station upon which telecoms equipment elsewhere depended. A falling beam from an unstable building in the vicinity crashed into an operator's central switching office, damaging the machines. By late evening, systems that had survived went down simply because they overheated. And telecom services were disrupted when backup generators ran out of fuel because trucks carrying new provisions were blocked from entering lower Manhattan.*
>
> *In short, the incident highlights both the vulnerability and resilience of information infrastructure – and importantly, its interdependence with other infrastructures. For instance, the communications network is dependent on the electrical grid; the back-up generators are dependent on the roadway network. And of course, it bears noting, that the target of the attack in New York was not communications infrastructure at all, but two office buildings. What might have been the consequences if critical information infrastructure had been targeted as well?"*

attacks and their potential relevance for critical infrastructures, such as financial services, power grids, telecoms, and government and business continuity.

[11] See Luiijf *et al.*, *Critical (information) infrastructure protection in the Netherlands*, at http://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-1.pdf.

Figure 1. Example of interdependencies between sectors


Fuels, Lubricants
Fuel Transport, Shipping
Fuel for Generators, Lubricants
Fuels, Lubricants
Power for Signaling, Switches
Oil
Transportation
Power for Pumping Stations, Storage, Control Systems
Fuel Transport, Shipping
Shipping
Power for Pump and Lift Stations, Control Systems
Power for Compressors, Storage, Control Systems
SCADA, Communications
Water for Production, Cooling, Emissions Reduction
Electric Power
Natural Gas
SCADA, Communications
Fuel for Generators
Water for Cooling, Emissions Reduction
SCADA, Communications
Heat
Water
SCADA, Communications
Power for Switches
Water for Cooling
SCADA, Communications
Telecom
Shipping
Fuel for Generators
Water for Production, Cooling, Emissions Reduction

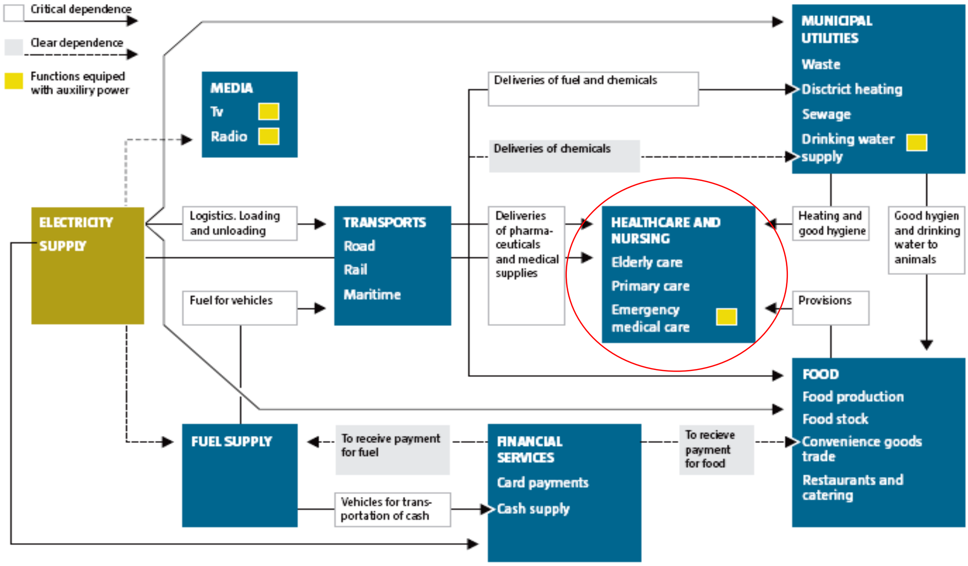
Source: Rinaldi et al. (2001).

Critical infrastructures are even more interdependent in the context of the EU Single Market – consider the ongoing deployment of trans-European networks (TENs):[12] however, the increased integration of the economies of the EU 27 is not mirrored by a significant coordination of national CIP policies to date, despite significant efforts devoted to this task by the European Commission. On the contrary, national policies for CIP are very fragmented. If a successful attack or any other discontinuation of service happened now, there is no way to call ‘Europe’, i.e. an EU-wide European crisis reaction centre. No single contact point exists, and there is no coordinated response to any potential threat either. This has become a

[12] See http://ec.europa.eu/ten/index_en.html.

very pressing problem, especially as calls for more pan-European infrastructures are mounting.[13]

Figure 2. Example of propagation chain for the electricity network



Source: Gustavsson (2010).

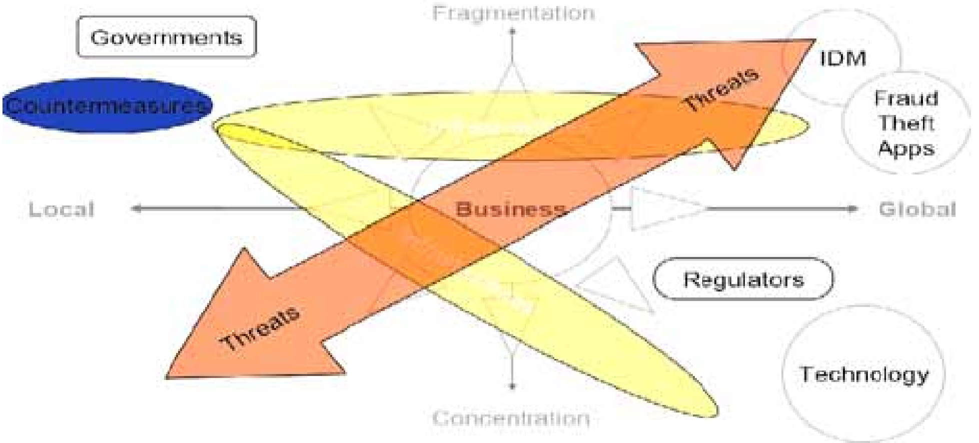
Furthermore, the waves of privatisation and market liberalisation have made the protection of critical infrastructure more difficult to achieve by government alone, as most of the critical infrastructures (approximately 85%) are owned by the private sector. Since private suppliers are growing in importance, especially in the ICT field, they must be kept in the picture when designing a policy for CIP. This also means that, without adequate collaboration between public and private sector representatives, no effective CIP policy can be put in place.

As shown during Task Force meetings, critical infrastructures – once only local and fragmented – are increasingly global. In addition, they are becoming more concentrated. However, the policies in place to remedy the increased vulnerability of infrastructures are still eminently local. Because of this, regulators need to coordinate better at a global level. Actions,

[13] See the Trans-European Networks (TENs) agenda, and also the recent Monti Report on the future of the Single Market, pp. 64-66, at: http://ec.europa.eu/bepa/pdf/monti_report_final_10_05_2010_en.pdf.

however, tend to remain local due to enforcement, jurisdiction, and capacity issues. In this respect, what might be termed a 'glocal' strategy, *i.e.* a circuit of globally coordinated local regulators, is needed.

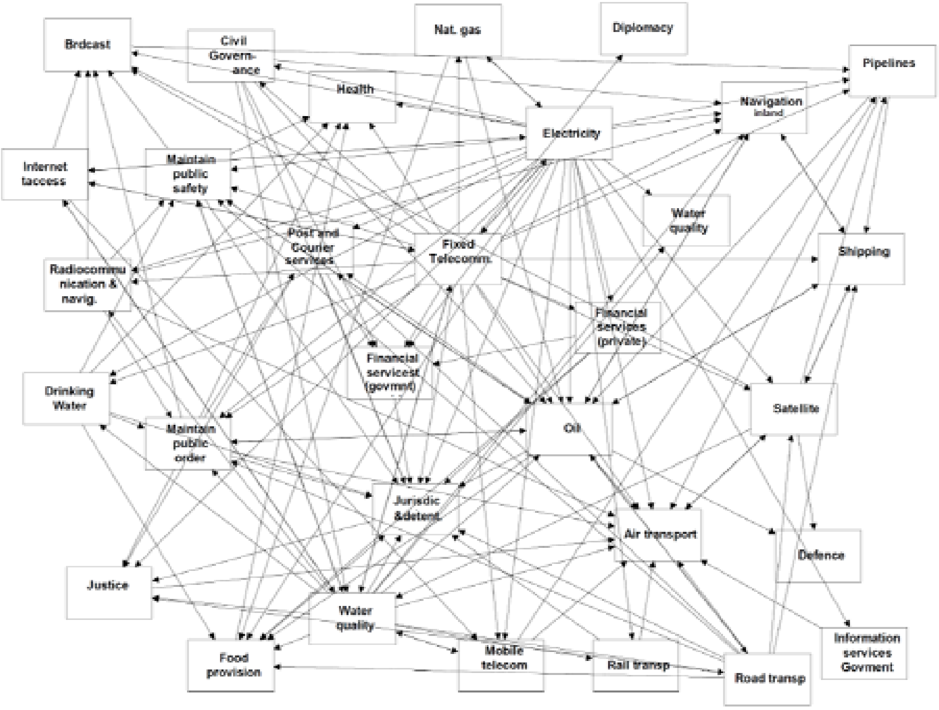
Figure 3. Threats and remedies in current CIP policy



Source: Gresser (2010), the PARSIFAL project.

Faced with this problem, EU member states are still pursuing fragmented C(I)IP policies, and there is still a significant lack of cooperation between national governments and EU institutions in setting up a coordinated emergency response to potential threats. Put another way, the higher risk to which we expose our daily activities is not mirrored by an increased response potential on the part of the EU institutions. And this is even more important if we think that member states are indeed interdependent: even if the internet backbone is not evenly spread over the EU27, several critical infrastructures are cross-border infrastructures, and for those the weakest links – i.e. the countries with a weaker emergency response potential – affects the vulnerability of all countries. For example, if 26 out of 27 countries have sufficiently strong policies to protect the internet backbone or challenge the spread of malware, this does not guarantee the resilience of the internet network throughout the EU. It takes no more than one country to disrupt the whole system and expose it to threats. This reasoning applies increasingly to the global level, and potentially calls for cooperation even beyond EU borders. Failing to achieve this goal also means increasing the likelihood of a successful attack.

Figure 4. Interdependencies



Source: Luiijf et al. (2008).

In more detail, the challenge of protecting critical infrastructure has the following features:[14]

- **Private and public.** The actors are many, and most infrastructures are private. The state can no longer ensure security and must rely on information-sharing with other actors involved. A well-conceived public-private partnership is thus needed and crucial to the success of any CIP policy.
- **Unbounded.** Specifically in the case of Critical Information Infrastructures (CIIs), there are no physical barriers or political boundaries. Identifying who is responsible for what in terms of security policies and attributing malicious activity is a challenging task.

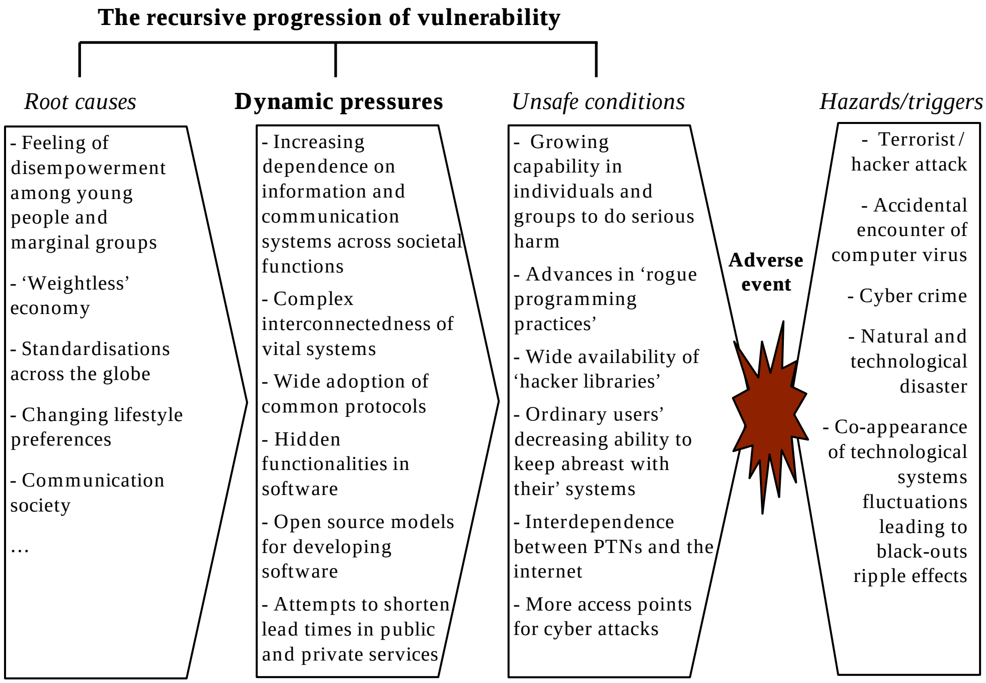
[14] Presentation by Roberto Filippini (European Commission Joint Research Centre), at the second meeting of the CEPS Task Force, CEPS, Brussels.

- **Networked**. Critical infrastructures are an increasingly large-scale, open network, time-dependent and dynamically evolving environment. The size and number of interconnections may increase in response to the demands of various actors.
- **Complex.** Critical infrastructures are complex: simplifications necessary to master the security problem and operate the systems may neglect states that can manifest suddenly (by surprise) with unpredictable consequences. This problem is exacerbated by the fact that simply decomposing the problem by *divide et impera* strategies does not work. Issues that create or increase complexity include the fact that large networks are inherently unstable;[15] the fact that local disruptions may have an impact on many countries; the fact that global legal frameworks and institutions are lacking; and the huge administrative burden faced by global players with multinational presence when responding to fragmented national CIP policies.
- **Human.** Critical infrastructures depend on human decisions and sufficiently knowledgeable and educated experts. In this respect, knowledge of ordinary tasks may become inadequate to face emergencies.
- **Vulnerable**. Vulnerabilities are in all infrastructures and may expose sensitive information that can be exploited by attackers. Attackers that have been targeting CI for a long period (military) are increasingly using the cyber space.

Figure 4 below – from Hellström (2007) – provides a view of the vulnerability problem and existing trends in CIP in terms of the root causes of potential adverse events of critical infrastructure; dynamic pressure exerted by changing patterns of production or consumption, and increasingly unsafe conditions in the cyber-world. The analysis applies, as a matter of fact, to all infrastructures – and only *a fortiori* to critical ones. When all sectors become regionally or globally interconnected, a first challenge is to sort out the critical infrastructures from the other types of infrastructure.

[15] See Gardner & Ashby (1970), *Connectance of Large Dynamic (Cybernetic) Systems: Critical Values for Stability*, Nature 228, 784 (21 November 1970); doi:10.1038/228784a0. And May, R. M. (1972). *Will a large Complex System be Stable?*, Nature 238, 413-414. 1974. Stability and Complexity in Model Ecosystems. New Jersey: Princeton University Press.

Figure 5. The progression of infrastructure vulnerability

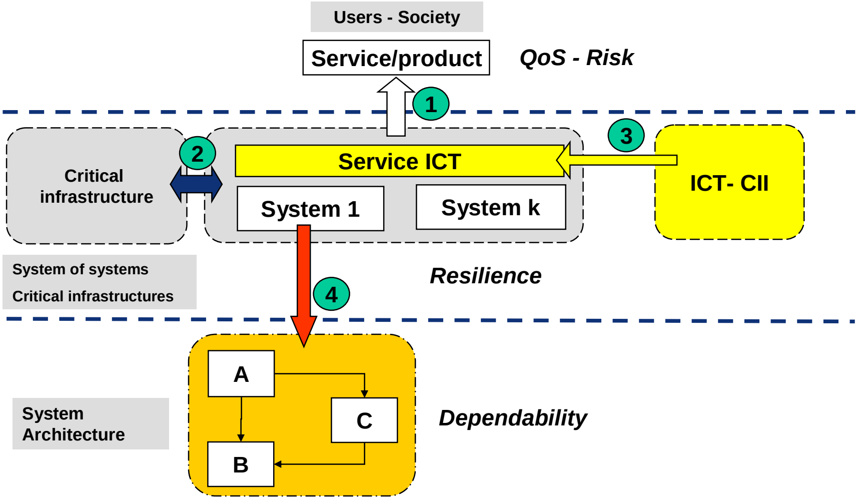

The recursive progression of vulnerability
Root causes
Dynamic pressures
Unsafe conditions
Hazards/triggers
- Feeling of disempowerment among young people and marginal groups
- 'Weightless' economy
- Standardisations across the globe
- Changing lifestyle preferences
- Communication society
…
- Increasing dependence on information and communication systems across societal functions
- Complex interconnectedness of vital systems
- Wide adoption of common protocols
- Hidden functionalities in software
- Open source models for developing software
- Attempts to shorten lead times in public and private services
- Growing capability in individuals and groups to do serious harm
- Advances in 'rogue programming practices'
- Wide availability of 'hacker libraries'
- Ordinary users' decreasing ability to keep abreast with their' systems
- Interdependence between PTNs and the internet
- More access points for cyber attacks
Adverse event
- Terrorist/ hacker attack
- Accidental encounter of computer virus
- Cyber crime
- Natural and technological disaster
- Co-appearance of technological systems fluctuations leading to black-outs ripple effects

Source: Hellström (2007).

Finally, there is a growing cross-border dimension in critical infrastructure protection, which becomes even more visible in the case of information infrastructure. Figure 5 below shows a typical case of cross-border negative externalities, which couples the increased interdependency between infrastructures with the increased interdependency between countries.[16] The current development of CIP policies has led to advancements in the understanding of "type 1" problems, i.e. the causes of failure of a given infrastructure due to a fault in a single component. However, the dynamics with which the failure propagates to other critical infrastructures ("type 2"), the impact of faults in ICT on critical infrastructures ("type 3") and the inter-state propagation of failures ("type 4") are little known today.

[16] Presentation by Roberto Filippini (JRC, European Commission) at the 2nd meeting of the CEPS Task Force, CEPS, Brussels.

Figure 6. Cross-border interdependencies



Source: Filippini (2010).

This report explains how the goal of protecting critical infrastructure – including critical information infrastructure – can be reconciled with the current architecture of EU policy-making, and be made more pervasive in the daily operations of EU institutions. In addition, we explore how increasingly global threats can effectively be dealt with through essentially local (but coordinated) measures. Section 2 below introduces CIP policy in more detail and discusses the national and EU initiatives in this field in more detail. Section 3 introduces the economics of CIP and explores the pending issues in developing a consistent and efficient CIP policy in Europe, ranging from the need to ensure cooperation between member states and national emergency response teams, to the need to shape an effective public-private partnership, and also to the need to develop an ontology and metric structure for risk assessment and management. Section 4 illustrates the results of the CEPS Task Force in terms of how to address the main policy challenges in this field. We then summarize all the policy recommendations from the CEPS Task Force in a concluding chapter.

CHAPTER 1: MAIN FINDINGS

- Businesses, government and society are increasingly dependent on infrastructure, some of which are critical for the functioning of our economy: their disruption may cause major social disturbance and even lead to substantial loss of life or life-years.
- Critical infrastructures are increasingly dependent on each other and partly interdependent, and the information infrastructure is increasingly interlinked with nearly all other infrastructures, including both critical and non-critical infrastructure. Accordingly, isolating critical from non-critical infrastructure is a challenge.
- Our understanding of the causes of failure or attack to infrastructure is still limited, in particular when it comes to infrastructure (inter)dependency.
- Countries are becoming increasingly dependent on CIs, and the understanding of cross-country (inter-)dependencies must be improved.
- EU member states have fragmented and often uncoordinated CIP policies: there is no way to 'call the EU' in case of emergency. To achieve the power and efficiency of coordination, CIP policies should be strengthened in years to come and look at ways to deal with the fragmentation of most infrastructures, as well as at the fragmentation of current national policies.
- A meaningful CIP policy is not possible without involving the private sector, as CIs are mostly owned by private players.

2. Critical infrastructure protection: Basic facts and existing policies

Defining critical infrastructures and distinguishing them from other infrastructures is a key challenge for policy-makers, and one that has been addressed in different ways by national governments. The challenge is made even greater by the fact that the concept of critical infrastructure is an evolving and dynamic one – think about the growing importance of the internet, which may warrant an inclusion of (parts of) this infrastructure in the list of CIIs. Section 2.1 below discusses the extent to which existing definitions diverge at national level, while Section 2.2 highlights the 'moving frontier' between CIP and the protection of critical information infrastructure. Section 2.3 describes the role of the key players that operate in the CIP context, whereas Section 2.4 contains an illustration of the life cycle of CIP and the related policy actions. Finally, Section 2.5 provides an overview of the recent EU policy actions in this domain.

2.1 Defining and scoping critical infrastructures

Several definitions of critical infrastructure exist in the literature and in official policy documents. The European Commission defines critical infrastructures as:

> [A]n asset, system or part thereof located in member states that 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 on a member state as a result of the failure to maintain those functions.[17]

The OECD has recently given two definitions of the term "critical" and "infrastructure", which attempt to reconcile the various definitions given in the OECD member states. According to this definition:[18]

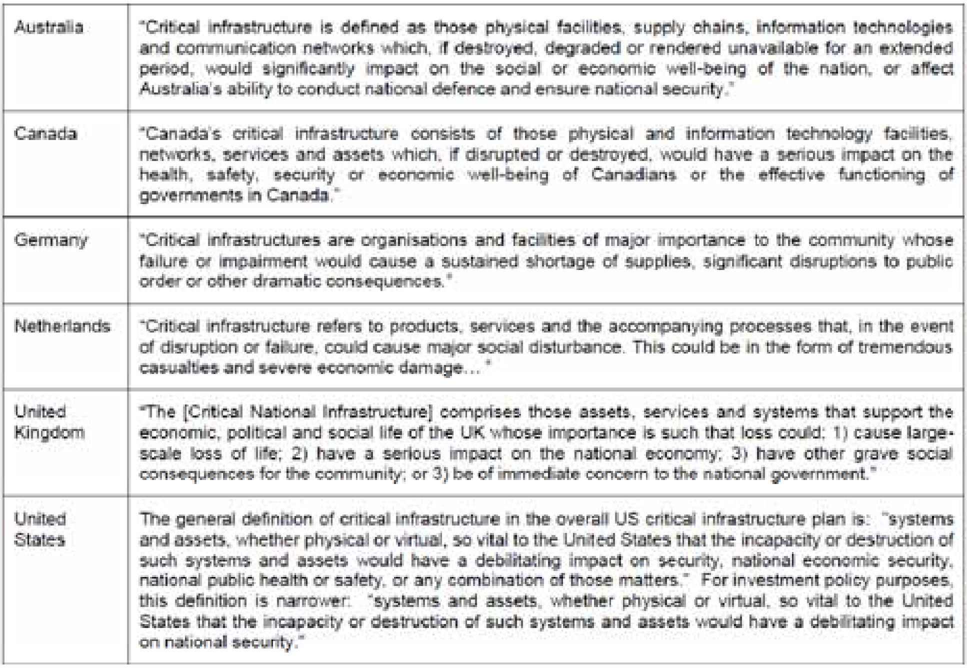
[17] European Council Directive 2008/114/CE.

