COSMOTE
our world is you

seccrit
SEcure Cloud computing for CRitical infrastructure IT