[18] See http://www.oecd.org/dataoecd/2/41/40700392.pdf

- The term "**critical**" refers to infrastructure that provides an essential support for economic and social well-being, for public safety and for the functioning of key government responsibilities, such that disruption or destruction of the infrastructure would result in catastrophic and far-reaching damage.
- National definitions of "**infrastructure**" refer to physical infrastructure and often also intangible assets and/or to production or communications networks. These definitions are very broad, certainly broader than the notion of infrastructure commonly used in other fields of policy (e.g. the "essential facility" notion in competition law) and end up including not only the tangible assets, but also the intangibles that run with them (e.g. software, services, etc.).

Against this background, the definition of critical infrastructures is still a moving target. Table 1 below shows the definitions adopted in a number of countries, revealing important differences in the way the issue is addressed at the policy level.

Table 1. Definitions of critical infrastructure in selected countries

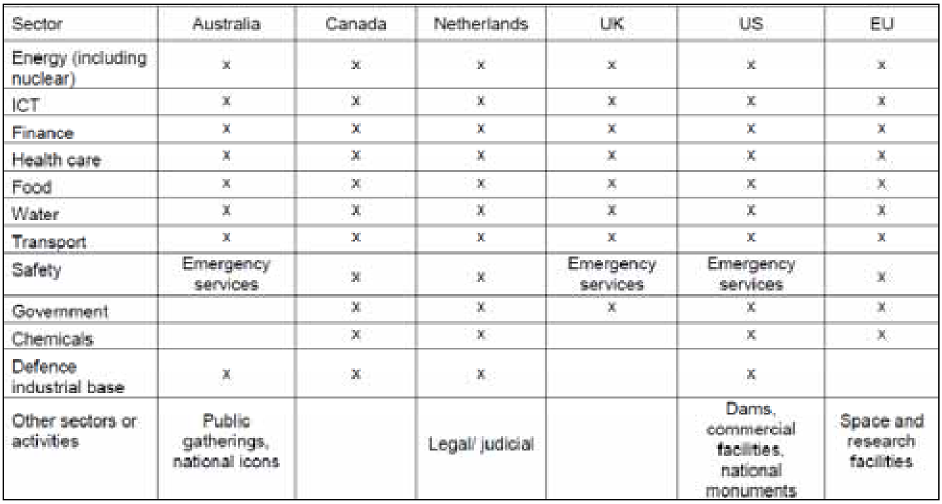


Australia	"Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security."
Canada	"Canada's critical infrastructure consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada."
Germany	"Critical infrastructures are organisations and facilities of major importance to the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences."
Netherlands	"Critical infrastructure refers to products, services and the accompanying processes that, in the event of disruption or failure, could cause major social disturbance. This could be in the form of tremendous casualties and severe economic damage… "
United Kingdom	"The [Critical National Infrastructure] comprises those assets, services and systems that support the economic, political and social life of the UK whose importance is such that loss could: 1) cause large-scale loss of life; 2) have a serious impact on the national economy; 3) have other grave social consequences for the community; or 3) be of immediate concern to the national government."
United States	The general definition of critical infrastructure in the overall US critical infrastructure plan is: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." For investment policy purposes, this definition is narrower: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security."

Source: OECD (2008).

Table 2 below shows the different sectors that are covered by national CIP plans. Here too, several commonalities can be identified, together with some minor differences in scope as regards safety, government, chemicals, the industrial defence base and other sectors.

Table 2. Sectoral coverage of national CIP plans



Sector	Australia	Canada	Netherlands	UK	US	EU
Energy (including nuclear)	x	x	x	x	x	x
ICT	x	x	x	x	x	x
Finance	x	x	x	x	x	x
Health care	x	x	x	x	x	x
Food	x	x	x	x	x	x
Water	x	x	x	x	x	x
Transport	x	x	x	x	x	x
Safety	Emergency services	x	x	Emergency services	Emergency services	x
Government		x	x	x	x	x
Chemicals		x	x		x	x
Defence industrial base	x	x	x		x	
Other sectors or activities	Public gatherings, national icons		Legal/ judicial		Dams, commercial facilities, national monuments	Space and research facilities

Source: OECD (2008).

2.2 CIP and CIIP: A moving frontier

One interesting aspect of the current debate on critical infrastructure protection is whether and to what extent critical information infrastructure (CII) should be considered as a specific province within the generic umbrella term CI. As explained by Brunner and Suter (2008),

> [M]ore than ten years after the beginning of the CIP debate, there still is little clarity with regard to a clear and stringent distinction between the two key terms ‘CIP’ and ‘CIIP’. In official publications, the term CIP is frequently used even if the document is only referring to the information aspects of the issue.[19]

[19] Brunner, E. and M. Suter, *International CIIP Handbook 2008/2009*, available online at http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=91952&lng=en.

Overall, it is widely acknowledged that CIIP can be seen as a subset of CIP, albeit essential for the purposes of infrastructure protection.

Critical Information Infrastructure (CII) generally refers to Information and Communication Technology systems that are essential to operations of national and international Critical Infrastructures. Examples include i) telecommunication networks, management, location-based services for emergency calls; ii) transportation: air traffic control, train routing and control, traffic management; iii) financial services: credit card transactions, settlement systems, transaction records, electronic stock/bond trading; and iv) control systems/SCADA (Supervisory, Control and Data Acquisition) to manage energy production and distribution, chemical manufacturing and refining processes. In a recent OECD recommendation, CII was defined as referring to:

> those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy.

CIIs can include i) information components supporting critical infrastructures; ii) information infrastructures supporting essential components of government business; and/or iii) information infrastructures essential to the national economy. Another widely accepted definition of CII is:

> communications or information service[s] whose availability, reliability and resilience are essential to the functioning of a modern [national] economy, security, and other essential social values.[20]

As recently observed:

> all critical infrastructures (transportation, finance, electric power, water, etc.) are increasingly dependent on the evolving information infrastructure – the public telephone network, the internet, and terrestrial and satellite wireless networks – for a

[20] See Cukier, K., *Ensuring (and Insuring?) Critical Information Infrastructure Protection: A Report of the 2005 Rueschlikon Conference on Information Policy*", at http://www.rueschlikonconference.org/pressdocs/56_R_05_Report_Online.pdf

> variety of information management, communications, and control functions.[21]

The meetings of the CEPS Task Force confirmed that many of the key concerns expressed by industry representatives in specific sectors of the economy (including finance and energy) are intimately related to the growing importance of the information infrastructure entangled with the traditional physical infrastructure. For example, theft of financial data and disruption of electrical and/or smart grids through cyber attacks are among the key concerns of stakeholders from the respective sectors.

The fact that boundaries between CIP and CIIP are increasingly blurred is also testified by recent accidents. For example, in March 2007 an experiment (*the Aurora Generator Test*) conducted by the Idaho National Labs in the US demonstrated that a large diesel generator could be severely damaged by exploiting a computer vulnerability, revealing that physical damage could be done through the computer system. As reported also by PwC (2010), "the results of this test elevated the cyber attack threat to a new level. Prior to conducting the test, utility companies had focused primarily on protecting their physical assets from more conventional attacks".[22] The same applies to recent news that in April and June 2009 Russian and Chinese spies had penetrated the US electrical grid and that the North American Electric Reliability Corporation (NERC) was teaming with a defence contractor to create an initiative to evaluate power companies' ability to withstand cyber attacks.[23] The NERC eventually accepted 83 standards for security of the electrical grid, condensed them into eight CIP standards and empowered the Federal Energy Regulatory Commission (FERC) to oversee their implementation.[24] However, there has

[21] See the *National Academic Press* article at: http://www.nap.edu/catalog.php?record_id=10685

[22] See Price Waterhouse Coopers, *Cyber Attacks: is your Critical Infrastructure Safe?*, at: http://www.pwc.com/en_US/us/industry/utilities/assets/cyber-attacks.pdf.

[23] Idem. NERC is the North American Electric Reliability Corporation, a self-regulatory organisation, subject to oversight by the US Federal Energy Regulatory Commission and governmental authorities in Canada, whose mission is to ensure the reliability of the bulk power system in North America.

[24] See, inter alia, The Project Grey Goose Report on Critical Infrastructure, February 2010, at http://dataclonelabs.com/security_talkworkshop/papers/25550091-Proj-Grey-Goose-report-on-Critical-Infrastructure-Attacks-Actors-and-Emerging-Threats.pdf. The Federal Energy Regulatory Commission (FERC) is the US federal

been criticism that the standards identified do not go far enough, and a more comprehensive approach to risk and security in this domain would be needed.[25]

Furthermore, the transition towards smart electric grids highlights the increasing interdependencies between physical and electronic infrastructures. As described, by Anderson and Fuloria (2010), among others:

> the EU is strongly encouraging its 27 member states to replace utility meters with 'smart meters' by 2022 … Yet it is not at all clear what it means for a meter to be secure … there are at least half-a-dozen different stakeholders with different views on security – which can refer to information, to money, or to the supply of electricity.[26]

A similar rationale can be applied to cloud computing, to name one emerging sector.[27]

A more controversial issue is whether the internet should be considered as a CII. In this respect, the CEPS Task Force observed that although society's reliance on internet services, including e-commerce, telecommuting, communication, remote control and diagnostics is growing and a major internet outage can have a significant economic impact, the internet is not considered a CII.[28] However, many CIIs, especially control and communication systems are increasingly connected to the internet and rely on public online services, which can make them vulnerable to cyber attacks. Furthermore, with an increasing number of high-value services available through the internet and the accelerating shift towards perimeter-

agency with jurisdiction over interstate electricity sales, wholesale electric rates, hydroelectric licensing, natural gas pricing, and oil pipeline rates. FERC also reviews and authorises liquefied natural gas (LNG) terminals, interstate natural gas pipelines and non-federal hydropower projects.

[25] See the Critical Infrastructure blog of 16 July 2009: http://criticalinfrastructure.blogspot.com/2009/07/cip-standards-may-not-be-enough-to.html

[26] Anderson, R. and S. Fuloria, (2010) *On the Security Economics of Electricity Metering*, Harvard University, WEIS'10.

[27] For example, see Molnar and Schechter, *Self Hosting vs. Cloud Hosting: Accounting for the security impact of hosting in the cloud*, WEIS'10.

[28] Presentation by Matt Broda at the CEPS Task Force, Brussels.

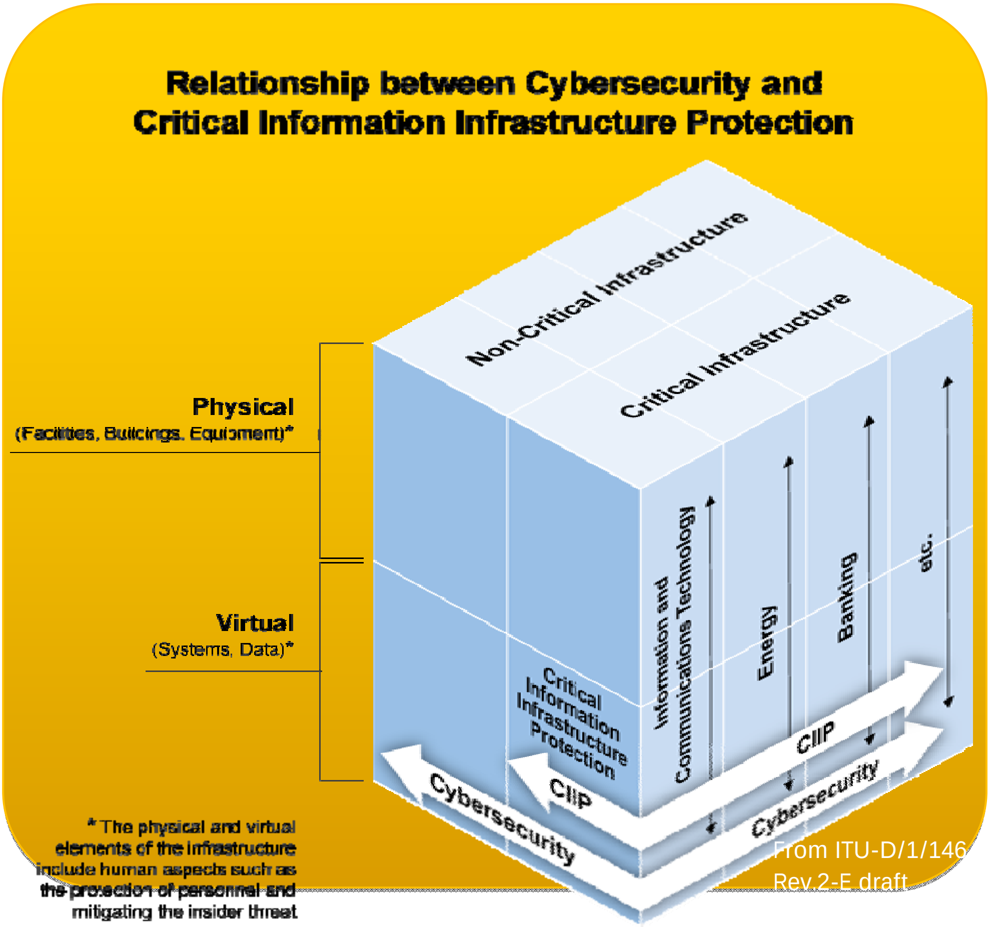
less enterprise computing models the internet and online services are becoming increasingly critical to social stability and the economy (e.g. email, instant messaging, weather reports and warnings, e-commerce and online banking, outsourced IT support and services, e-government services, e-health, cloud computing). The reliance continues to increase and infrastructure evolves to adapt to the changing needs of society. This also leads to an increased interplay between the domain of cyber security and that of CIIP policy (see Figure 7 below).

A key role in CIIP is played by centralised control systems and SCADA systems, which are widely employed to monitor and control infrastructures remotely. However, SCADA-based systems are not always considered to be secure, as recalled by Brunner and Suter (2008):

> once-cloistered systems and networks are increasingly using off-the-shelf products and IP-based networking equipment, and require interconnection via the internet, which opens the door to attackers from the outside in addition to those on the inside.[29]

[29] Brunner and Suter, *op. cit.*, at p. 38.

Figure 7. Cyber-security and CIIP


Relationship between Cybersecurity and Critical Information Infrastructure Protection
Physical
(Facilities, Buildings, Equipment)*
Virtual
(Systems, Data)*
* The physical and virtual elements of the infrastructure include human aspects such as the protection of personnel and mitigating the insider threat
Non-Critical Infrastructure
Critical Infrastructure
Information and Communications Technology
Energy
Banking
etc.
Critical Information Infrastructure Protection
CIIP
Cybersecurity
CIIP
Cybersecurity
From ITU-D/1/146
Rev.2-E draft

Source: Broda (2010).

The CEPS Task Force strongly recommends that a coordinated, holistic approach be adopted, encompassing both CIP and CIIP. An early recognition of the need for a coordinated approach between these two policy domains came in 2003 from the “G8 Principles for Protecting Critical Information Infrastructures” adopted by the G8 Justice & Interior Ministers, which clearly state that:

> In order effectively to protect critical infrastructures … countries must protect critical information infrastructures from damage and secure them against attack … Effective protection also requires communication, coordination, and cooperation nationally and internationally among all stakeholders – industry, academia, the

private sector, and government entities, including infrastructure protection and law enforcement agencies.[30]

2.3 C(I)IP: Key players

Over the years, and in particular during the past decade, the CIP universe has been populated with increasingly diverse and specialised entities, which play a key role as "the infrastructure of critical infrastructure protection". In this section, we briefly introduce the non-expert reader to these often-unknown bodies.[31]

- *Government*

Responsibility for the coordination of CIP and CIIP policy rests with government in the very first instance. At national level, departmental ministers in charge of homeland security are mainly responsible for coordinating the policy.

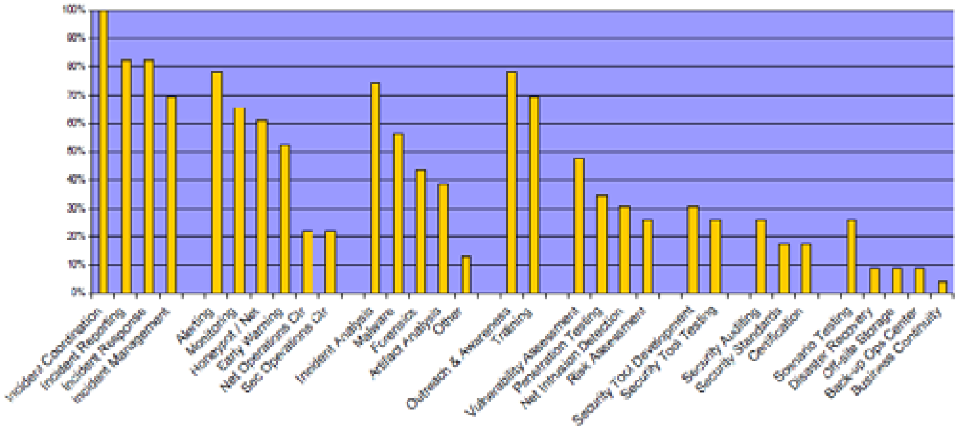
- *Specialised response teams*

Every country that has a CIIP policy relies on some form of response team. Depending on the country, the name can be replaced by synonymous terms such as – CERT/CC (Computer Emergency Response Team/Coordination Centre); CSIRT (Computer Security Incident Response Team); IRT (Incident Response Team); CIRT (Computer Incident Response Team); SERT (Security Emergency Response Team). Initially a mere reaction force, CERTs have extended their capacities to become a complete security service provider, including prevention services such as alerts, security advisories, training and security management services. The term "CERT" is a protected label of Carnegie Mellon CERT, the first CERT of the world. As a result, the new term "CSIRT" was established at the end of the 1990s. At the moment both terms (CERT and CSIRT) are used synonymously, with CSIRT being the more precise term. Figure 8, below shows the main services offered by CERTs with National Responsibility in Europe.

[30] http://www.justice.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf

[31] These players do not fill every possible gap in the CIP cycle. Depending on the country, dedicated institutions such as sectoral regulators (e.g. in energy, telecommunications, finance) and political institutions (e.g. the US Senate) contribute to policy actions aimed at strengthening CIP policy.

Figure 8. Services offered by CERTs with National Responsibility



Source: ENISA.

- *Analysis, communication and reporting centres*

A key role in the CIP landscape is played by dedicated centres that deal with a number of steps in the CIP cycle, including warning and alerts, information-sharing, reporting and often also awareness-raising and education. For example, Warning, Advice and Reporting Points (WARPs) have been established in the UK as part of the information-sharing strategy of NISCC (the National Infrastructure Security Co-ordination Centre) to protect the UK Critical National Infrastructure from electronic attack. WARPs have been shown to be effective in improving information security by stimulating better communication of alerts and warnings, improving awareness and education, and encouraging incident reporting. WARP members agree to work together in a community and share information to reduce the risk of their information systems being compromised and therefore reduce the risks to their organisation. This sharing community could be based on a business sector, geographic location, technology standards, risk grouping or whatever makes business sense.[32]

[32] In more detail, WARPs: i) receive warnings/advice from WARPs/CSIRTs/CERTs and other sources, filter and assess them, and reissue them to their community where appropriate (perhaps with increased priority or added value); ii) provide email and/or telephone advice to community members on security matters; iii) solicit and record IT-security incident reports from the community; iv) share (possibly sanitised) incident reporting data with other WARPs/CERTs etc., with whom a sharing agreement has been reached (formal or

In the US experience on critical infrastructure protection, the role of Information Sharing and Analysis Centers (ISACs) is considered essential, since these bodies represent private CI owners in various sectors of the economy. ISACs began with the National Coordinating Center for Communications (NCC) back in 1984 and the Financial Services ISAC in 1999.[33] Today, there are 14 ISACs in place, and they also jointly formed an ISAC Council.

An ISAC is defined as a trusted, sector-specific entity, which

- Provides to its constituency a 24/7 Secure Operating Capability that establishes the sector's specific information/intelligence requirements for incidents, threats and vulnerabilities.
- Collects, analyses, and disseminates alerts and incident reports to its membership based on its sector focused subject matter analytical expertise;
- Helps the government understand impacts for its sector;
- Provides an electronic, trusted capability for its membership to exchange and share information on cyber, physical and all threats in order to defend the critical infrastructure; and
- Shares and provides analytical support to government and other ISACs regarding technical sector details and in mutual information-sharing and assistance during actual or potential sector disruptions whether caused by intentional, accidental or natural events.

- *Private sector*

Given that most of the critical infrastructure is operated on a commercial basis, it goes without saying that no concrete and effective policy can be implemented without strong public-private collaboration. Brunner and Suter (2008) report that:

> all countries examined have recognized the importance of public-private partnerships (PPP) … Different types of such partnerships

informal);[32] v) contribute incident data, resources and/or expertise/knowledge to peers etc to help deal with widespread problems; vi) participate in 'networking' and sharing of experiences and knowledge with other members of the information-sharing network; vii) develop close links with selected WARPs/CSIRTs/CERTs for support and collaboration on problems.

[33] See ISAC Council (2004), at http://www.isaccouncil.org/whitepapers/files/Information_Sharing_and_Analysis_013104.pdf

> are emerging, including government-led partnerships, business-led partnerships, and joint public-private initiatives. In Switzerland, Korea, the UK, and the US, strong links have already been established between the private business community and various government organisations. One of the future challenges in many countries will be to achieve a balance between security requirements and business efficiency imperatives. Satisfying shareholders by maximizing company profits has often led to minimal security measures. This is because like many political leaders, business leaders tend to view cyber-attacks on infrastructures as a tolerable risk.[34]

It must be recalled, however, that the private sector is itself very heterogeneous. In particular, several infrastructure owners and operators are local by their very nature, and do not necessarily exhibit a large scale. At the same time, CI suppliers – in particular those belonging to the IT sector – have much more limited local capabilities, and are more global in scale. This makes public-private cooperation potentially more difficult, but also more fruitful. At the same time, it needs to be noted that the private sector already works together via associations/organisations such as ICASI[35] (Industry Consortium for the Advancement of Security on the internet) and FIRST.[36] A good example is the Conficker Work Group, where industry representatives came together on a common issue. These pro-active self-forming industry efforts should be connected to the PPPs.

2.4 The Critical Infrastructure Protection life cycle

CIP policy is not limited to securing an immediate and effective response in case of disruption. On the contrary, there are widely recognized phases in the CIP cycle that combine prevention and cure. More specifically, governments and private parties involved should make sure that effective policy measures are in place for prevention and early warning, detection of major threats, risks and vulnerabilities. When a major failure occurs, measures should be in place to ensure a timely reaction and efficient crisis management.

[34] Idem., p. 535.

[35] See their website at: www.icasi.org

[36] See their website at: www.first.org

More specifically, the US experience has led to the identification of six main phases of the critical infrastructure protection event cycle, occurring before, during, and after an event that may compromise or degrade the infrastructure. These six phases build on one another to create a framework for a comprehensive solution for infrastructure assurance. They are structured as follows:

Phase 1. *Analysis and assessment*. The analysis and assessment phase is the foundation and most important phase of the CIP life cycle. This phase identifies the assets or functions that are absolutely critical to mission success and determines the assets' or the functions' vulnerabilities, as well as their interdependencies, configurations, and characteristics. An assessment is then made of the operational impact of infrastructure loss or degradation. For example, Proactive Cyber Defence may anticipate an attack against computers and networks. It applies equally well to all critical infrastructure sectors, as it involves intercepting and disrupting an attack or a threat, either pre-emptively or in self-defence.

Phase 2. *Remediation*. The remediation phase involves precautionary measures and actions taken before an event occurs to fix the known cyber and physical vulnerabilities that could cause an outage or compromise a CI, critical asset or function. For example, remediation actions may include education and awareness, operational process or procedural changes or system configuration and component changes.

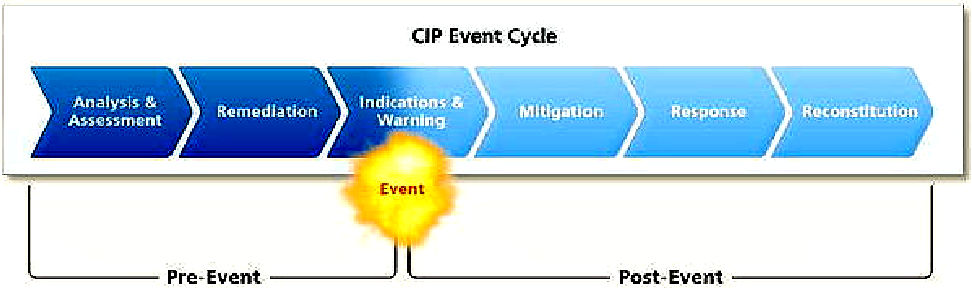
Phase 3. *Indications and warnings (before and/or during an event)*. The indications and warnings phase involves monitoring to assess the mission assurance capabilities of critical infrastructure assets and to determine if there are event indications to report. Indications are preparatory actions that indicate whether an infrastructure event is likely to occur or is planned. Indications are based on input at the tactical, operational, theatre, and strategic level. At the tactical level, input comes from asset owners. At the operational level, input comes from the CI sectors. At the theatre level input comes from regional assets such as allied intelligence, NATO, command intelligence, allied governments, and coalition forces. At the strategic level, input comes from intelligence, law enforcement, and the private sector. Warning is the process of notifying asset owners of a possible threat or hazard.

Phase 4. *Mitigation (occurs both before and during an event).* The mitigation phase comprises actions taken before or during an event in response to warnings or incidents. Critical asset owners, CI sectors, Department of Defense installations, and military operators take these actions to minimize the operational impact of a critical asset's loss or debilitation.

Phase 5. *Incident Response (after the event).* Incident response comprises the plans and activities taken to eliminate the cause or source of an infrastructure event.

Phase 6. *Reconstitution (after an event).* The last phase of the CIP life cycle, involves actions taken to rebuild or restore a critical asset capability after it has been damaged or destroyed. This phase is the most challenging and least developed process.

Figure 9. Phases of the CIP event cycle



Source: US Department of Defense.

The approach and the phases described above are, indeed, referred to as a single event. However, there is increased awareness of the fact that real-life events like erupting volcanoes or forest fires are seldom isolated, and even in the 9/11 attack there was a 'succession of events' rather than a single event. Already a few institutions, like the Tripartite Forum in the financial area, prefer to take a more holistic perspective and deal with 'a crisis' or even crises instead of just one event.

This leads to the notion of 'crisis life-cycle', which differs from the previous approach in three ways:

a. its goal is almost uniquely operational in that it deals with actual facts when they occur,

b. in dealing with real life situations it takes into account a multiplicity of events, thus

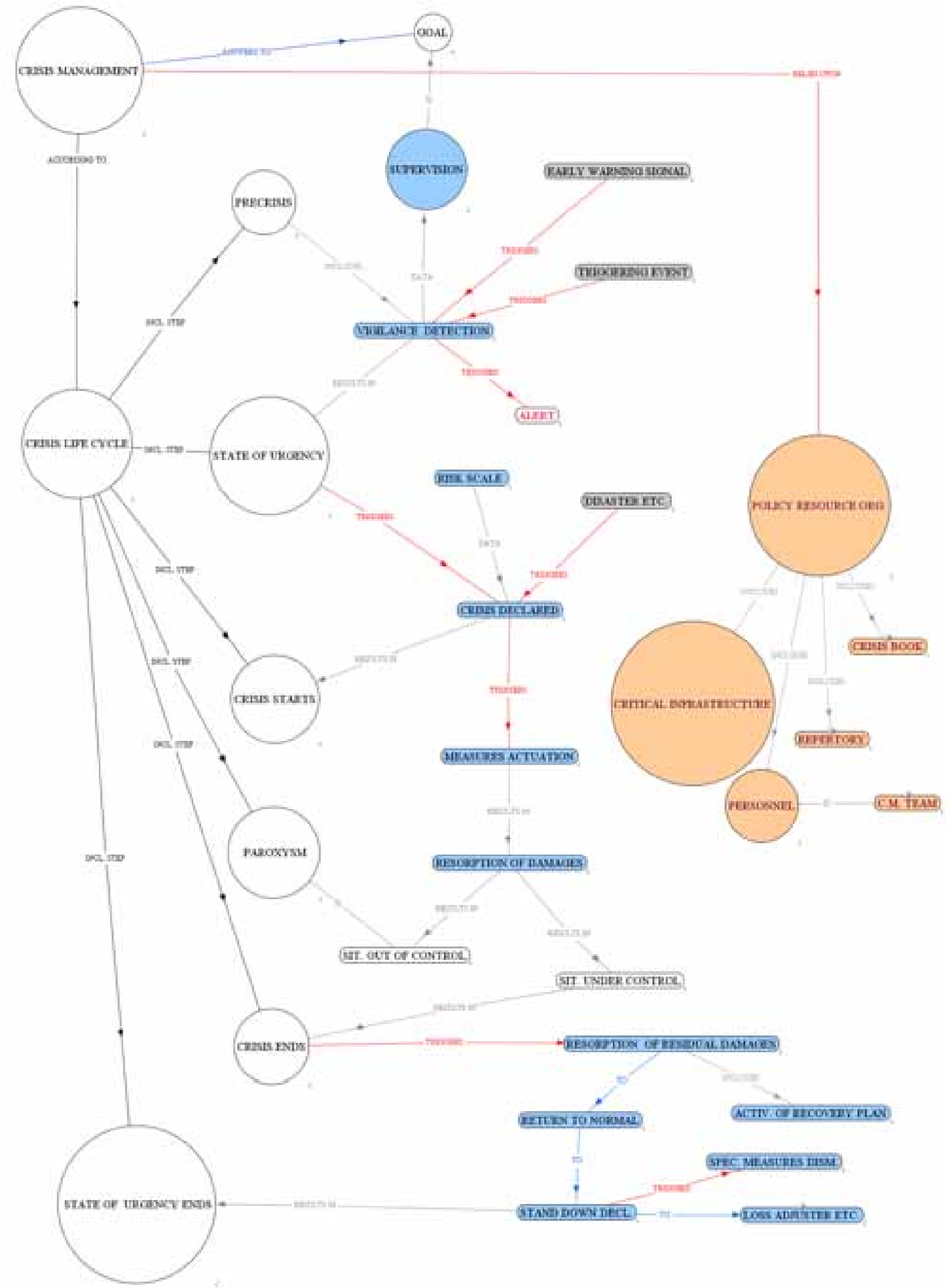
c. focusing on issues that are relevant for practical proceedings.

The concept originated from debates on the structuring of a “Business Continuity Glossary” of the IT Expert Group of the Tripartite Forum, where a chapter was dedicated to “Crisis management”. Early versions of this chapter dealt with issues like “phasing and acting” on one side and “landmarks” on another. Notions like “early warning signal”, “emergency situation”, “alerts”, “triggers”, “escalation procedure” were scattered unevenly. Some of them were common to several phases, others were specific. There was a need for more consistency and clearer articulation.

Figure 10 below is a simplified version of the current model. This model was successfully applied to actual financial crises. Its scope could easily be extended. Apart from its overall practicality, such a model draws attention to several factors, such as:

- the importance of (often weak) warning signals; and
- the dynamics of events ‘inside’ a crisis; which analysis should provide a less disputable answer to the question “is the crisis over ?”

Figure 10. The crisis life-cycle (simplified)

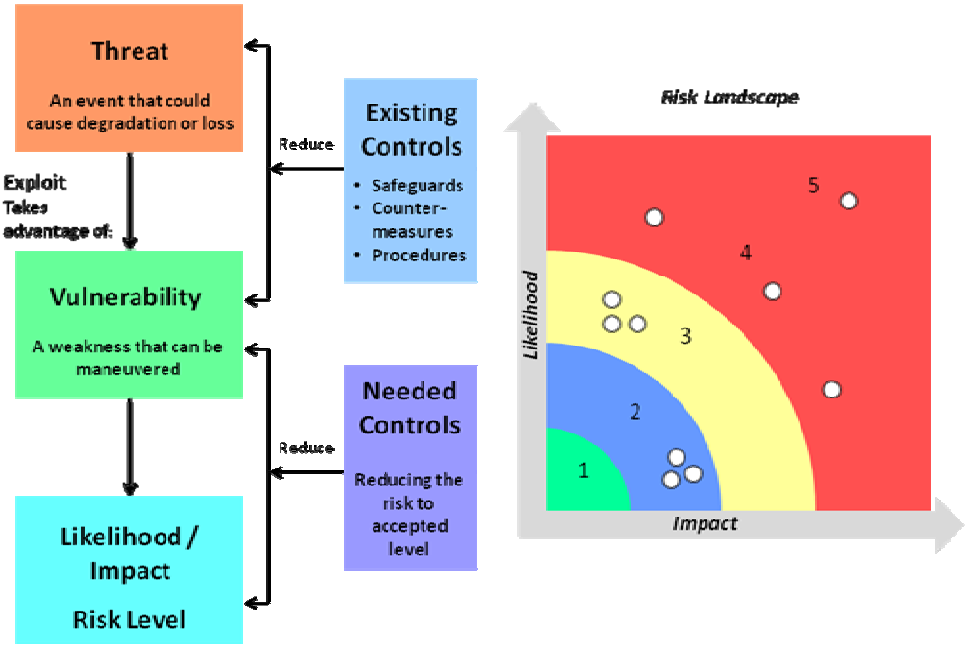


Source: Gresser , Parsifal project (see footnote 74).

2.4.1 *Focus: Assessing infrastructure vulnerability*

Infrastructure vulnerability is referred to as "the characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard".[37] Assessing vulnerability means undertaking "a systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities". Figure 11 below shows the main dimensions of the assessment exercise, from threats to vulnerability to impact to the final determination of the risk level. These include the evaluation of existing controls; identification of the controls that are needed to reduce the risks to an accepted level; the creation of the risk landscape that enables the understanding of the global situation, and to take informed decisions.

Figure 11. Basic elements of vulnerability assessment



Source: E. Adar, Task Force participant (2010).

[37] US Department of Defense, Directive 3020.40, January 14, 2010, at http://www.fas.org/irp/doddir/dod/d3020_40.pdf.

Key parameters in infrastructure vulnerability assessment are the following:

- *Discoverability*: How easy is it to find the vulnerability?
- *Reproducibility*: How easy is it to reproduce the attack?
- *Exploitability*: Measures how complex the process is to exploit the vulnerability (unproven, proof of concept, functional, and highly likely).
- *Access vector*: Measures whether a specific vulnerability is exploitable locally or remotely.
- *Access complexity*: Measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system.
- *Authentication*: Measures whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability.
- *Remediation level*: Measures the level of solution available (official fix, temporary fix, workaround, unavailable).
- *Report confidence*: Measures the degree of confidence in the existence of the vulnerability and the credibility of its report (unconfirmed, uncorroborated, and confirmed).

In the case of CII, additional parameters can be added in the vulnerability assessment, such as:

- C-I-A (confidentiality, integrity and availability) impact of the vulnerability;
- Sensitivity to latency;
- Regulatory restrictions that have an impact on technical support;
- Embedded security services;
- Unknown vulnerabilities for specific devices;
- Complexity level of the IT asset.

Moreover, another important parameter is the independence, dependence, or mutual dependence of the infrastructure at hand. This also affects the likelihood and type of cascading and escalating effects. In a *cascading failure*, a disruption in one infrastructure causes a disruption in a second infrastructure; in an *escalating failure*, a disruption in one infrastructure exacerbates an independent disruption of a second infrastructure (e.g., the time for recovery or restoration of an infrastructure increases because another infrastructure is not available); finally, in a so-called *"common cause" failure*, a disruption of two or more infrastructures at the same time occurs because of a common cause (e.g., natural disaster, right-of-way corridor).

The present description does not aim to be exhaustive. Rather, it is meant to highlight the growing complexity of vulnerability assessment in the prevention phase of the CIP life cycle. In this respect, a frequently stressed need is that of adopting an 'all-hazards' approach to CIP policy. This requires that all potential sources of risk (natural, man-made) as well as their likely interdependencies and domino effects are taken into account when defining a strategy to enhance preparedness towards given threats.

2.5 Existing CIP policies

2.5.1 Trends in national policies for CIP and CIIP

As reported during meetings of the CEPS Task Force, member states are currently grappling with several challenges in respect of CIP policy: i) the world economic situation has led to an underinvestment in CIP; ii) there are missing business cases, meaning that there are a limited number of examples where threats have been realised, and this had led some stakeholders to wonder if the investment is justified; iii) there are questions regarding the problems to be addressed in practice-attacks, coordination, global or regional levels, etc.; iv) there needs to be a prioritization among sectors on the basis of clear criteria, which means that some sectors will not be a priority focus; v) there is a lack of understanding of the amount of investment needed to offset the risk; (vi) the long-term impact of CIP protection, as well as the prevalence of threats to society are still to be fully understood.

More generally, although the challenges are global, accountability still mostly rests with national governments. In addition, there are important cultural and legal specificities that inform responses and are different across countries. This makes establishing a harmonised global approach towards C(I)IP more complex.

For example, while the UK employed a multi-agency approach with coordination between the public and private sector, France's strategy seems to be more focused on the role of the public sector;[38] and the strategy used by the Netherlands relies on a form of public-private coordination, but with significant input from the private sector.

In 2008, a report by the Swiss Crisis and Risk Network (CRN) looked at CIP policy developments in 25 countries and noted the emergence of three main trends.

- First, many countries pay *increasing attention to the concepts of resilience and all-hazard approaches*. The reason for the increased focus on resilience is mostly related to the fact that comprehensive protection of all critical infrastructures – once they have been identified – against all threats and risks is impossible, not only for technical and practical reasons, but also because of cost. Priorities must thus be established by distinguishing between critical infrastructures that deserve a greater level of attention, or by identifying vital points within a critical infrastructure. But this calls for the availability of data. Without reliable data, the only way to organise a meaningful CIP policy is to strengthen the understanding of the causes and effects of infrastructure failures, including natural accidents and man-made attacks. This leads to the conclusion that it is beneficial to adopt an 'all-hazards' approach, designed for comprehensive protection irrespective of the nature of the threat, with a focus on the capability to respond to a whole spectrum of unanticipated events. Recent examples that go in this direction include the Canadian Public Safety department's document on "Working Towards a National Strategy and Action Plan for Critical Infrastructure"; and the approach adopted by the new Swedish Civil Contingencies Agency (SCCA) created in January 2009.
- Second, this has direct implications for how CIP is organised: a move towards the *centralisation of responsibility* in this policy domain can be observed. This is mostly driven by the increasingly holistic nature of the threats and the risks to which society is exposed, as well as by the trend (described above) towards an all-hazards approach to CIP policy. Recent examples can be observed in Canada, Sweden and the UK.
- Third, there is continued or even growing attention to the *cyber-dimension* of the issue, linked to the growing awareness that globally

[38] N. Robinson, presentation at the CEPS Task Force, meeting 4, CEPS, Brussels.

> connected information and communication technologies have become a particularly vulnerable part of every country's national infrastructure (often also discussed in terms of 'cyber war'). Initiatives by the US and France, but also by NATO, are guided by the concern that the information and communication infrastructures are increasingly vulnerable not only because of their extremely dense connectivity, but also due to both the state's and society's dependence on them.

2.5.2 EU-level policy initiatives

At the EU level, the European Commission has defined as European Critical Infrastructures (ECIs):

> those designated critical infrastructures which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS, or a single member state if the critical infrastructure is located in another member state.[39]

Following the bomb attacks by al Qaeda in Madrid, the June 2004 Council asked for the preparation of an overall strategy to protect critical infrastructure. On 20 October 2004, the Commission adopted a Communication on Critical Infrastructure Protection in the Fight against Terrorism, which put forward suggestions for what would enhance European prevention, preparedness and response to terrorist attacks involving Critical Infrastructures (CI).

The Council conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" adopted by Council in December 2004 endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP) and agreed to the setting up by the Commission of a Critical Infrastructure Warning Information Network (CIWIN). Following this call, several initiatives have been launched at the EU level to contribute to a more integrated CIP policy. These include the European Programme for Critical Infrastructure Protection (EPCIP); the European Public Private Partnership for Resilience; the European Forum of Member States; the appointment and proactive role of ENISA and the EISAS feasibility study.

[39] See European Commission Communication on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final, 12 December 2006.

2.5.2.1 The EPCIP

Back in November 2005, the Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP), which provided policy options on how the Commission could establish EPCIP and CIWIN. The December 2005 Justice and Home Affairs (JHA) Council Conclusions on Critical Infrastructure Protection called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection. A 2006 Communication set out the principles, processes and instruments proposed to implement EPCIP. The implementation of EPCIP will be supplemented where relevant by sector-specific Communications setting out the Commission's approach to particular critical infrastructure sectors. Critical information infrastructures (CIIs) are tougher to identify. The ECI directive simply writes that ICT will be the next sector to which the EC will look to define criteria for the criticality of ICT CIs. Thus, there is no formal definition at the moment, but this is a priority for the Commission.

The second pillar of the CIIP initiative is the 2006 Communication on Secure Information Society. It is part of the i2010 Strategy, which in turn was part of the Lisbon Strategy. The initiative must be framed by what the Commission is trying to do in information security activities. One of the core principles is the idea that security and resilience must in some way boost trust. Security is not a value in itself. It must serve a purpose to drive forward the information society.

As the action plan is based on a Communication, it is not based on a regulatory instrument in a conventional binding sense. The member states are not bound by any obligations. There are three main reasons for this:

- First, the Commission does not have the legal basis to enact binding law of the nature contained in the Communication.
- Second, the whole goal of the initiative is to make stakeholders talk to each other and to TRUST each other. Trust is not easily engendered through binding regulation.
- Third, developing a legal basis would have taken too much time, as it must go though the European Council etc. There was/is a need for action now.

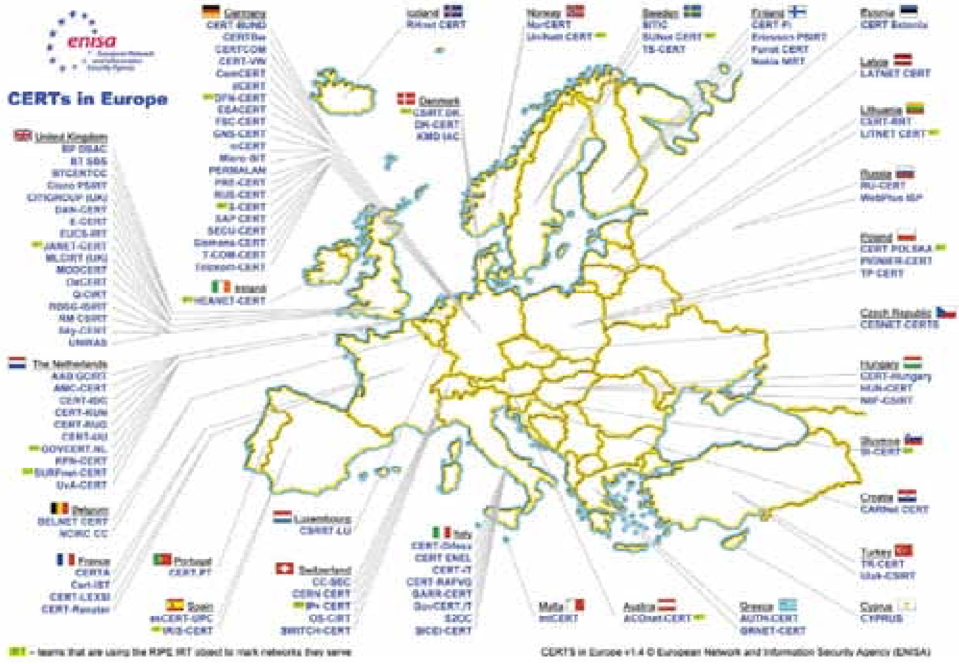
2.5.2.2 The EP3R: Its objectives and its tools

An example of an activity is the European Public-Private Partnership for Resilience (EP3R). This is still in its preparation stage, and accordingly the exact scope and goals of this initiative still need to be determined. Overall, the goal of the EP3R is to improve information-sharing between the public and private sectors. Below, in Section 4 of this report, we provide some suggestions as to how this can be done in a fruitful way.

2.5.2.3 The European Forum for Member States

The European Forum for Member States allows the Commission and member states to discuss freely and privately the important issues and share practice, such as prevention and reaction capabilities. Also, the European Security Response Group aims to get the national CSIRTs talking to one another. Presently, few CSIRTs are sharing information. This is important because some CSIRTs are not performing at a high level and could benefit from a knowledge transfer from other CSIRTs.

Figure 12. CSIRT activity in Europe



Source: ENISA, EISAS Final Report (2010).

Another initiative of the Commission is to increase international cooperation at the global level. The goal here is to identify principles and guidelines (specifically for internet protection, but to be expanded to other areas of ICT) at EU and global level. The US, Canada, and Japan are the main actors in this area. One of the key obstacles to be overcome is of a very preliminary nature: some member states do not even consider the internet to be a critical information infrastructure, and this obviously hampers international dialogue. The goal is then to take this EU agreement and coordinate it at the global level. The Commission approach takes into account the fact that the internet is very diffuse. A top-down approach is therefore not really possible; a more mixed approach (top-down and bottom-up) is needed.

2.5.2.4 CIIP policies and the role of ENISA

ENISA is an EU body established in 2004 to carry out very specific technical, scientific tasks in the field of Network and Information Security.[40] This work is only performed within the 'Community domain' ('first pillar' and internal market of the EU): as a "European Community Agency". ENISA's mission is essential to achieve a high and effective level of Network and Information Security within the European Union. Together with the EU-institutions and the member states, ENISA seeks to develop a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organisations in the European Union. ENISA helps the European Commission, the member states and the business community to address, respond and especially to prevent network and information security problems. The agency also assists the European Commission in the technical preparatory work for updating and developing Community legislation in the field of network and information security.

ENISA's mandate was extended to 2012 during the lengthy and difficult negotiations that led to the revision of the telecoms package in Europe. Member states are now starting to agree that ENISA's scope should be extended. To help co-ordinate Europe's response, the European Commission has proposed a new regulation to strengthen and modernise ENISA and reinforce cooperation across EU member states, law enforcement authorities and the industrial sector. Under its new mandate, ENISA would engage EU member states and private sector stakeholders in

[40] ENISA came into being following the adoption of Regulation (EC) No 460/2004 of the European Parliament and of the Council on 10 March 2004. Operations started in Crete in September 2005, after a recruitment period in Brussels, and with the arrival of staff that were recruited through EU-wide selections. See www.enisa.europa.eu.

joint activities across Europe, such as cyber security exercises, public private partnerships for network resilience, economic analyses and risk assessment and awareness campaigns. A modernised ENISA would have greater flexibility and adaptability and would be available to provide EU countries and institutions with assistance and advice on regulatory matters.

Finally, to respond to the increased intensity of cyber security challenges, the proposed Regulation would extend ENISA's mandate for five years and gradually increase its financial and human resources. The Commission proposes that ENISA's governance structure also be strengthened with a stronger supervisory role of the management board, on which the EU member states and the European Commission are represented.

Two of the achievements of ENISA are the completion of the European Information-Sharing and Alert System (EISAS) feasibility study (see Section 2.4.2.5 below) and the recent publication of the Country Reports on Network and Information Security (NIS), carried out by Deloitte, which provide a comprehensive 750 pages-plus overview of the status of NIS in 30 European countries, including identification of stakeholders and trends.[41] The reports find that European countries are highly varied in how prepared they are for dealing with cyber crime, attacks and in terms of network resilience.

2.5.2.5 The EISAS feasibility study

ENISA was asked by the European Commission to analyse the current state of affairs as regards existing systems and initiatives across Europe that have the goal of disseminating appropriate and timely information on Network and Information Security (NIS) vulnerabilities, threats, risks and alerts, as well as sharing good practices. In addition, ENISA was empowered with the task of identifying possible sources of security information that could potentially contribute to an EISAS. This led to the publication of a first EISAS feasibility study in 2007.

As reported by ENISA, in defining the most promising scenario for European involvement in this field, the study analysed first the findings of previous projects and other studies with a similar scope and second the status quo of the existing (national) information-sharing systems for home-

[41] See http://www.enisa.europa.eu/media/press-releases/eu-agency-maps-key-online-security-actors-strategies-good-practices-in-europe.

users and small and medium enterprises (SMEs). Two types of involvement for the European Union (operating and facilitating) in the three parts of the information-sharing process (information gathering, processing and dissemination) were examined under three different perspectives (technical / organisational, political and social / cultural).

The study concluded that the most effective level of involvement for the European Union in the establishment and operation of an information-sharing system for its home-users and SMEs would be that of a facilitator; a moderator of discussion and a 'keeper of good practice'. The report concludes with proposals for the next steps to be taken and a 'proof of concept' scenario.

2.5.2.6 The digital agenda

On 19 May 2010, the European Commission presented its Digital Agenda, which forms an integral part of the EU 2020 strategy launched by the second Barroso Commission. In the Agenda, significant emphasis is placed on the need to improve the security of information infrastructure. In more detail, the Commission presents two separate lines of action:

- The "Key Action 6" entails the commitment to present measures in 2010 aiming at a reinforced and high level Network and Information Security Policy, including legislative initiatives such as a modernised European Network and Information Security Agency (ENISA), and measures allowing faster reactions in the event of cyber attacks, including a CERT for the EU institutions;
- The "Key Action 7" implies that the Commission will present measures, including legislative initiatives, to combat cyber attacks against information systems by 2010, and related rules on jurisdiction in cyberspace at the European and international level by 2013;

In addition, the Commission plans to establish a European cyber crime platform by 2012; examine the feasibility by 2011 to create a European cyber crime centre; work with global stakeholders notably to strengthen global risk management in the digital and in the physical sphere and conduct internationally coordinated targeted actions against computer-based crime and security attacks; and support EU-wide cyber-security preparedness exercises, from 2010.

As regards the obligations that the Agenda places on member states, the Commission requires that national governments:

- Establish a well-functioning network of CERTs at national level covering all of Europe by 2012;
- In cooperation with the Commission, carry out large-scale attack simulation and test mitigation strategies as of 2010; and
- Set up or adapt national alert platforms to the Europol cyber crime platform, by 2012, starting in 2010.

2.5.3 EU actions in the various phases of CIP

EU policy initiatives have so far focused on the following phases of the CIP policy cycle:

- *Preparedness & prevention*. The EP3R and the Pan-European Forum for Member States, together with initiatives on the Baseline Capabilities of National/Gov CERTs fall into this first phase of the CIP cycle.
- *Detection and response*. The European Information-Sharing and Alert System (EISAS) provides a first step in this direction.
- *Mitigation and recovery*. Pan-European exercises on large-scale network security incidents, National Contingency Plans and reinforced cooperation between national/governmental CERTs all contribute to this phase.

In addition, international cooperation was stimulated by the adoption of principles and guidelines on long-term internet resilience and stability. The European Commission is also very active in the funding of research in the field of CIP.[42]

[42] For an overview of current projects being funded, see Marino and Skordas (2010), *EU research on critical infrastructure protection - CIP*, European CIIP Newsletter, April/May 2009, Volume 5, Number 1.

CHAPTER 2: MAIN FINDINGS

- The definition of critical infrastructure is still a moving target, and the boundaries between CIP and CIIP are a moving frontier. Countries have adopted slightly different definitions, different governance patterns and different forms of public-private partnerships to address the issue.
- The role of critical information infrastructure and its relevance for CIP policy is on the increase, leading also to more interplay between cyber-security and CIP policy. This also means that global problems still rely on very local competences and remedies: such a structural bias between 'attack' and 'defence' is what makes CIs globally interdependent nowadays.
- The key players in CIP policy – governments, specialised response teams, analysis, communication and reporting centres, the private sector, PPPs, sectoral regulators and political institutions – play very different roles in different countries, making international cooperation difficult.
- The key phases of the CIP event cycle are i) analysis and assessment; ii) remediation; and iii) indications and warnings, before the adverse event occurs. In addition, they include: iv) mitigation; v) incident response; and vi) reconstitution, after the event has occurred. It is important, however, to realize that real life events seldom come as isolated events; accordingly, referring to successions of events and, more generally, to the crisis life-cycle would be more appropriate.
- In the *ex ante* phase of CIP policy, infrastructure risk assessment plays a key role, and should be subject to further research and standardisation. Key parameters can already be identified both for CIP and CIIP, but more widely adopted standards would certainly strengthen international cooperation and the dissemination of best practices.
- At national level, CIP policy is increasingly: i) focused on resilience and an all-hazards approach; ii) centralised in one single body; and iii) focused on the cyber-dimension of the issue.
- EU actions in this domain – including the EP3R and the European Forum of member states – contribute to some of the phases of the CIP cycle, namely preparedness and prevention, detection and response, and mitigation / recovery.

3. IDENTIFYING THE POLICY CHALLENGE

The CIP domain exhibits a number of potential challenges for the policy-maker. In this section we illustrate the main economic issues behind the critical infrastructure protection problem, focusing in particular on the economics of CIP (Section 3.1, below) and on the issue of identifying and classifying risk to obtain more effective CIP strategies (Section 3.2). Section 3.3 then presents an analysis of sectoral specificities, potentially warranting an *ad hoc* approach. Section 3.4 concludes by translating our findings into policy recommendations to be further elaborated in Section 4, below.

3.1 The economics of C(I)IP

An often-neglected dimension of critical infrastructure protection in Europe is the economic one. Few attempts have been made in Europe to obtain a systematic and comprehensive analysis of the economics behind CIP and CIIP policy.[43] On the other hand, information security economics has become a thriving research area in academia.[44]

The CEPS Task Force reflected on the issue from a number of perspectives, and reached the following conclusions:

- *An efficiency-security trade-off*

One important economic problem behind the current exposure to systemic risk is the *efficiency-security trade-off* related to the increased reliance on interconnected infrastructures. According to this view, our increased independence on critical infrastructure has led to an over-exposure to risk due to the need to achieve productive efficiency, i.e. achieving a given

[43] A notable exception is the report entitled “Security Economics and the Internal Market” by Prof. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore for ENISA in February 2008, available online at http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec.

[44] See, *i.a.*, Moore, T., R. Clayton, and R. Anderson, *The Economics of Online Crime*, Journal of Economic Perspectives, Vol. 23, N. 3, summer 2009, pp. 3–20. See also http://infosecon.net/workshop/bibliography.php for a comprehensive bibliography on information security.

objective at the lowest possible cost. One example in this respect is public-private partnerships to build infrastructure such as motorways: in many European countries, from Hungary to Portugal, the absence of private incentives to use quality materials to build the road infrastructure has led the asset to perish very quickly, because the revenues associated with the execution of contractual obligations were not made dependent on any measure of reliability and sustainability over time.[45] Likewise, the recent 'oil spill' case off the coasts of Louisiana is a self-evident example of the absence of a 'plan B' when developing an infrastructure: the difficulty of improvising a recovery plan has caused enormous damage to the ecosystem. The trade-off between productive efficiency and security is all the more evident as the boundaries between CIP and CIIP have become increasingly blurred. As CIP expert Joe Weiss recently declared:

> When I was … involved in advanced controls and instrumentation, we viewed adding intelligence to the critical infrastructure as being a single-edge sword – nothing but productive improvements could accrue. We never realized that for all the positives there's a negative – "cyber". It's a double-edged sword and you have to address that. If you don't, the consequences can be devastating. If you do, the benefits can be phenomenally valuable. It is a trade-off between productivity and security.[46]

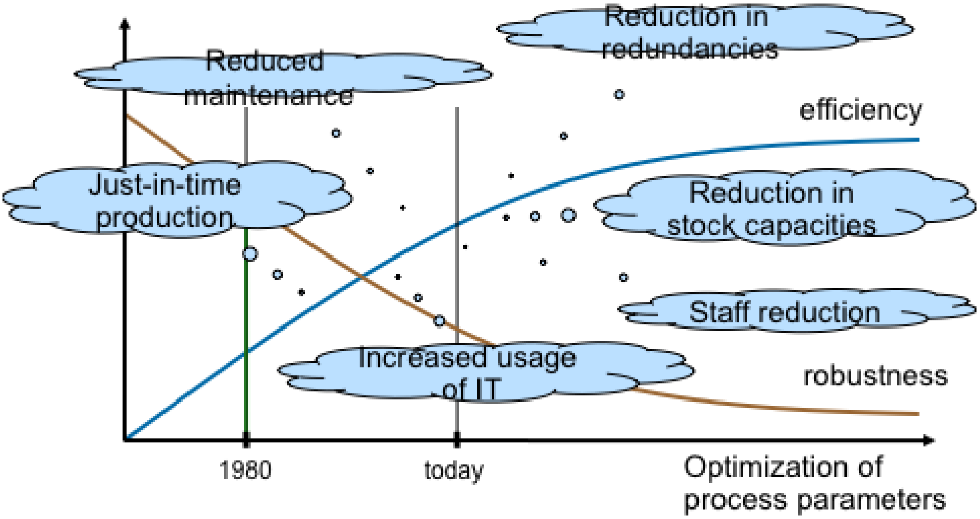
Figure 13, below shows the dimension of the trade-off, with increased efficiency often leading to just-in-time production chains, reduced maintenance efforts, stock capacities and staff, and – most importantly – a reduction in redundancies that are costly to preserve, but often also create potential alternatives in case of a major disruption to an infrastructure.

[45] See *i.a.* Renda, A. and L. Schrefler (2006), *Public-Private Partnerships. Models and Trends in the European Union*. Study requested by the European Parliament's Committee on Internal Market and Consumer Protection.

[46] See Interview with CNET, 10 May 2010, at http://news.cnet.com/8301-27080_3-20004505-245.html?tag=mncol;title (visited on November 5, 2010). Of course, the efficiency-resilience trade-off is not always a real dilemma. For instance, replacing rotary telephone switches with digital switches has significantly increased the robustness of the telephone network. Furthermore, migration from digital PSTN switching to Carrier VoIP has also increased, or at least not negatively affected, the robustness of the network. In any event, it is important to stress that the use of IT needs to be informed by the resilience requirements for the given service.

Also the increased use of IT is seen as potentially leading to more efficiency.

Figure 13. Efficiency and robustness



Source: T. Hauschild, CEPS Task Force.

- *An efficiency-privacy trade-off*

Another important dynamic that must be addressed by public policy when looking at CIP is the one between security and privacy.[47] Such an issue – often pitting privacy again security and vice versa – is a generally recognised one, especially when it comes to phone-tapping, deep-packet inspection on the internet and the keeping of personal data from internet searches.

The details of this trade-off must however be clarified and qualified. On the one hand, privacy can easily be seen as an element of security, since to ensure privacy and a trusted environment strong security is a requirement – whereas security can be interpreted as referring to authentication, authorization, access control, data protection, encryption, etc., on the other hand, national security or law enforcement interests often

[47] See, *i.a.* the recent publications by the EU agency ENISA on privacy in the IT environment, available at http://www.enisa.europa.eu/publications/position-papers.

require the use of monitoring and/or data collection technology that may negatively affect individual privacy. The network security mechanisms such as firewalls or intrusion detection devices as well as SPAM filters are in a grey area, since they provide security and convenience to the user at the cost of monitoring high-level traffic; at the same time, it is also true that this monitoring does not result in permanent/long-term data storage and only portions of the network traffic that are used in routing the packets are inspected (as opposed to the human-readable contents).

Similarly, some commentators have pointed to a growing tension between security and ease of use, which seems to be tipping in favour of the latter as a driver of enhanced demand by increasingly sophisticated customers. For example, Coucher (2010) recently wrote that:

> There are good commercial and operational reasons for the new or emerging networks and infrastructures such as 'Cloud Computing'; satellite-based networks with broad and narrowcast services; merged mobile, internet and corporate networks. User demands for instant availability and access to all data sources and services are forcing a simplified and common approach – so-called 'convergence' … The networks and database systems are designed to push data out as quickly and in as common a form as possible, rather than questioning the rights to access. Passwords are hidden, hard-coded, minimised or ignored in the rush to gain speedy access. So the balance of security and access is tipping towards ease of use, simplifying and minimising the overheads that would otherwise maintain separation and security, so creating a huge looming future vulnerability.

It should be noted that in this case, if well designed, robust security architectures can provide a simple and user-friendly interface. If good security practices are followed, strong security does not have to sacrifice much ease of use – in fact, in certain cases strong security can actually result in improved ease of use.[48] As in the case of privacy, the important lesson to be drawn is that security architects should be aware of possible consequences for privacy and ease of use when designing their systems.

[48] For instance, the introduction of a strong 2-factor single sign on schemes makes it unnecessary for the user to remember multiple complex passwords.

- *Principal-agent problems*

The efficiency-security trade-off can become more challenging, depending on how the infrastructure is owned and operated. Today's environment, partly resulting from the wave of privatisations that has led to a major restructuring of a number of industries, entrusts private economic agents with the task of acting in line with the public goal of securing resilience of critical infrastructures. The divergence between private payoffs from economic activities and the public payoff from resilience may lead to principal-agent problems, where the goals pursued by the principal (the public sector) must be achieved through action by the agent (the private sector). This situation may lead to problems such as: i) the need to specify ways to understand steps taken by private parties in managing critical infrastructures; ii) asymmetry of information between principal and agent; iii) the need to build a constructive dialogue between public policy-makers and private economic agents; iv) the need, in regulated sectors, to reward investment in infrastructure resilience by ensuring that positive externalities (i.e. enhanced resilience) are internalised to some extent by the investors.[49]

- *Complexity and unpredictability*

From an economic perspective, the C(I)IP market exhibits a significant degree of incomplete information, i.e. economic actors normally do not possess all the information needed to take informed decisions on how to define and manage risk. Defining and managing risk has become increasingly difficult due to the complexity and unpredictability of the threats associated with the operation of a given infrastructure, as well as the interconnectedness of the CIs in place, which makes domino effects likely and increases the difficulty of locating the potential sources of system failure. This problem is particularly evident in the case of the so-called 'black swans'.[50] Un- or very low predictability is the inherent difficulty of

[49] See, *i.a.* Laffont and Martimort, *The Theory of Incentives. The Principal-Agent Model*, Princeton University Press, (2001).

[50] A 'black swan' is a highly improbable and hard to predict event, which may either have devastating or major beneficial consequences. The attacks of the twin towers of the World Trade Centre on 9/11/2001 was a so-called black swan. The rise of the internet is a more positive black swan. One could almost theorize that major changes in our world came from 'black swans'.

these phenomena. Security experts know well that more damages will result from unanticipated events: statistics are inefficient to predict them, and accordingly black swans call for imagination, creativity, and 'thinking the unthinkable' type of foresight.

- *Positive and negative externalities*

The existence of **positive externalities** associated with the investment in infrastructure resilience limits the individual incentive to undertake such investments. This is often a result of externalities being generated in terms of enhanced security and resilience not being entirely captured by the investor, but accruing to society as a whole.[51] The flip side of the coin is that the damage that would accrue to society in the case of a major accident caused by failure of a given infrastructure is unlikely to be fully internalized – this, in turn, leads to **negative externalities** stemming from insufficient investment in security and, consequently, suboptimal resilience.[52] All in all, this creates a collective action problem, in which a collectively desirable action is not undertaken individually due to failure to coordinate individual activities and to allocate responsibility.

- *The potential role of liability*

In the law and economics literature, the existence of these externalities may require an examination of legal mechanisms, such as liability, for cases of negligence in the adoption of security measures.[53] However, the definition of an optimal liability system based on negligence presupposes that optimal standards are identifiable with reasonable certainty, which is problematic due to the problem of incomplete information but also due to

[51] See Varian, H. R. (2004), *System Reliability and Free Riding*, in Economics of Information Security, Kluwer.

[52] See, i.a. *Critical Information Infrastructure Protection and the Law: An Overview of Key Issues*, National Academy of Sciences, at: http://www.nap.edu/catalog/10685.html.

[53] For a seminal contribution on this issue, see Guido Calabresi, *The Costs of Accidents: A Legal and Economic Analysis*, New Haven: Yale University Press (1970). See also John Prather Brown, *Toward an Economic Theory of Liability*, 2 Journal of Legal Studies (1973) pp.323-350; Steven Shavell, *Economic Analysis of Accident Law*, Cambridge (MA): Harvard University Press (1987); and Landes, W.M. and R. A. Posner, *The Economic Structure of Tort Law*, Cambridge (MA): Harvard University Press (1987).

the *ex post* and case-by-case nature of what constitutes negligence or diligence. This may warrant the introduction of alternative liability regimes, such as strict liability. It is important to note that there are limits in the case of CIP, due to the difficulties in establishing causation links and the multi-party, multi-risk environment in which CIP providers operate. The fact that domino and cascading effects may materialize in this field along with dependencies and mutual dependencies between different infrastructures makes the assessment of liability almost prohibitive in some circumstances. Among others, Dari Mattiacci (2003) explains that tort law generally fails to provide first-best internalization of both positive and negative externalities, and may have to be complemented by other legal instruments, such as the definition of homogeneous standards and – in some cases – subsidies.

- *An incomplete insurance market*

A related issue that stems directly from incomplete information, exposure to unknown risk and difficult allocation of liability is the current lack of a well-developed insurance market for CIP. Notwithstanding the growing exposure to risk of several businesses and administrations, the development of insurance policies for these types of risk has not led to a more refined understanding of their nature, probability or the effectiveness of any countervailing measures. A more mature insurance market would certainly prove essential for the production of information on several issues such as: i) the nature and extent of certain risks; ii) the consequences that can derive in financial and economic terms from given behaviour by businesses or public authorities; and iii) the remedies that can prove more effective in reducing the negative impact of given occurrences. For example, if insurance companies were ready to grant discounts in their premium in case a business *A* adopts a given product *x* to protect itself from cyber attacks, this would automatically provide information on the effectiveness of product *x* in limiting the exposure of *A*.[54]

[54] Baer, W.S. (2003), *Rewarding IT Security in the Marketplace*, in: TPRC 2003.Keysan, Majuca and Jurcic (2004) state that "cyberinsurance results in higher security investment, increasing the level of safety for information technology (IT) infrastructure. Second, cyberinsurance facilitates standards for best practices as cyberinsurers seek benchmark security levels for risk management decision-making. Third, the creation of an IT security insurance market redresses IT security market failure resulting in higher overall societal welfare. We conclude that this is

The absence of a mature market is also justified by the fact that the insurance industry inevitably faces a number of problems when assessing CIP-related risks and the consequent premium level. Furthermore, with insufficient information about the causes, nature and features of current threats, insurance companies would inevitably expose themselves to **moral hazard** and **adverse selection**, which would lead to inefficient contracts and potential losses on their side.[55] The current reaction in the industry seems to be the introduction of fairly low maximum coverage, which provides very partial compensation if the event occurs.[56]

- *Rational ignorance*

A potential imperfection in the CIP market is due to the cost of gathering information *ex ante*, which hampers the attempt to invest in prevention in a way that would maximize the amount of information available before the event, and thus also maximize preparedness. The problem here is one of 'rational ignorance', i.e. a situation in which it is rational not to acquire all

a significant theoretical foundation, in addition to market-based evidence, to support the assertion that cyberinsurance is the preferred market solution to managing IT security risks". See *The Economic Case for Cyberinsurance*, at http://law.bepress.com/cgi/viewcontent.cgi?article=1001&context=uiuclwps.

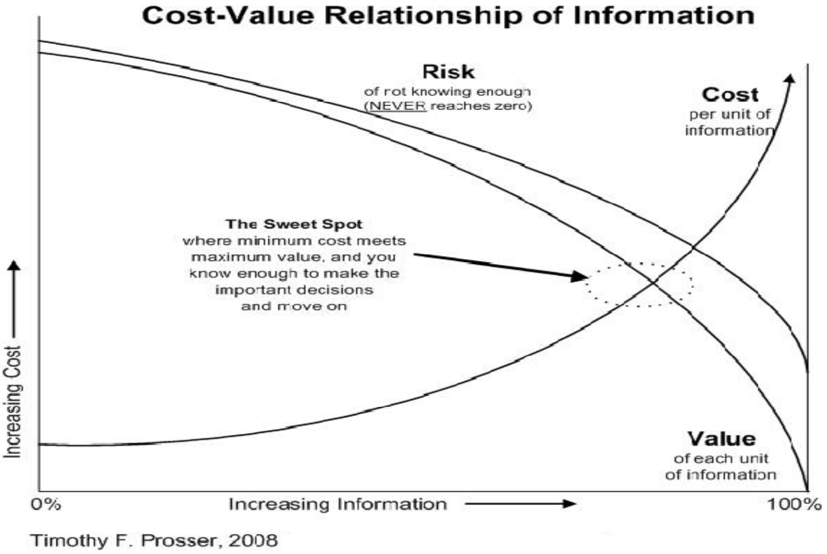
[55] Moral hazard occurs when a party insulated from risk behaves differently than it would behave if it were fully exposed to the risk. A typical example occurs in insurance contracts against theft, whenever full coverage leads the insured party to pay insufficient attention to his property. Adverse selection refers to a situation in which suboptimal results occur because buyers have asymmetric information: for example, if buyers only know the average quality of the goods sold in a given marketplace, and are not able to distinguish between good quality and bad quality products, they will not be willing to pay any additional price for supposedly good products. This will progressively lead better-than-average products out of the market, and worse-than-average products to survive. See Akerlof, George A. (1970). *The Market for 'Lemons': Quality Uncertainty and the Market Mechanism*. Quarterly Journal of Economics (The MIT Press) 84 (3): 488–500. For an application to the CIP policy domain, see Shetty, N., G. Schwartz, M. Felegyhazi and J. Walrand, *Competitive Cyber-insurance and Internet Security*, Economics of Information Security and Privacy, 2010, 229-247.

[56] See presentation by Simon Milner of Lloyd's at the CEPS Task Force 5th meeting.

the information that would potentially be available to policy-makers and private actors prior to the event.[57]

Figure 14, below shows a graphical representation of the rational ignorance concept. All else being equal, the more costly the information, the lower the amount of information that is optimal according to an *ex ante* cost-benefit analysis of information acquisition (so-called 'sweet spot' in the figure).

Figure 14. Rational ignorance



Timothy F. Prosser, 2008

The concept of rational ignorance demonstrates that action both before the event and after the event is warranted to maximize the preparedness and reaction potential of a given system.[58]

- *Systematic biases in hazard prevention*

A related issue in the analysis of behavioural patterns in CIP is that of systematic decision-making biases, which is intimately linked with

[57] See, for a seminal contribution on the issue, George J. Stigler, *The Economics of Information*, Journal of Political Economy, Vol. 69, Issue 3, 213-225 (1961).

[58] In addition, issues related to corporate secrecy and national interest do not allow access to more information in many circumstances.

behavioural economics and cognitive science.[59] In particular, Kunreuther et al (2008) analyze what they call the "psychology of hazard prevention".[60] Behaviours such as the systematic underestimation of low-probability high impact events, budgeting heuristics, learning failures, endowment effects and path dependency all point in the direction of a risk of under-investment in CIP especially by private parties.[61] Although a complete analysis of those behavioural biases would fall outside the scope of this report, suffice it to recall that most of them depend on the need to make decisions on incomplete information, as well as on the need to compare upfront costs with uncertain future benefits, which depend on the individual perception of the magnitude of the uncertain event, as well as the likelihood that it will actually occur. In most cases, these systematic biases call for public intervention, as private individuals would not be able to reach optimal decisions in isolation.

3.2 Measuring risk: Building common metrics

The several imperfections existing in the CIP 'market' – which may exhibit peculiarities also on a sectoral basis – call for action to improve the availability of information on the basis of which risk can be classified, analysed and mitigated. This, in turn, might also help the development of a (more) mature insurance market for the different risks connected to the operation of a critical infrastructure, something that today – as illustrated in the previous section – is still missing.

More specifically, the CEPS Task Force has discussed, with the help of experts, the problem of how to i) define an ontology of risk; ii) establish appropriate risk metrics, from an operational, organisational and technical perspective; and iii) how to define vulnerability parameters and a framework for risk management.

[59] See: http://opim.wharton.upenn.edu/risk/library/C2009_HK,RJM,EMK.pdf August 2009.

[60] Idem.

[61] Risk assessment becomes almost prohibitive in cases of very low probability. See, *i.a.* Taleb, N. N. (2007), *The Black Swan: The Impact of the Highly Improbable*, New York, Random House, 2007, 366 pages. In some circumstances, the risk calculation is not feasible, since near zero likelihood times near infinite cost do not fulfil the statistical requirements to be applied. And see *supra*, note 52 and associated text.

The main results of the debate in the CEPS Task Force imply two important recommendations. First, it is necessary to increase standardization in the taxonomy of risks as well as in the definition of available metrics. Secondly, the definition of a global framework for risk management is needed.

As a preliminary remark, as stated by one of the Task Force participants, the minimal requirements that a methodology for risk assessment of CI should meet are as follows:[62]

- **Identification of current risks**
  - Possibility of performing threat and vulnerability analysis on the CI and its components and also at the level of interdependencies and services when ICT are involved.
- **Risk quantification**: R = R (IE, S) → (C, L)
  - Enumeration of operation scenarios (S).
  - Identification of initiating events (IE) and protection measures.
  - Unambiguous evaluation of consequences (C).
  - Calculation of likelihood (L) based on available data.
- **Risk management**
  - Comparison of result of risk quantification versus tolerable risk.
  - Identification of protection measures that prevent/detect/respond to the identified 'initiating events' (IE), in order to reduce risk to a tolerable level.
  - Global approach to risk reduction versus local approach.
- **Identification of foreseeable risks**
  - Analyse/prevent changes in scenarios, initiating events, etc.

In addition, the basic principle of risk management must identify those protection measures that reduce the risk for the benefit of society and not only for business. Finally, since protection measures to reduce risk may involve several CI operators and may be more than one country, it is

[62] Filippini (European Commission, Joint Research Centre), presentation at the CEPS Task Force, CEPS, Brussels.

important to decide in advance who is going to pay for the implementation of identified risk reduction measures. In particular, given that in most European CIs EU-level coordination is required, it might also make sense for the EU (perhaps the agency whose creation we are proposing) to distribute funding in a way that results in the greatest impact to the protection of European CIs.

3.2.1 Risk metrics

Approaches to risk metrics needed to facilitate the identification and assessment of risks to include the following types:[63]

- **Operational metrics** – assess how well the organisation's formal policies and procedures are implemented by staff members;
- **Organisational metrics –** assess the adequacy of the standards, policies, and procedures adopted to enhance security;
- **Technical metrics** – assess the adequacy of the security being imposed to protect specific components of personal communications systems (PCS); the metrics of day to day system security;
- **Brainstorming metrics –** used in some cases to assess the 'big picture type of metrics'.[64]

Last, it should be based on existing security standards whenever applicable, with extensions for specific sector-driven domains. In particular, the following standards already exist and are in use in the field of CIIP and risk assessment / management:

- *ISO/IEC 27000 and NIST 800-53.* These standards are used in many CIIs for security metrics taxonomy.[65] They are focused on management of IT security and general IT technologies, and can provide sufficient solutions for the 'Enterprise ICT' domain. However, they provide only partial coverage for the 'Sector-Specific' domains that need to be addressed within the broader CIP policy.

[63] See Ronda Henning et al., Proceedings of the Workshop on Information Security System Scoring and Ranking, Applied Computer Security Associates, Williamsburg, Virginia, May 21-23, 2001, *http://www.acsac.org/measurement /proceedings/wisssr1-proceedings.pdf.*

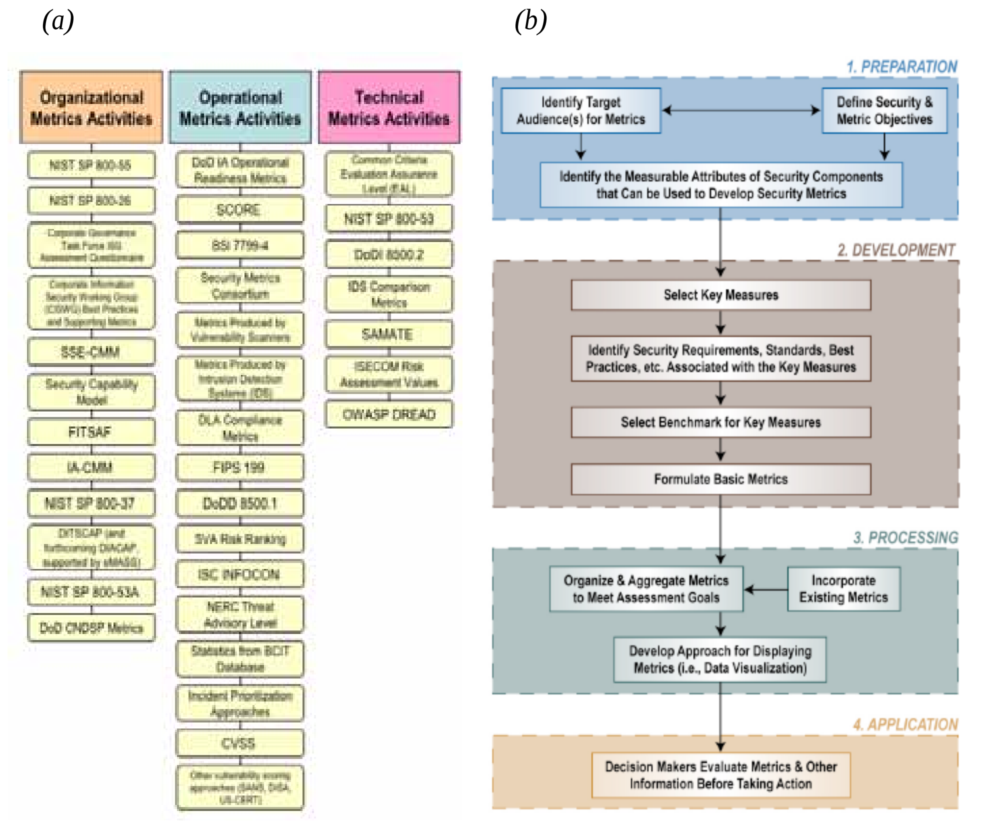
[64] Source: VTT Technical Research Centre, Finland.

[65] ISO 27004:2009 was intended to define metrics associated with ISO 27000 standards.

- *ANSI/ISA-TR99.00.01-2004*. The TR99.1 is focused on “Security Technologies for Manufacturing and Control Systems” (ANSI 2004). It provides a categorization and discussion of metrics primarily directed at the PCS domain, and may help refine the overall metrics categorisation or framework offered by ISO / NIST.

Figure 15, below shows two examples of metrics development: a) the categorization of metrics by the National SCADA test bed; and b) the Security Metrics Development framework by the Institute for Information Infrastructure Protection (I3P).

Figure 15. NSTB library and the I3P Security Metrics Development framework

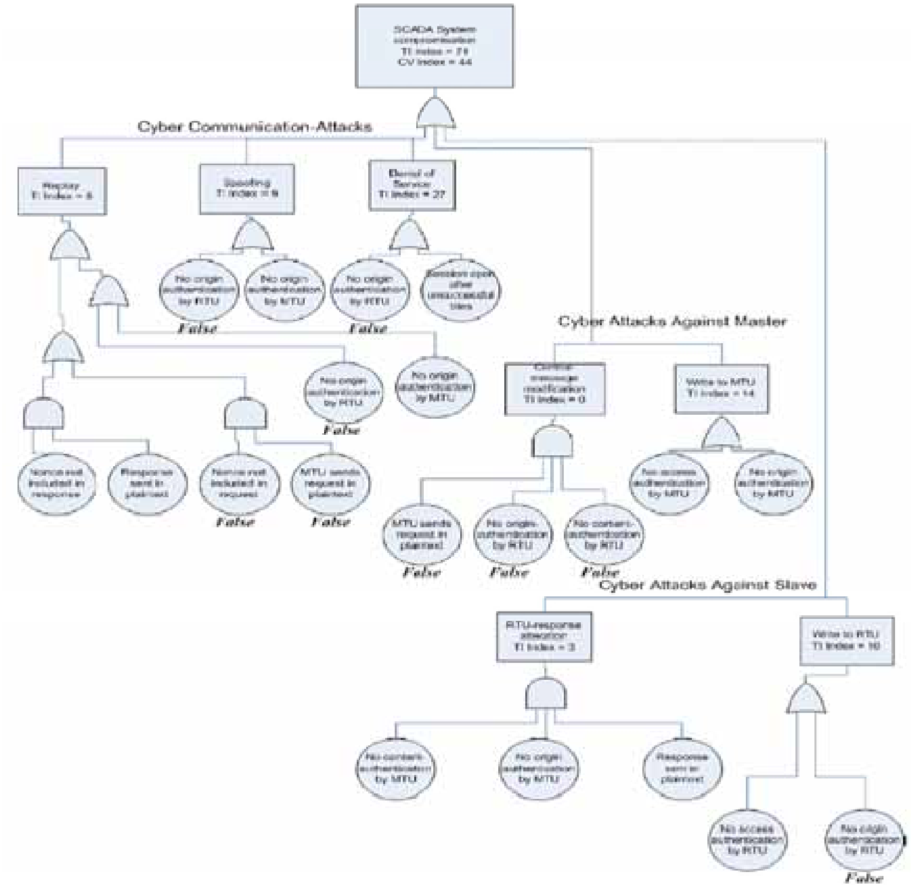

(a)
Organizational Metrics Activities
NIST SP 800-55
NIST SP 800-26
Corporate Governance Task Force ISG Assessment Questionnaire
Corporate Information Security Working Group (CISWG) Best Practices and Supporting Metrics
SSE-CMM
Security Capability Model
FITSAF
IA-CMM
NIST SP 800-37
DITSCAP (and forthcoming DIACAP, supported by eMASS)
NIST SP 800-53A
DoD CNDSP Metrics
Operational Metrics Activities
DoD IA Operational Readiness Metrics
SCORE
BSI 7799-4
Security Metrics Consortium
Metrics Produced by Vulnerability Scanners
Metrics Produced by Intrusion Detection Systems (IDS)
DLA Compliance Metrics
FIPS 199
DoDD 8500.1
SVA Risk Ranking
ISC INFOCON
NERC Threat Advisory Level
Statistics from BCIT Database
Incident Prioritization Approaches
CVSS
Other vulnerability scoring approaches (SANS, DISA, US-CERT)
Technical Metrics Activities
Common Criteria Evaluation Assurance Level (EAL)
NIST SP 800-53
DoDI 8500.2
IDS Comparison Metrics
SAMATE
ISECOM Risk Assessment Values
OWASP DREAD
(b)
1. PREPARATION
Identify Target Audience(s) for Metrics
Define Security & Metric Objectives
Identify the Measurable Attributes of Security Components that Can be Used to Develop Security Metrics
2. DEVELOPMENT
Select Key Measures
Identify Security Requirements, Standards, Best Practices, etc. Associated with the Key Measures
Select Benchmark for Key Measures
Formulate Basic Metrics
3. PROCESSING
Organize & Aggregate Metrics to Meet Assessment Goals
Incorporate Existing Metrics
Develop Approach for Displaying Metrics (i.e., Data Visualization)
4. APPLICATION
Decision Makers Evaluate Metrics & Other Information Before Taking Action

Source: Adar, E. presentation at the CEPS Task Force, CEPS. Brussels, based on (a) “I3P Research Report No. 1. (2005) - Process Control System Security Metrics”. (b) “I3P Report No. 12, (2007) - Security Metrics Tools Final Report”.

In terms of risk assessment for critical (information) infrastructures, several methodologies are available, as amply described in the literature.

Risk assessment methods such as the Hierarchical Holographic Model (HHM), the Inoperability Input-Output Model (IIM), and the Risk Filtering and Ranking Method (RFRM) have been applied successfully to SCADA systems with many interdependencies and have highlighted the need for quantifiable metrics. Probability risk analysis (PRA) includes methods such as Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and Failure Modes and Effects Analysis (FEMA). For example, Ralston et al. (2007) discuss two recent methods (one based on compromise graphs and one on augmented vulnerability trees) that quantitatively determine the probability of an attack, the impact of the attack, and the reduction in risk associated with a particular countermeasure. Figure 16 below shows an example of vulnerability tree analysis developed by these authors.

Figure 16. Example of vulnerability tree


SCADA System compromisation TI index = 71 CV Index = 44
Cyber Communication-Attacks
Replay TI index = 6
Spoofing TI index = 9
Denial of Service TI index = 27
No origin authentication by RTU
No origin authentication by MTU
No origin authentication by RTU
Session open after unsuccessful tries
False
False
No origin authentication by RTU
No origin authentication by MTU
False
Nonce not included in response
Response sent in plaintext
Nonce not included in request
MTU sends request in plaintext
False
False
Cyber Attacks Against Master
Control message modification TI index = 0
Write to MTU TI index = 14
No access authentication by MTU
No origin authentication by MTU
MTU sends request in plaintext
No origin authentication by RTU
No content authentication by RTU
False
False
False
Cyber Attacks Against Slave
RTU-response alteration TI index = 3
Write to RTU TI index = 10
No content authentication by MTU
No origin authentication by MTU
Response sent in plaintext
No access authentication by RTU
No origin authentication by RTU
False

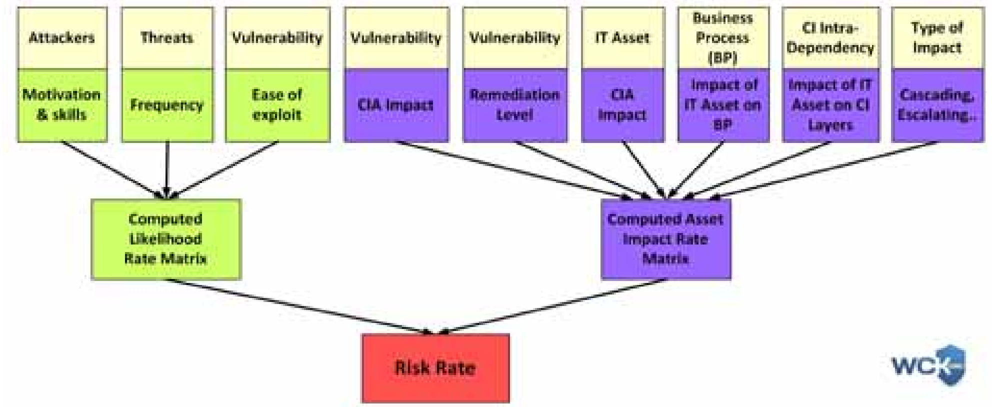
Source: Ralston et al. (2007).

3.2.2 A global framework for risk management

Assessing the risk level related to a given critical infrastructure by using a comprehensive, all-hazards approach has become a priority, in order to allow a better flow of information and increase the efficiency of the market and the risk management capacity of private and public actors. Figure 17, below shows an example of risk evaluation matrix for CIIP, tailored to the IT world, which is supposed to yield a determination of the risk rate related to a given infrastructure.

The integration of impact parameters of the IT assets related to the given infrastructure enables a more accurate quantification of the risk level. Such parameters include: hierarchy of the IT asset within its business process, the way it may affect other CI layers and the type of impact. The evaluation takes into consideration not only the immediate impact on the IT world, but also the potential consequences in relation to the given infrastructure. This process enables a better understanding of the nature of the IT risk, and subsequently, an appropriate illustration of remediation activities.

Figure 17. A risk evaluation matrix for CIIP



Source: E Adar, www.wck-grc.com (2010).

As shown on the left of the figure, the type of vulnerability, threat and attacker are translated into a computed likelihood rate matrix, which constitutes an input to the determination of the risk rate. The other input – represented on the right-hand side – is the computed Asset Impact Rate matrix, which incorporates information related to the 'CIA' impact, an assessment of the remediation level, the type of impact, as well as the level of intra-dependency of the critical infrastructure at hand.

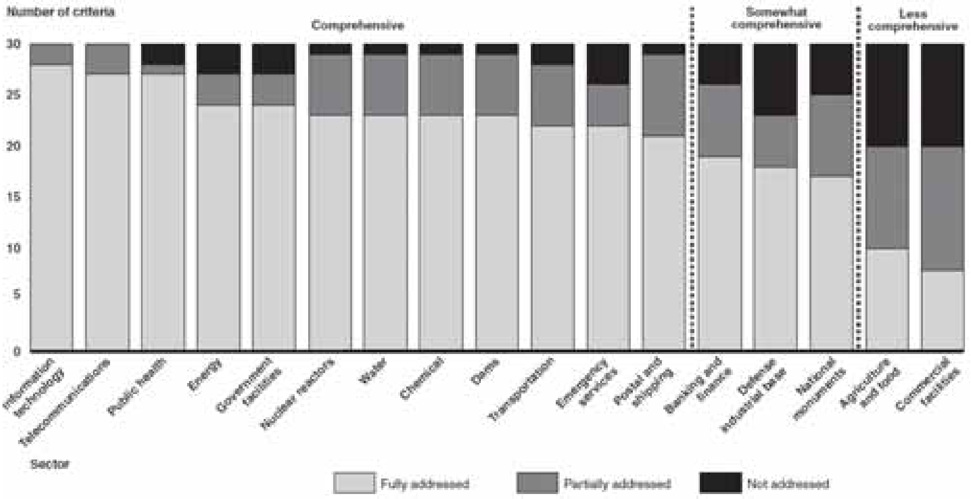
A global framework for CIP risk management could assist the industry by sharing information, procedures and best practices. In particular, it could facilitate:

- The development of common assessment methods, working procedures, libraries of controls and metrics (thresholds can be discussed on country or enterprise levels);
- Typical threats and attack scenarios, its characteristics and probability;
- Typical vulnerabilities scenarios, unknown vulnerabilities;
- Typical key IT processes for each sector;
- European aspects for each sector.

3.3 Assessing the EU's preparedness: Sectoral views

One of the key roles of the public sector in CIP is the analysis of the preparedness of specific sectors. Debate in the CEPS Task Force revealed that different sectors may exhibit different needs when it comes to the adoption of prevention and remediation methods, as well as for risk identification, assessment and management purposes. One example of assessment of the different levels of preparedness in different CIP domains is offered by a recent Government Accountability Report in the US, as shown in Figure 18 below.

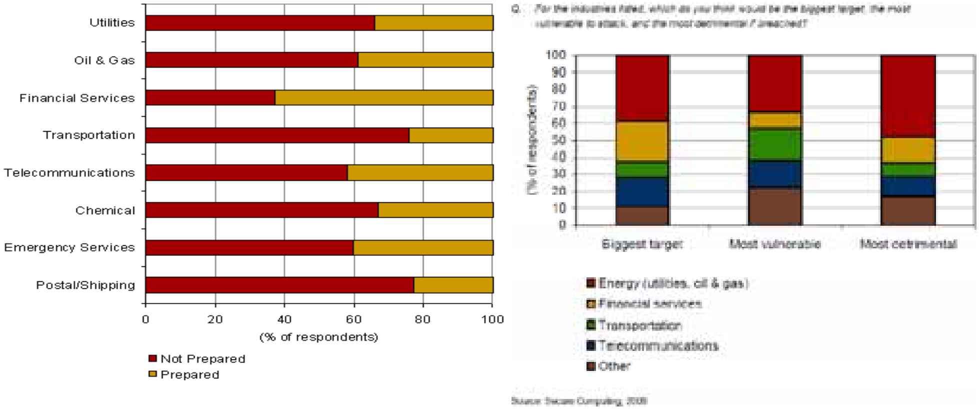
Figure 18. Comprehensiveness of sector-specific plans in the US



Source: GAO Report, GAO-08-64T, http://www.gao.gov/new.items/d0864t.pdf

In 2008, a survey of 199 leading experts in the CIP sector by Secure Computing yielded important results, in particular pointing to the energy sector as the one perceived as the most vulnerable and likely to be attacked in years to come.

Figure 19. Results of a survey



Source: Secure Computing, 2008

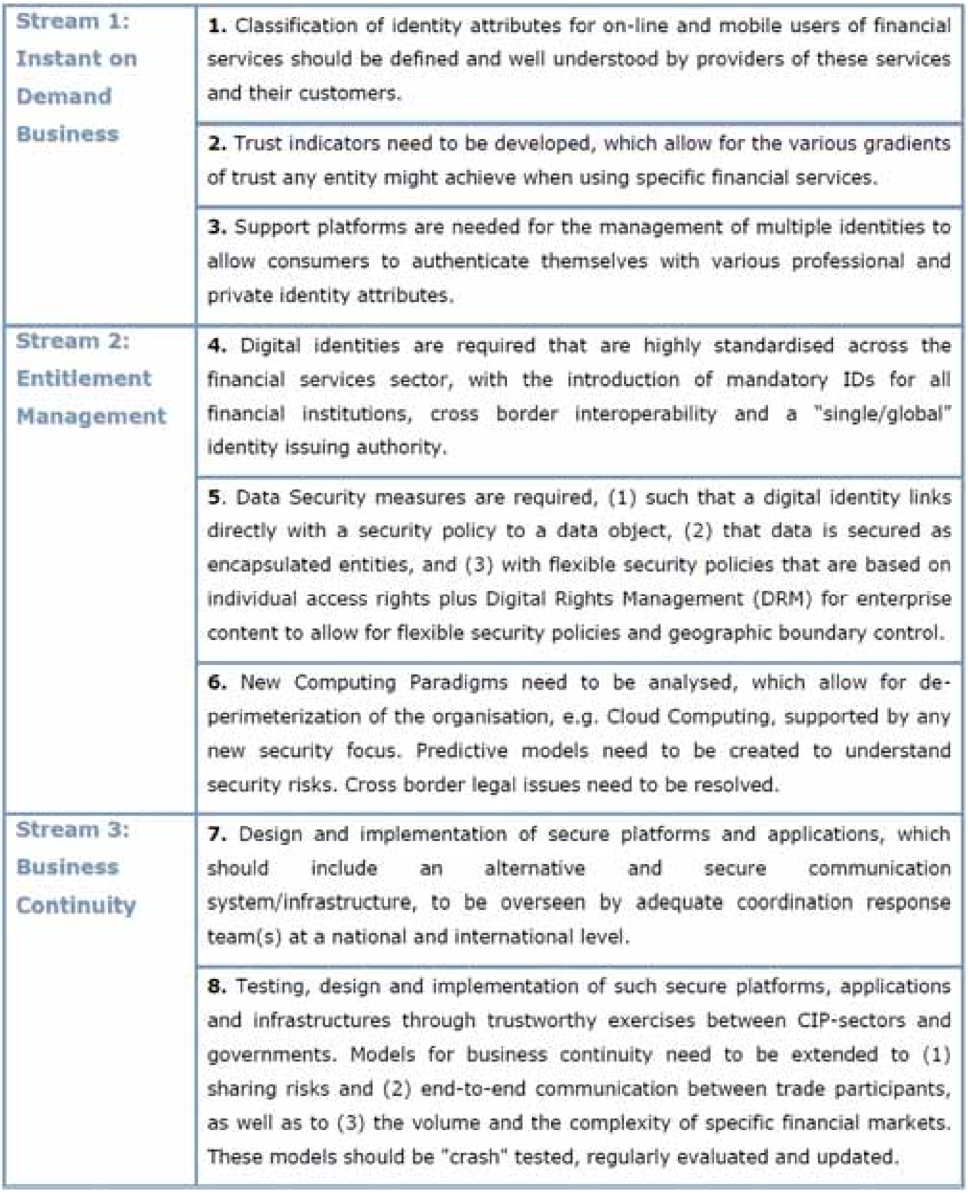
At the EU level, the analysis of preparedness in the 27 member states is still in its infancy. Below, we report the specific problems that emerged during the course of the CEPS Task Force meetings for a number of sectors, from financial services to energy, telecoms and IT.

3.3.1 Financial services

In the financial services sector, the main problems identified are intimately linked with the protection of the IT infrastructure. For example, global companies such as Swift rely on dedicated networks, resilience plans and service-level agreements (SLAs) in order to ensure business continuity in all parts of the globe.

A major research project termed PARSIFAL (Protection and Trust in Financial Infrastructures) has reached eight policy recommendations, which are summarized below, in Table 5.

Table 3. PARSIFAL main recommendations



Stream 1: Instant on Demand Business	**1.** Classification of identity attributes for on-line and mobile users of financial services should be defined and well understood by providers of these services and their customers.
	2. Trust indicators need to be developed, which allow for the various gradients of trust any entity might achieve when using specific financial services.
	3. Support platforms are needed for the management of multiple identities to allow consumers to authenticate themselves with various professional and private identity attributes.
Stream 2: Entitlement Management	**4.** Digital identities are required that are highly standardised across the financial services sector, with the introduction of mandatory IDs for all financial institutions, cross border interoperability and a "single/global" identity issuing authority.
	5. Data Security measures are required, (1) such that a digital identity links directly with a security policy to a data object, (2) that data is secured as encapsulated entities, and (3) with flexible security policies that are based on individual access rights plus Digital Rights Management (DRM) for enterprise content to allow for flexible security policies and geographic boundary control.
	6. New Computing Paradigms need to be analysed, which allow for de-perimeterization of the organisation, e.g. Cloud Computing, supported by any new security focus. Predictive models need to be created to understand security risks. Cross border legal issues need to be resolved.
Stream 3: Business Continuity	**7.** Design and implementation of secure platforms and applications, which should include an alternative and secure communication system/infrastructure, to be overseen by adequate coordination response team(s) at a national and international level.
	8. Testing, design and implementation of such secure platforms, applications and infrastructures through trustworthy exercises between CIP-sectors and governments. Models for business continuity need to be extended to (1) sharing risks and (2) end-to-end communication between trade participants, as well as to (3) the volume and the complexity of specific financial markets. These models should be "crash" tested, regularly evaluated and updated.

CEPS Task Force participants advocated for a twofold strategy in the financial services sector, aimed at coupling a national public-private partnership (PPP) with a Global Industry specific Partnership.[66] On the one hand, engaging in *national public-private partnerships* allows a better understanding of interdependencies in order to mitigate asymmetric surprises; in addition, it allows for a better monitoring of the supply chain of resources, and triggers effective regulatory advice and knowledge exchange.

Moreover, forming a *global industry-specific partnership and intelligence centre* is more controversial since it shares the potential shortfalls of national PPPs, but probably exhibits a higher administrative burden (due to the need for at least one interface per country of operation) and may feature conflicting objectives, despite the general wish of all participants to increase security. Also, the operation of a global partnership may be hampered by the excessively different knowledge base at the operational level, by the limited added value of the public sector in 'never owned' sectors and the questionable ability of international coordination given the vast complexity of the subject matter and the wide territorial coverage.

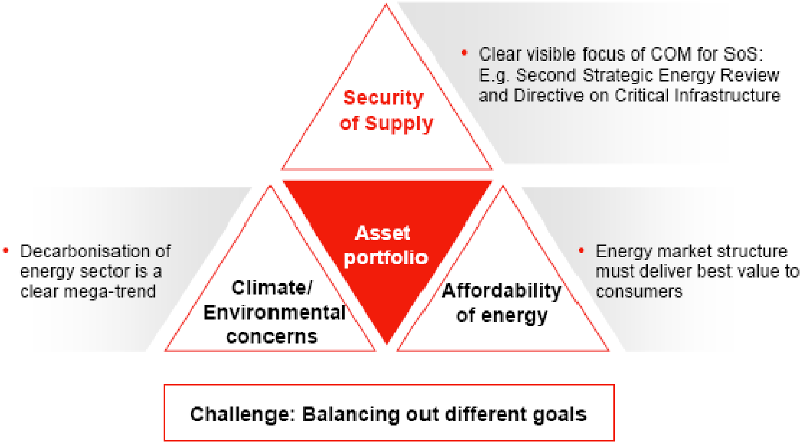
Coupling the two modes of governance would probably allow for maximum information-sharing, while still protecting the privacy requirements of firms. However, the problems in designing the global PPP would have to be carefully tackled beforehand.

3.3.2 Energy

In the energy field, the need to reduce costs and ensure security of supply may lead to conflicting public policy goals, and insufficient incentives on the side of private actors to invest in enhanced infrastructure resilience and robustness. Security of supply, climate and environmental concerns and the need to secure the affordability of energy for residential and business customers from what is termed the energy 'trilemma' (see Figure 20, below).

[66] Presentation by Kai Jensen-Kusk, CEPS Task Force, CEPS, Brussels.

Figure 20. The energy trilemma


• Clear visible focus of COM for SoS: E.g. Second Strategic Energy Review and Directive on Critical Infrastructure
Security of Supply
Asset portfolio
• Decarbonisation of energy sector is a clear mega-trend
Climate/ Environmental concerns
Affordability of energy
• Energy market structure must deliver best value to consumers
Challenge: Balancing out different goals

Source: Zafiriou (2010).

Security of supply is a cornerstone for economic development. Risks to energy supplies involve three components:

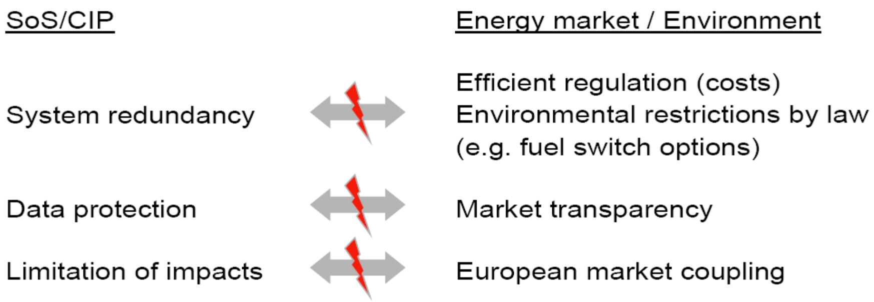
- Risks of targeted attacks on 'critical infrastructure' (e.g. terror, hacker);
- Influence of non EU-countries;
- Security of resources / raw-materials.

Zafiriou (2010) also explained the two different possible reasons for electricity supply disruptions:

- *A major failure due to violation of system parameters* (e.g. system breakdown due to frequency collapse after outage of technical equipment beyond (n-1)-security). The main characteristics of this type of incident are: i) the large-area supply disruption; ii) the absence of significant additional damage to network and other infrastructure assets; iii) relatively short-term recovery of supply expected (hours); and iv) reconstruction via "system re-configuration" (no additional resources needed).
- *Failure due to destruction of key infrastructure* (e.g. extreme weather conditions (snow, storm, flood) or targeted attacks). This type of incident possesses different features, such as: i) in general there is no system breakdown; ii) regional limited areas affected; iii) relatively long-term failure of supply possible (days / weeks); iv) reconstruction takes place via additional resources (material, personal).

A coherent framework for CIP is crucial as there are potential conflicts among the factors in the trilemma.

Table 4. Market-based v. security-based issues in the energy field



SoS/CIP		Energy market / Environment
System redundancy	↔	Efficient regulation (costs) Environmental restrictions by law (e.g. fuel switch options)
Data protection	↔	Market transparency
Limitation of impacts	↔	European market coupling

Source: Zafiriou (2010).

3.3.3 *IT and the cloud*

In the case of the IT industry (including telecoms), the most broadly acknowledged emerging issue is that of the security and resilience of cloud computing resources.[67] Today, the issue of cloud resilience is emerging as one of the key factors that will drive the future of the internet in years to come. Programmes such as IBM's "Resilient Cloud Validation", which evaluates the resilience of cloud service provider environments using a rigorous set of benchmarking and design validation programs, leading to a certification by IBM; or the Cloud Security Alliance, which promotes best practices in cloud security assurance; or ICASI - the Industry Consortium for Advancement of Security on the internet (ICASI) – which relies on a multi-supplier common effort for global incident response by leveraging bilateral or multilateral response experts to manage complex issues.

The main issue raised as regards cloud computing is that it adopts essentially a very efficient, though extremely centralized model. Cloud computing models transfer most of the computing work to centralised

[67] Other important issues related to this sector include the lack of redundancy in the undersea cable infrastructure, DNS vulnerabilities and the need to migrate to DNSSEC, etc. For a comprehensive analysis see the 2007 Study on Availability and Robustness in Electronic Communications Infrastructure (ARECI), available online at http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm.

servers, leaving end users' terminals as little more than 'dumb' terminals. This solution is seen as a cost-effective, but not always resilient solution. If we accept that 'resilience design' principles include concepts such as diversity, redundancy, decentralisation, transparency, collaboration, flexibility, openness and others, cloud computing may appear too centralised to match all the requirements.[68] On the other hand, data centre security and mirroring of data centres may also make many cloud applications more resilient, especially compared to current solutions adopted by SMEs that lack specific skills and expertise. All in all, cloud computing seems to exhibit a different risk profile, which calls for the need to properly set up IDM and access management. These issues will have to be carefully taken into account and addressed before cloud computing becomes the dominant means of using IT resources.

[68] See Jamais Cascio, *Dark Clouds,* at http://openthefuture.com/2009/01/dark_clouds.html. See also Creane, M., *Security: Why every cloud needs a resilient lining,* BT White Paper, at http://globalservices.bt.com/static/assets/pdf/white_papers/riskpaper_why_every_cloud_needs_a_resilient_lining_en.pdf.

CHAPTER 3: MAIN FINDINGS

- The economics of CIP features important peculiarities, from the need to solve the efficiency-security trade-off to principal-agent problems, positive and negative externalities leading to possible market failure, the difficult but promising role of liability and insurance, and behavioural problems related to rational ignorance and bounded rationality. In addition, CIs feature a unique combination of low-probability (due to existing protection measures) and very significant consequences of accidents. All these issues call for a coordinated public-private intervention.
- There is a strong need for establishing a common taxonomy, metrics and a common risk management framework for CIP-related risks and threats, possibly leading to a common framework for the CIP cycle overall. Standardisation in this domain – also relying on existing standards from e.g. ISO, NIST and ANSI – would significantly improve the circulation of best practices and the development of a mature insurance market.
- The assessment of EU preparedness is still in its infancy, and is necessarily sector-specific. The different scale of emerging problems and risks may warrant different solutions in sectors that are more national in scope (e.g. transport) compared to others that feature more cross-country (inter-)dependencies (e.g. energy, e-communications).
- Coupling national PPPs with a global partnership and intelligence centre in the financial sector would be the best way to increase the resilience of the financial infrastructure. However, global action is made very difficult due to the heterogeneity of potential participants, as well as conflicting interests, diverging knowledge bases and high transaction costs.
- In the energy sector, security of supply, climate and environmental concerns and the need to secure the affordability of energy for residential and business customers form a peculiar ‘trilemma’ that must be solved by carefully balancing all the interests and incentives at stake.
- In the IT sector, there is currently intense debate about cloud computing, especially in terms of its resilience and security. Excessive centralisation of computing may lead to more and essential dependence of networks and must be taken into account in the development of new business models.

4. ADDRESSING POLICY CHALLENGES: TOWARDS A HOLISTIC APPROACH TO C(I)IP

In the previous sections we identified the policy problems related to the protection of critical infrastructure as lying in particular in the increased importance, complexity, interdependence and vulnerability of existing infrastructures; the increased importance of the information infrastructure; the need to build capacity and awareness and examine the possible role that incentives can play in the creation of an effective system of critical infrastructure protection.

Against this complex background, any meaningful CIP policy should be based on the need to develop tools that are able to address the market failures that may emerge in different sectors. This means, specifically:

- *Providing a clear risk management and assessment framework* to help address the informational asymmetry problem;
- *Promoting information-sharing between public policy-makers* to reduce the informational asymmetry and create synergies and economies of scale and scope in identifying risks, vulnerabilities and (inter-)dependencies of critical infrastructures;
- *Building up a central CIP modelling and simulation centre for the EU* to allow cross-border and multilateral infrastructure simulation, understanding complexity, dependencies and cascading effects;
- *Facilitating information-sharing and cooperation between public and private agents*, to ensure coordination in promoting the public goal of securing resilience of critical infrastructures and dissemination of best practices;
- *Promote awareness-raising initiatives* to ensure that actors at all layers of the CI value chain are sufficiently alerted of the importance of critical infrastructure protection, and mainstream CI protection in the policy process at EU and national level.
- *Take action to ensure that missing CIP profiles and skills are developed* through university education, in order to avoid a shortage of key professional profiles on an issue that will increase in

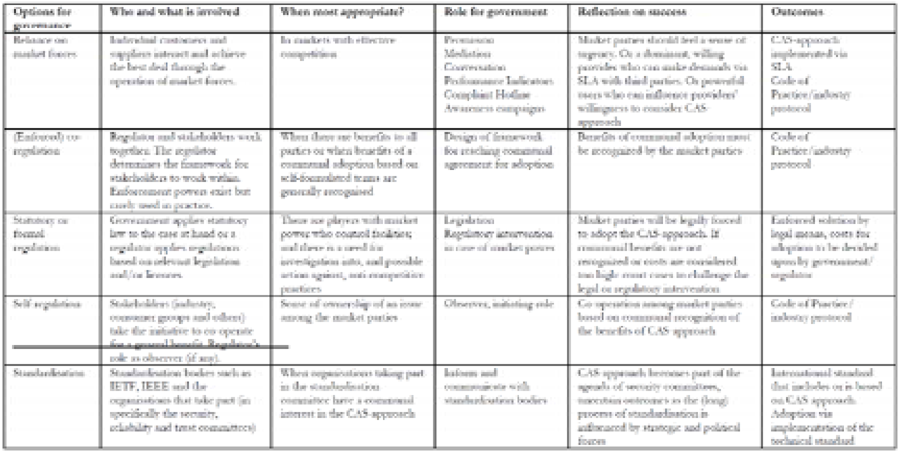
importance in years to come. The development of the CIP professional knowledge and capability profile is especially important.

Below, we explore these issues in more detail. Section 4.1 deals with the public policy issues related to inter-governmental cooperation and multi-level governance between the EU and member states. Section 4.2 briefly hints at the transatlantic dimension by advocating stronger cooperation in the field of security and CIP within the existing Transatlantic Economic Council. Section 4.3 offers suggestions related to the upcoming EP3R, and Section 4.4 comments on the need for skills in the domain of C(I)IP as a public policy problem to be dealt with at the EU level. Section 4.5 discusses ways to mainstream critical infrastructure protection in the European Commission's policy cycle.

4.1 Shaping the public-private partnership

Intervening in the field of CIP requires selecting – above all – the mode of intervention that proves most appropriate for the specifics of the problem at hand. The literature on regulatory reform and responsive regulation can help find the right way to intervene in this complex policy domain. In particular, social sciences have gone a long way towards providing guidance on the 'what', 'why' and 'how' of public policy intervention. For example, Ubacht (2010) refers to a scheme initially developed by Oftel, the UK telecommunications regulator, and advocates for the development of a co-regulatory scheme in the field of CIP.

Table 5. Options for governance



Options for governance	Who and what is involved	When most appropriate?	Role for government	Reflection on success	Outcomes
Reliance on market forces	Individual customers and suppliers interact and achieve the best deal through the operation of market forces.	In markets with effective competition	Promotion Mediation Conversation Performance Indicators Complaint Hotline Awareness campaigns	Market parties should feel a sense of urgency. Or a dominant, willing provider who can make demands via SLA with third parties. Or powerful users who can influence providers' willingness to consider CAS approach	CAS-approach implemented via SLA Code of Practice/industry protocol
(Enforced) co-regulation	Regulator and stakeholders work together. The regulator determines the framework for stakeholders to work within. Enforcement powers exist but rarely used in practice.	When there are benefits to all parties or when benefits of a communal adoption based on self-formulated teams are generally recognised	Design of framework for reaching communal agreement for adoption	Benefits of communal adoption must be recognized by the market parties	Code of Practice/industry protocol
Statutory or formal regulation	Government applies statutory law to the case at hand or a regulator applies regulations based on relevant legislation and/or licences.	There are players with market power who control facilities; and there is a need for investigation into, and possible action against, anti-competitive practices	Legislation Regulatory intervention in case of market power	Market parties will be legally forced to adopt the CAS-approach. If communal benefits are not recognized or costs are considered too high court cases to challenge the legal or regulatory intervention	Enforced solution by legal means, costs for adoption to be decided upon by government/ regulator
Self regulation	Stakeholders (industry, consumer groups and others) take the initiative to co operate for a general benefit. Regulator's role as observer (if any).	Sense of ownership of an issue among the market parties	Observer, initiating role	Co operation among market parties based on communal recognition of the benefits of CAS approach	Code of Practice / industry protocol
Standardisation	Standardisation bodies such as IETF, IEEE and the organisations that take part (in specifically the security, reliability and trust committees)	When organisations taking part in the standardisation committee have a communal interest in the CAS-approach	Inform and communicate with standardisation bodies	CAS approach becomes part of the agenda of security committees, uncertain outcomes to the (long) process of standardisation is influenced by strategic and political forces	International standard that includes or is based on CAS approach. Adoption via implementation of the technical standard

Source: Ubacht (2010), ECN newsletter (quoting Oftel).

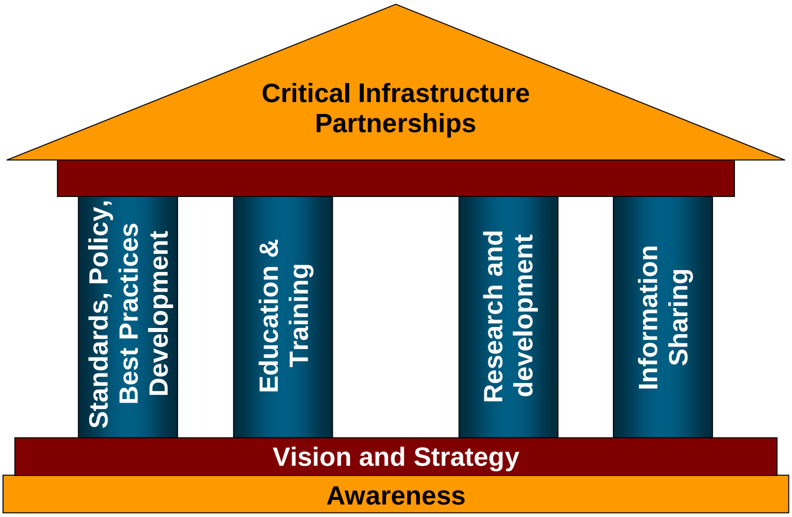
Against this background, the most appropriate approach depends on the possibility of establishing an effective principal-agent scheme that ties the actions of public and private players to clearly defined objectives, and establishes incentive schemes and sanction mechanisms in case some of the involved parties deviate from the agreement reached. In addition, the choice of the best governance system also depends on:

- The degree of informational asymmetry between public and private actors, as well the completeness of the information available to private players, including both local service providers and mostly global suppliers, each experiencing completely different problems and information.
- The transaction cost that would emerge in an inter-governmental scheme, compared with the benefits that such a scheme may bring;
- The (transaction) costs of a public-private partnership scheme, especially if compared to the corresponding benefits.
- The degree of legal certainty that a given policy option would ensure for public and – most importantly – private players.

In other words, the decision related to the most appropriate governance option is essentially a cost-benefit one, which should be subject to a careful impact assessment.

Looking at the governance architecture, the CEPS Task Force hosted a lively debate that led to the identification of the need for a holistic approach to CIP policy. Figure 21, below shows the key foundations and pillars of CIP policy as described during CEPS Task Force meetings.

Figure 21. Key pillars of a CIP strategy



Source: Chris Gow, meeting 4.

First, there is a strong need for an overall **vision** of what CIP should achieve both from an *ex ante* and *ex post* perspective (see above, Section 2.2), together with a **strategy** and **strong political commitment** to achieve the desired results. Such a vision should be disseminated among all stakeholders and CI owners/operators in order to promote **awareness** of the need for a CIP policy. Vision, strategy and awareness can be described as the essential foundations of any effective CIP policy.

Second, the main pillars that must be built on the foundations described above include:

- The development of **standards** and the sharing of **best practices**, which aim at solving – as far as possible – the problem of incomplete information that affects current CIP policies. This implies:
  - A thorough risk assessment aimed at the identification of gaps, and in particular the cases in which the lack of policies and standards causing a decrease in the ability to protect CIs;
  - the identification of key stakeholders, including both organisations, businesses and groups of individuals;
  - the identification of solutions based on interaction and agreement between stakeholders; and
  - the enactment of policies.

- The promotion of **education and training** initiatives, in order to fill the skills gap and contribute to raising the awareness of private and public operators as regards the importance of protecting critical infrastructure. This entails:
  - Efforts and investment in the field of education to improve and transform the academic environment, producing graduates (i.e. future workforce) with knowledge and skills targeted at CI development and protection;
  - Promote **training** initiatives to develop and constantly update the skills of the current a future workforce in a way that is commensurate with the needs of CI protection.
  - **Sourcing** efforts, to get the right people into the right jobs, including identification, tagging, placement, gap analysis, career development, and skills assessment.
- Third, there is a need to promote **research and development** to constantly invent new technological solutions to effectively protect CIs. This requires, inter alia, continual gap analysis, identification and abridgement. R&D investment must be targeted at CIP needs, in particular when it comes to ensuring that evolving threats are given updated prevention and remediation strategies.
- Fourth, **information-sharing** must be ensured to maximize the preparedness of CI owners/operators and speed up emergency responses. One of the key reasons for creating a public-private partnership for CIP is information-sharing. In this respect, it is essential to decide and define what information should be shared between private and public partners, and at what moment in time. Table 9, below shows the main dimensions of information-sharing, as emerging from the US debate and as potentially applicable to the EU PPP.

Table 6. Information-sharing in the US: Key dimensions

What to share	Who should share	When to share	Protecting information
Government: ▪ Threat intelligence ▪ Warnings and advisories **Private sector:** ▪ Vulnerabilities ▪ Solutions ▪ Advisories ▪ Advice	▪ Intelligence agencies ▪ Law enforcement agencies ▪ CI owners / operators ▪ Coordination partnerships (at all levels)	**Pre-event** ▪ Advisories ▪ Warnings **During and after the event** ▪ Remediation steps ▪ Coordination of resources	▪ Use of PKI (public key infrastructure) ▪ Strong policies (with penalties for misuse) ▪ Must protect both private / proprie tary and government information

Source: Ken Watson, meeting 4.

The main components of information-sharing can be summarized as follows:

- *Coordination*. To achieve better coordination actors must identify gaps in policies and standards, identify stakeholders, agree on solutions jointly, and enact policy through legislation.
- *Capability enhancement*. This can be achieved through improvements in education, training, and sourcing (i.e. identifying the right roles and getting the best people into these roles).
- *Innovation through R&D*. An effective R&D strategy includes identifying resources for R&D and establishing effective research processes. Research should be dedicated to analysing where CIP gaps exist. It should also contain a mechanism whereby the results of R&D can be subject to continuous feedback as well as be deployed.
- *A focus on funding/building capabilities that can be used by various trust models* (or affinity groups) such as a secure conferencing capability, secure electronic communication, encrypted key exchange, etc. These common secure capabilities could be rolled together to facilitate the necessary trusted information-sharing needs by a particular group.
- *Common operational picture* for information-sharing. As shown in Table 9, governments and industry should work together to establish who shares what, and when. The table offers some recommendations on how tasks could be divided among the public and private sector

for information-sharing, as well as what agencies could be involved in the process.

- The final component is *institutionalised trust*. This can be achieved by establishing core competencies for government and the private sector, as well as mechanisms for governing information exchange. For example, trust must be built into the institutions so that when an employee leaves the replacement must be trusted quickly.[69]

4.1.1 Focus: The trust dimension

Compared with other policy domains, in CIP policy trust plays a very prominent role. Given the limited availability of information and the consequent need for information-sharing between governments, as well as between public and private players, building trust becomes the only possible way to develop a meaningful and coordinated CIP policy.

However, several problems can emerge with respect to the objective of building reasonably long-term trust.

- *Intergovernmental trust may be limited in a global context*, since some governments are often considered to be involved in cyber attacks aimed at stealing valuable information from other governments and/or private players – this problem may be less evident at the intra-EU level;
- *Supranational PPPs may face a problem of size*. As pointed out by national experts in the CEPS Task Force, PPPs can obtain important results if the number of participants does not become excessive.[70] When the number and the national origin of participants increase, transaction and coordination costs, together with a lack of trust between parties, may skyrocket. This requires a novel approach that is more scalable than the existing national PPPs. If successful, it will serve as a model for a globally-scalable approach.

[69] It needs to be noted however, that there are different trust models depending on the goals of the information-sharing activity – for example, sharing network sensor data related to a specific attack during a national incident has an entirely different trust model than sharing threat or vulnerability trend data related to the attacks seen over the past six months. The PPP should therefore be flexible enough to comprehend these various models.

[70] Presentation by Timo Hauschild, at the CEPS Task Force, Brussels.

- *PPPs may be sector-specific by nature.* For example, the optimal geographical dimension of a PPP on energy may be larger than a PPP on transportation networks, which tend to be more national in scope and exhibit a lower number of cross-border inter dependencies. And when it comes to the internet, clearly information-sharing and trust should be global, as the threats and risks coming from this infrastructure are virtually borderless.

In all this, trust stands as a key concept. The CEPS Task Force has debated extensively the conditions for trust, from confidence to challenges, and reached the conclusion that trust needs specific rules, a key definition of roles and incentives, and the protection of information. In particular, in order to build trust there should be:

- rules for the coordination of emergency responses.
- persistent reputation and attribution.
- balanced with effective privacy and personal data protection.
- common metrics to ensure monitoring of efforts and results.

Another aspect of information-sharing and intra-industry cooperation for CIP is the need to provide legal certainty for what concerns practices that are allowed, and those practices that may be considered as infringing existing rules such as, antitrust law, for example. At the EU level, more clarity would be needed, especially in those cases where information exchange potentially touches upon sensitive information such as price levels or technology choices, which may be interpreted by antitrust authorities as signs of collusion between competing firms.

In the US, the Homeland Security Act (Public Law 107-296, Sec. 214) allows information defined as critical infrastructure information to be exempted from the Freedom of Information Act (FOIA). Since the approach to information-sharing between competitors is more rigid in Europe than in the US in antitrust terms, action would be needed to clarify the conditions under which competing firms may be allowed to share critical infrastructure information (CII) without incurring antitrust sanctions.

At the EU level, the recent European Commission impact assessment on the Communication on CIIP approaches the problems related to the creation of a PPP in an explicit way:[71]

[71] See COM(2009)399 of 30.3.2009.

> public-private partnerships (PPPs) have emerged as the reference governance model because they seem the most reasonable mechanism to manage the peculiar combination and intersection of governments' and private sector's role and responsibilities. However, PPPs are quite challenging to implement in practice, as information exchange mechanisms between governments and the private sector basically become a trust issue … although there is a general consensus that PPPs … can be a workable solution, the European dimension of such an approach has not materialised so far.

4.2 The EU policy-making process and CIP

There was agreement among Task Force participants that the EU can play a leading role in facilitating global cooperation. In particular, the EP3R presents a key opportunity for Europe to engage local and global industry players in guiding and reviewing important aspects of emerging cyber policy. This is likely to result in the application of effective policy levers, ensuring that emerging technologies are well addressed, and ensuring alignment with other similar initiatives outside the EU. In this respect, Europe can also act as a model for the rest of the world.

However, several critical factors stand on the way of the launch of a successful EP3R. In particular, the size of the expected PPP, the need to accommodate several diverging interests at the same table, the sectoral specificities that would have to be merged into a single platform, and the difficulty of allocating responsibility in what is still chiefly a national prerogative may prove very difficult issues to address, and could potentially undermine the success of this very welcome initiative. Below, we discuss the main obstacles to the development of a comprehensive and effective CIP policy in the EU, while Section 4.2.2 contains suggestions on how to mainstream CIP objectives into the broader context of EU policy-making.

To be sure, the EP3R will have to be complemented by actions at the policy level. Establishing a level playing field among Europe's member states is crucial to defining a consistent and effective policy for CIIP. However, at this point individual member state priorities on CIP and CIIP differ widely and a careful approach to defining the right progressive goals and providing incentives to national governments is required to bridge the gap.

At the same time, European policy must address the fragmented approach to CIP across the member states decisively. A subsidiarity test must be applied to identify the functions that should exist at EU level and the ones that are most effectively addressed at member state level.

In addition, what makes things even more difficult is that the level playing field that must be established between member states must be one that allows for a real paradigm shift in the way we think about security, resilience and disaster management (or response capabilities). The issue of critical infrastructure protection has today become so important that it must be effectively mainstreamed into the policy-making process of EU and national institutions.

In many cases, this may provoke the emergence of policy trade-offs between the goal of increasing short-term static efficiency through cost-cutting strategies (especially in times of financial crisis) and the need to ensure longer-term resilience and dynamic efficiency by providing a reasonably safe environment. The trade-off between short-term efficiency and resilience, however, is not the only one that is likely to emerge. As we have shown in this report, the objective of cyber security may clash with that of protecting users' privacy and personal data on the internet (e.g., in case deep packet inspection is used), and a similar problem emerges also in many real-life situations. In addition, there may be a tension between the goal of preserving an open internet – in the extreme version so far adopted by some net neutrality advocates – and that of building a more secure cyberspace, where traffic is filtered to avoid spam, malware and easy attacks to the information and physical infrastructures on which our lives and businesses increasingly depend.

To be sure, a reasonable C(I)IP policy should not only look at recovery measures and emergency response, but also focus on striking an efficient balance between prevention and cure. This also means that the "infrastructure of critical infrastructure protection" must be strengthened through the development of adequate skills in the labour market, and the creation of a fruitful interaction between players that shape CIP policy, from government to the private sector to CERTs/CSIRTs, ISACs, WARPs and many others. This, in turn, also means that responsibility for action to protect critical infrastructure should be efficiently allocated to the cheapest cost avoiders, and incentives to behave efficiently must be introduced into the legal system to a larger extent than occurs today.

These are the challenges faced by many national governments around the world. Recent gatherings between CIP experts – including, most notably, those organised by ENISA – have testified to a variety of national experiences, some of which have reached maturity and also relative success. In all this, the European Union faces the big challenge of having to coordinate 27 member states, some of which also have a federal structure; and the huge opportunity of becoming the leading force in this field by stimulating interaction and dialogue between private and public actors in a way that subsequently triggers a more global exchange. Furthermore, an approach that will work across 27 EU member states will serve as an excellent model for addressing similar challenges globally.

4.2.1 Policy recommendations for EU CIP policy in the future

While recognizing that the European Commission is already very active in many fields of CIP, with encouraging prospects, the CEPS Task Force recommends that increased attention be given to the following aspects of future CIP policy.

4.2.1.1 Perform a thorough, forward-looking subsidiarity test

Subsidiarity is a well-established principle in EU policy-making, and postulates that policy action be taken at the most efficient level within a multi-level governance context. In the case of CIP policy, many policy actions are currently taken at national level, but the need to reach synergies and economies of scale in information-sharing, the increasing interdependence between infrastructures and between countries, as well as the inter-links between physical infrastructure and the information infrastructure create a strong argument for coordination of CIP policy at the international level. This is why the European Commission should run a thorough, in-depth subsidiarity test to clearly identify areas where acting in common (between the EU27) is more desirable, and areas that may remain under national competence in CIP, CIIP and for each of the sectors involved.

In the impact assessment on the Communication on CIIP mentioned above, the European Commission observes that:

> Because of the high interconnectedness between CII and societal systems, which rely upon CII, it is unfeasible, ineffective and counterproductive, and would run against the basic principles underlying the European Union, for each member state to only guard its own backyard. Certain failures in one member state will unavoidably produce effects in another. This is why it is necessary for all the member states to coordinate their efforts in one direction

> and to try and achieve a satisfactory level of preparedness with a similar timescale …For the reasons stated above, the proposed policy action fully respects the principle of subsidiarity, in its dual dimension of respect for the added-value test (it would be difficult for any member state to achieve the objective by itself) and of the boundary test (European action will be limited to what member states cannot achieve satisfactorily by themselves, providing a framework for coordination and, where appropriate, complementing their activities).

A subsidiarity test must draw the line between what is to be done at the EU level and what will remain under the control of national governments. In this respect, it must be recalled that the European Commission already identified as European critical infrastructure the CIs that affect two or more member states. In carrying out the subsidiarity test, however, the Commission should also carefully look at existing domino effects and interdependencies between infrastructures, a domain in which we reportedly do not have sufficient information today. For example, a pure national transport network may be attacked as a way to create a disruption of a cross-border energy network: in this case, also the operation of national CIs that are interconnected with European or global CIs should be subject to procedural obligations and minimum resilience standards. The internet, which is emerging as the next Critical Infrastructure, is an example of an infrastructure that cannot be effectively governed at the national level.

4.2.1.2 Centralise EU CIP governance

The European Commission and EU bodies in charge of CIP policy are well aware of the importance of an all-hazards approach, which takes into account all types of risks and threats, independently of whether they come from natural events or are purely man-made. In line with a consolidated trend in many national governments, an efficient treatment of information flows and emergency responses require that the governance of CIP policy be centralised in the hands of a single institution. The EU must thus empower a single agency to deal with CIP and CIIP issues, given the increasing interlinks between the two domains (another consolidated trend in many countries).

In order to be fully effective in its mission, the institution responsible for the EU CIP must have full mandate for:

- Managing the process of identification European CI;

- Driving sectoral risk assessment on the identified EU CI;
- Collecting data from public and private players to enable sustainable risk identification, assessment and management as regards European CI;
- Managing the process of prioritizing gaps and investment;
- Distributing funds and incentives to maximize the benefit to EU;
- Continually assessing the level of European preparedness;
- Coordinating response to events that affect European CI.

Furthermore, the organisation will need to establish trusted working relationships with member state organisations responsible for national CIP as well as national and international private sector CI operators.

4.2.1.3 Make it possible to 'call the EU'

Many of the CEPS Task Force participants highlighted the fact that, in the event of warnings or an actual crisis, it is currently impossible to 'call the European Union'. This problem should be addressed by the Commission in the months to come, also in light of the need for a more coordinated and centralised CIP policy at the EU level. In more detail, the EU must launch a 'Call EU' hotline for emergency management and early warning, located in the agency in charge of CIP and CIIP (see above), to ensure that predetermined protocols agreed between national public institutions are triggered and coordinated from the central EU level. This capability should feature a method for sharing information related to threats and vulnerabilities in a timely manner with EU member national responders. Such a channel to push information out in a timely and coordinated manner across the EU would be a great improvement.

In addition, legal responsibility should be attributed to the central EU line for failure to react and / or follow predetermined procedures to ensure timely and effective emergency prevention / response.

4.2.1.4 Keep the PPP small and sector-specific

Participants to the CEPS Task Force highlighted the problem of size in the creation of a successful PPP. The public-private partnership must be structured in a way that does not lead to an excessively large group, and is potentially structured on a sectoral basis, with interactions between sectors aimed at locating interdependencies. Given the increasing importance of the information infrastructure for almost all physical infrastructures, it would be important to secure the presence and help of organising IT suppliers (including the global vendors and integrators), which improves the quality and timeline of the support and facilitates negotiation between stakeholders.

Moreover, also based on our reasoning in Section 4.1.1 above, governance of the PPP may end up being impossible if transaction costs and administrative burdens related to its operation skyrocket. This, in turn, would also create a trust problem due to conflicting interests, different levels of knowledge and potential free riding behaviour. Accordingly, it would be advisable to give the PPP a clear focus and goals, and then organise the work in a reasonable group size on a sectoral basis or in a still more fragmented fashion.

4.2.1.5 Develop common risk metrics and standards

The European Commission has a unique opportunity to lead the development of common standards that would facilitate the flow of information and the achievement of economies of scale in CIP policy, both in and outside the territory of the Union. As discussed in Section 3 above, CIP policy – also given the structural gap between attack and defence in terms of information gathering and scope of action – urgently needs a degree of standardisation in the identification, classification and treatment of risks and threats.

Accordingly, the EU should promote the development and adoption of common risk metrics and standards for risk identification, assessment and management in the field of CIP and CIIP. EP3R emerges as the right forum to initiate this process.

This, in turn, would also facilitate the development of a mature insurance market, which would help to disseminate and update market information on existing risks and remedies in a timely and efficient way.

4.2.1.6 Adopt a flexible policy approach

Threats, risks and technologies that revolve around the protection of critical infrastructure constantly evolve, making it difficult to adopt a traditional ‘command and control approach’ to policy-making. As already mentioned, the need to provide for efficient prevention and remediation phases involves both a constantly updated set of information, as well as the strong participation of the CI owners/operators and their key supply chain partners. Hence, a flexible approach to policy is essential. More specifically, the approach to CIP policy at the EU level could usefully draw the existing 'new approach to standardization', a policy approach that stands as one of the most successful reforms enacted in the history of the EU. This approach entails establishing through primary legislation only the general principles and main outcomes sought through EU CIP policy, and leaving it to the industry to devise the best technical measures (at any given point in time) that fulfil the desired levels of resilience.

4.2.1.7 Address the 'skills gap'

As observed in Section 3 above, both R&D and education policies are essential pillars of a comprehensive CIP policy. At the EU level, there is currently too little attention paid to the need to develop education and training curricula to ensure that the growing demand for an interdisciplinary profile able to deal with complex CIP issues is satisfied. The EU, through its framework programmes for research and its education policy, should provide incentives and funding to universities that want to offer higher education and lifelong training in these fields.

4.2.1.8 Develop common modelling and simulation capabilities

The recently launched Digital Agenda for Europe already highlights the need to carry out large-scale attack simulation and test mitigation strategies as of 2010. In this respect, the need to exploit synergies and reach adequate economies of scale in the understanding and detection of threats and risks, as well as in mitigation and remediation strategies leads to the need to build up a central CIP modelling and simulation centre for the EU. This would be an essential step to allow cross-border and multilateral infrastructure simulation, understanding complexity, dependencies and cascading effects.

A good example of a research project that looks at existing capabilities for simulation is the DIESIS project, also presented at the CEPS Task Force. The project final report recognises that "in contrast to the utmost importance of critical infrastructures like electricity and telecommunication for all European citizens, the European economy and the European society at large, the understanding of the complex system of critical infrastructures with all their dependencies and interdependencies is still immature".[72] In order to address these challenges, DIESIS proposes to

[72] See the DIESIS report on available infrastructure simulators, at http://www.diesis-project.eu/include/Documents/Deliverable2.3.pdf

establish the basis for a European modelling and simulation e-infrastructure based upon open standards to foster and support research into all aspects of critical infrastructure with a specific focus on its protection. Developing modelling and simulation tools that enable a better understanding of the interdependency of European critical infrastructures is a prerequisite for an adequate solution for Critical Infrastructure Protection (CIP) strategies.

The DIESIS project was funded by the European Union 7th Framework Programme for Research, and led to important technical and non-technical results, including i) an ICT architecture and a work flow for member states and administrations in CIP; ii) an interoperability middleware for CI simulators; iii) a communication middleware for distributed federated simulation via the internet; iv) an ontology for CI in railway transport, electrical power transmission, and telecommunication; v) a working demonstrator, a distributed federated simulation coupling four simulators (SINCAL™, NS2, Open Track™, Aqua).[73] In addition, the project included a study of the legal and economic aspects of carrying out simulation work and the potential business model for the simulation centre European Infrastructures Simulation and Analysis Centre (EISAC). The results of DIESIS are a very good starting point for future work in this direction.

4.2.2 Mainstreaming CIP objectives into EU policy-making

Protecting critical infrastructures requires constant attention to the consequences of policy actions in several fields. That said, how can one make sure that CIP policy is always kept in the picture when developing EU policies? There are three main ways to achieve this result in the years to come:

- First, impact on CI could be introduced as a mandatory step in the Commission’s Impact Assessment system, whenever the policy issue at hand potentially affects, even if indirectly, the resilience or vulnerability of CIs. This way, Commission DGs in charge of proposing new policy initiatives would have to consider the impact on CIs at a very early policy stage, and this could guarantee a more balanced approach to EU policy-making.

[73] See Stephan Pickl, presentation at the CEPS Task Force, 4th meeting, CEPS, Brussels.

- Second, new methodologies to stress-test existing policies (i.e. the ‘stock’ rather than the ‘flow’ of rules) should be developed through public funding of *ad hoc* research projects. In particular, these projects should follow up on already funded projects to consolidate knowledge on how to model interdependencies between CIs and potential cascading effects triggered by failures of given infrastructures. A first attempt to achieve this result was already made by Luiijf et. al. (2006).
- Third, indicators for the success of national and EU-wide information-sharing initiatives are needed. As observed by one of the Task Force participants, success criteria could include the level of senior engagement in the process, establishing a form of public-private partnership, coordinating a multi-agency approach, having an all-hazards understanding of risk, establishing clearly defined goals for risk management, and demonstrating a value to all stakeholders. But also parameters related to the estimated preparedness and response capacity of the member states will be needed in the years to come.

CHAPTER 4: MAIN FINDINGS

- The key foundations of a CIP policy are a widely communicated vision and strategy, together with strong political commitment. The key pillars are then the development of standards and best practices, education and training, R&D and information-sharing, and modelling and EU-wide simulation capabilities.
- Trust is a key dimension in any CIP policy, but needs time, clear rules, sector-specific arrangements and a limited size of the PPP: this may create problems in international and EU cooperation efforts.
- A thorough subsidiarity test should be run at an early stage to clearly identify areas where acting in common is more desirable, and areas that may remain under national competence in CIP, CIIP and for each of the sectors involved.
- The EU must empower a single agency to deal with CIP and CIIP issues adopting an all-hazards approach; and launching an EU number for emergency management and early warning, located in the same agency.
- The public-private partnership must be structured in a way that does not lead to an excessively large group, and is potentially structured on a sectoral basis.
- The EU should promote the development and adoption of common risk metrics and standards for risk identification, assessment and management in the field of CIP, as well as the development of a mature insurance market.
- The EU should adopt a flexible approach to CIP policy, by establishing through primary legislation only the general principles and main outcomes sought through EU CIP policy, and leaving it to the industry to devise the best technical measures that fulfil the desired levels of resilience.
- CIP-related issues can be mainstreamed into the EU policy-making process in three main ways: i) including CIP impacts in the Impact Assessment Guidelines and in *ex post* evaluation; ii) developing methodologies for stress-testing EU policies in terms of their impact on critical infrastructure; iii) developing indicators to track the success of national and EU-wide information-sharing initiatives.

SELECTED REFERENCES

Anderson, R. (2001), *Why Information Security is Hard—An Economic Perspective,* Proceedings of the 17th Annual Computer Security Applications Conference, pp. 358–65. IEEE Computer Society.

Anderson, R. and S. Fuloria (2010), *On the Security Economics of Electricity Metering*, Harvard University, WEIS'10, 08-06-2010.

Anderson, R., and T. Moore (2006). *The Economics of Information Security*, Science, 314(5799): pp. 610–13.

Anderson, R., R. Böhme, R. Clayton and T. Moore (2008), *Security Economics and the Internal Market*, for ENISA in February 2008, and available online at http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec.

Andersson, J.J. and Malm, A. (2006), Public-Private Partnerships and the Challenge of Critical Infrastructure Protection', in Dunn, M. and Mauer, V. (Eds), International CIIP Handbook 2006 Vol II, Center for Security Studies, Zurich, pp. 139–166.

Anti-phishing Working Group internet Policy Committee (2008), *Anti-Phishing Best Practices Recommendations for Registrars*, An APWG IndustryAdvisory. http://www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf.

Baer, W.S. (2003), *Rewarding IT Security in the Marketplace*, in: TPRC 2003.

Boin, A., Ekengren, M. and Rhinard, M. (2006), 'Protecting the Union: Analyzing an Emerging Policy Space', Journal of European Integration, Volume 28, Number 5, pp. 405–421.

Boin, R.A. and McConnell, A. (2007), *Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience*, Journal of Contingencies and Crisis Management, Volume 15, Number 1, pp. 50–59.

Bouwmans, I., M. P.C. Weijnen and A. V. Gheorghe, *Infrastructures at Risk*, in A.V. Gheorghe, M. Masera, M Weijnen and De L. Vries (2006), "Critical Infrastructures at Risk", Springe Netherlands, 2006, pp 19-36.

Brunner, E. and M. Suter, *International CIIP Handbook 2008/2009*, available online at http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=91952&lng=en.

Calabresi, G. (1970), *The Costs of Accidents: A Legal and Economic Analysis*, New Haven: Yale University Press.

Cascio, J. (2009) *Dark Clouds*, at http://openthefuture.com/2009/01/dark_clouds.html.

Clarke, L. (2005), *Worst Cases: Terror and Catastrophe in the Popular Imagination*, University of Chicago Press, Chicago.

Computer Economics (2007), *Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and other Malicious Code*, at http://www.computereconomics.com/ page.cfm?name_Malware%20Report.

Council of the European Union (2004), 'EU Solidarity Program on the consequences of terrorist threats and attacks (revised/widened CBRN Programme', Council Document Number 15480/04 (Internal), 1 December 2004.

Creane, M. (2010), *Security: Why every cloud needs a resilient lining*, BT White Paper, at http://globalservices.bt.com/static/assets/pdf/white_papers/riskpaper_why_every_cloud_needs_a_resilient_lining_en.pdf.

Cukier, K. N., V. Mayer-Schoenberger, and L. Branscomb (2005), *Ensuring (and Insuring?) Critical Information Infrastructure Protection* (October 2005). KSG Working Paper No. RWP05-055. Available at SSRN: http://ssrn.com/abstract=832628.

de Bruijne, M. and van Eeten, M. (2007), 'Systems That Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment', Journal of Contingencies and Crisis Management, Volume 15, Number 1.

Duke, S. and Ojanen, H. (2006), 'Bridging Internal and External Security: Lessons from the European Security and Defence Policy', Journal of European Integration, 28, 5, pp. 477–494.

European Commission (2004), 'Communication from the Commission on Critical Infrastructure Protection in the fight against terrorism', COM(2004)702 final, Brussels, 20 October 2004.

——— (2005a), Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005)576 final, Brussels, 17 November 2005.

——— (2005b) Communication from the Commission on Pandemic Influenza Preparedness and Response Planning in the European Community, COM(2005)0607 final, Brussels, 28 November 2005.

——— (2006a) Green paper: A European Strategy for Sustainable, Competitive and Secure Energy, COM(2006) 105 final, Brussels, 8 March 2006.

——— (2006b) The European Programme for Critical Infrastructure Protection (EPCIP), MEMO/06/477, Brussels, 12 December 2006.

——— EU policy on secure Information Society, http://ec.europa.eu/information_society/policy/nis/index_en.htm

——— Page on EU CIIP activities, http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

——— ARECI study, http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm

——— Workshop on large scale attacks, http://ec.europa.eu/information_society/policy/ nis/strategy/activities/ciip/large_scale/index_en.htm

——— Public consultation “Towards a Strengthened Network and Information Security Policy in Europe”, http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm? item_id=4464

Executive Order (1996), President of the United States, ‘U.S. Executive Order 13010 on Critical Infrastructure Protection 11949’, 15 July 1996.

Gorbil, G. and E. Gelenbe (2009), *Design of a Mobile Agent-Based Adaptive Communication Middleware to Enable Federations of Critical Infrastructure Simulations*. In: Pre-proceedings of the fourth International Workshop on Critical Information Infrastructures Security (**CRITIS '09**), Erich Rome, Robin Bloomfield (eds.), Sankt Augustin: Fraunhofer IAIS, 2009, pp. 145-160. Conference: Bonn, Germany, September 30-October 2, 2009

Hellström, T. (2007), *Critical infrastructure and systemic vulnerability: Towards a planning framework*, Safety Science, Vol. 45, Issue 3, March 2007, pp. 415-430.

Keysan, J.P., R.P., Majuca and W. J. Jurcic (2004), *The Economic Case for Cyberinsurance*, at http://law.bepress.com/cgi/viewcontent.cgi?article=1001&context=uiuclwps.

Landes, W.M. and R. A. Posner (1987), *The Economic Structure of Tort Law*, Cambridge (MA): Harvard University Press.

LaPorte, T.R. (2007), 'Critical Infrastructure in the Face of a Predatory Future: Preparing for Untoward Surprise', Journal of Contingencies and Crisis Management, Volume 15, Number 1.

Laprie, J-C., K. Kanoun and M. Kaâniche (2008), *Modelling Interdependencies between the Electricity and Information Infrastructure,* SAFECOMP-2007, Springer, LNCS 4680-0054, Germany, September 2007.

Luiijf, H.A.M., Klaver, M.H.A. (2005), *International Interdependency of C(I)IP in Europe (Internationale Verflechtung von C(I)IP in Europa)*, In: B.M. Hämmerli, S. Wolthusen (Eds), *Proceedings of CIP Europe 2005 - Critical Infrastructure Protection*, GI CIS Forum, Bonn, Germany, 19 September 2005

Luiijf, H.A.M., and Klaver, M.H.A. (2006), *Protection of the Dutch Critical Infrastructure,* International Journal of Critical Infrastructures Volume 2, Number 2-3/2006, Pages 201-214.

Luiijf, H.A.M., Burger H.H., and Klaver, M.H.A. (2008), *Critical (Information) Infrastructure Protection in the Netherlands,* working paper, available at http://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-1.pdf.

Masucci, V., F. Adinolfi, G. Dipoppa, P. Servillo and A. Tofani (2009): *Ontology-Based Modeling and Simulation of Critical Infrastructures*. To appear in: Proceedings of the 2009 Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection (IFIP CIP 2009). Conference: Hanover, New Hampshire (US) March 22-25, 2009

Matzén, N. and Svantesson, M. (2005), 'Annex to Draft Report: An Inventory of Crisis Management Mechanisms, Procedures and Institutions Currently in Place at the EU Level', Research report available at the European Union Crisis Management (EUCM) project website: www.eucm.leidenuniv.nl, first published February, 2005.

Molnar, D. and S. Schechter (2010), *Self Hosting vs. Cloud Hosting: Accounting for the security impact of hosting in the cloud*, WEIS'10.

Monti, M. (2010), *A New Strategy for the Single Market*, available online at http://ec.europa.eu/bepa/pdf/monti_report_final_10_05_2010_en.pdf.

Moore, T., R. Clayton, and R. Anderson (2009), *The Economics of Online Crime*, Journal of Economic Perspectives, Vol. 23, N. 3, Summer 2009, pages 3–20.

OECD (2008), *Protection of 'critical infrastructure' and the role of investment policies relating to national security*, OECD: Paris, 2008.

Oxford Economics (2010), *The Economic Impact of air travel restrictions due to the volcanic Ash*, 2010, report available online at http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/aktuell.parsys.87229.DownloadFile.tmp/economicimpactsofvolcanoinisland2010.pdf

Prather Brown, J. (1973), *Toward an Economic Theory of Liability*, 2 Journal of Legal Studies 323-350.

Rinaldi, S. M., J. P. Peerenboom, and Terrence K. Kelly (2001), *Critical Infrastructure Interdependencies*, IEEE Control Systems Magazine, 2001.

Rome, E., S. Bologna, E. Gelenbe, E. Luiijf, V. Masucci (2009): *DIESIS - Design of an Interoperable European Federated Simulation Network for Critical Infrastructures*. In: Proceedings of the 2009 SISO European Simulation Interoperability Workshop (ESIW '09), Simulation Councils, Inc., San Diego, CA, USA, ISBN 1-56555-336-5, pp. 139-146. Conference: Istanbul, Turkey, July 13-16, 2009.

Shavell, S. (1987), *Economic Analysis of Accident Law*, Cambridge (MA): Harvard University Press.

Stiglitz, J.E. (2002), *Information and the change in the paradigm in economics*, American Economic Review, 92(3):460–501, June 2002.

Ubacht, J. (2010), *Complex Adaptive Systems – an Approach to increase Dependability*, European CIIP Newsletter April/May 2009, Volume 5, Number 1, at 16-20.

Van Eeten, M. and J. M. Bauer, (2009) *The economics of malware*, in: OECD, Computer viruses and other malicious software, Paris: Organisation for Economic Co-operation and Development.

Varian, H. R. (2004), *System Reliability and Free Riding*, in Economics of Information Security, Kluwer, 2004.

GLOSSARY OF TERMS

Alerts & Warnings. Information about NIS threats, disseminated by all possible means. Usually alerts & warnings must be accompanied by recommended actions the user should take to mitigate a threat arising on the internet.

CERT (Computer Emergency Response Team). An organisation that studies computer and network security in order to provide incident response services to victims of attacks, to publish alerts concerning vulnerabilities and threats and to offer other information to help improve computer and network security.

CSIRT (Computer Security and Incident Response Team). Another term for CERT.

Culture of security. Awareness about NIS-related matters and the corresponding behaviour of internet users, defined by the OECD guidelines "Towards a culture of Security".

EISAS (European Information Sharing and Alert System). A placeholder for a yet-to-be determined role that the European Union can take in the area of sharing NIS information with citizens and SMEs. Describes a concept, not necessarily a physical system.

ENISA (European Network and Information Security Agency) is an agency of the European Union created in 2004 by EU Regulation No 460/2004 and fully operational since 1st September 2005. The objective of ENISA is to improve network and information security in the European Union.

Hacker. A person who studies and explores software and systems with the aim of finding the weaknesses and vulnerabilities that allow him/her to break into remote computers.

Home-users. In the context of this study, a generic group of people who use the internet at home, as a tool, without deep knowledge about how it works.

NIS. Abbreviation for Network and Information Security.

Sensor network. A system using sensors to gather overall information about the current state of the network. A sensor is usually a computer system or a packet routing device connected to a network that collects information about data traffic in the segment to which it is connected.

SME. Small (fewer than 50 employees) and Medium (fewer than 250 employees) Enterprises. The numbers vary in the various member states. A more precise term would be 'micro businesses'.

Virus. Malicious code that might replicate itself and infect other computers with the help of a user (i.e. opening an e-mail or an attachment).

Vulnerability. Weakness in software or hardware or its configuration that may lead to a break-in or otherwise compromise the security of a system.

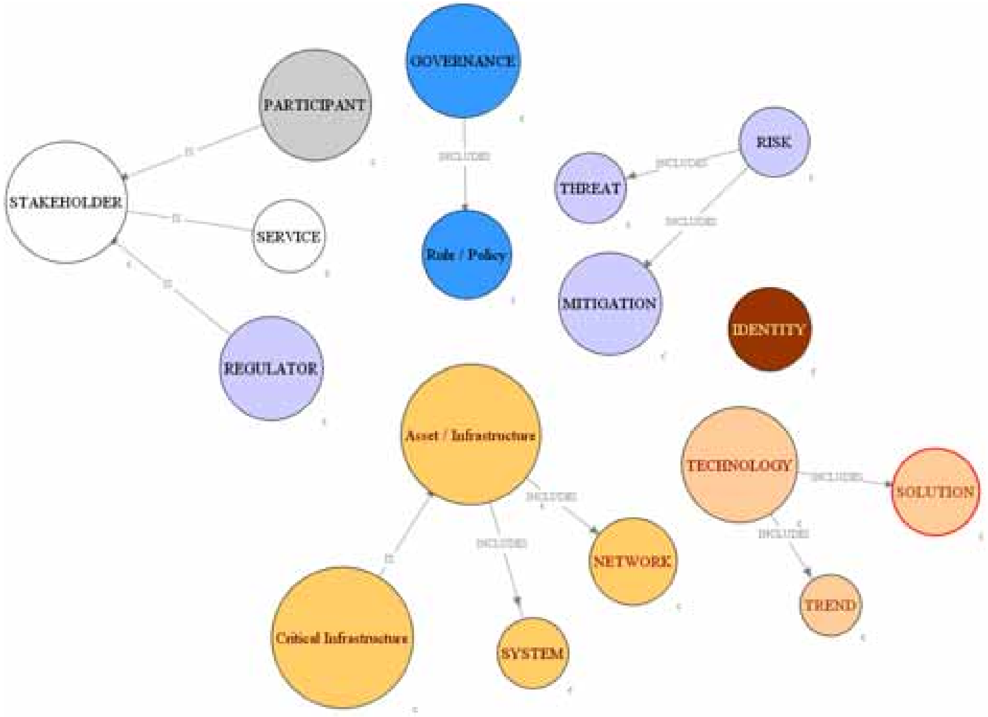
Worm. Malicious code that replicates itself and infects other computers without the interaction of a user.

XML (Extensible Markup Language). A data format widely used to facilitate the sharing of different types of data.

Financial Services: the Parsifal Glossary[74]

The glossary lists top-level concepts coming from different areas of expertise in CIP. Some of them are very technical, including those from CIIP common methodology. Others are closer to finance business players or supervisors. This glossary regroups concepts by ‘proximity’. Proximity may arise from hierarchical relationship (father-son, whole-part, derivation or extension). It may also result from the attachment of a concept to a specific area.

Top & Level 1 Categories of Parsifal Glossary



[74] J.-Yves Gresser, Draft Ontology Of Financial Risks & Dependencies Within & Outside The Financial Sector, Vol. 2, D2.1 Parsifal Projects, http://www.parsifal-project.eu/images/PublicDeliverables/parsifal%20d2.1%20draft%20ontology%20of%20financial%20risks%20and%20dependencies%20within%20and%20outside%20the%20financial%20sector.pdf

LIST OF TASK FORCE MEMBERS, INVITED GUESTS AND SPEAKERS

CHAIR: **Bernhard Hämmerli**
President, Swiss Informatics Society
bmhaemmerli@acris.ch; bmhaemmerli@bluewin.ch

RAPPORTEUR: **Andrea Renda**
Senior Research Fellow, CEPS
Andrea.Renda@ceps.eu

MEMBERS OF THE TASK FORCE

Mr. Eyal Adar
Founder & CEO
White Cyber Knight

Mr. Henning H. Arendt
President
Arendt Business Consulting

Mr. Ahmet Fethi Ayhan
Inf. Network Operations Systems Manager
Turk Telekom

Mr. Matt Broda
Senior Security Strategist
Critical Infrastructure Protection
Microsoft

Ms. Teresa Calvano
Associate Director
Fleishman-Hillard

Mr. Greg Day
Director of Security Strategy
McAfee

Ms. Paola Di Maio
W3C EIIF XG: Emergency Information Interoperability Framework Incubator Group

Mr. Philip Eder
Senior Account Executive
Fleishman-Hillard Company

Mr. Robert Filippini
Scientific Officer
Joint Research Centre

Mrs. Karen Gadd
RSA - Western Europe
BP International
karen.gadd@uk.bp.com

Mr. Andrea Glorioso
Policy Officer
DG INFSO - European Commission

Mr. Antonio Hilario Garcia del Riego
Head of Corporate Affairs in the EU
Banco Santander

Mr. Christopher Gow
Program Manager
Global Policy & Government Affairs
Cisco

Mr. Jean-Yves Gresser
Vice Chairman
The Black Forest Group Inc.

Mr. Timo Hauschild
Senior Expert on internet Security and CIIP
German Federal Office for Information Security (BSI)

Mr. Staffan Jerneck
Director & Director of Corporate Relations, CEPS

Mr. Martin Johns
Senior Researcher
SAP AG

Mr. Christoph Luykx
Public Policy Manager
Intel Corporation

Mr. Christian Krassnig
Policy Officer, F1 Fight against terrorism,
Justice, Freedom and Security, European Commission

Mr. Kai Jensen-Kusk
European Head of Business Continuity Management
Corporate Securtiy & Business Security
Deutsche Bank AG

Mr. Goran Mihelcic
Research Assistant
Department of Computer Science
University of the Federal Armed Forces, Munich

Mr. Simon Milner
Partner
Jardine Lloyd Thompson Ltd

Mr. Christopher Napoli
Research Assistant, CEPS

Mr. Harry Newman
Head of Banking Initiatives EMEA
Swift

Mr. Reginald Otten
Consultant
Fleishman-Hillard Company

Mr. Evangelos Ouzounis
Senior Expert - IT Security Policies
ENISA

Mrs. Maria Joao Paixao
Account Director
Brunswick Group

Mr. Jean-Paul Peers
Vice President - Energy Policy
Siemens AG

Dr. Stefan Pickl
Professor, Chair for Operations Research,
Department of Computer Science
Universität der Bundeswehr, München

Ms. Audrey Plonk
Senior global policy specialist
Intel Corporation

Mr. Neil Robinson
Senior Analyst
Rand Corporation

Mr. Erich Rome
Project Manager
Adaptive Reflective Teams
Fraunhofer Institute for Intelligent Analysis and Information Systems

Ms. Lorna Schrefler
Research Fellow
CEPS

Mr. Andrea Servida
Deputy Head of Unit
DG INFSO
European Commission

Pastora Valero
Director EU Public Policy
Global Policy and Government Affairs
Cisco

Mr. Harald Vogt
Senior Researcher
SAP AG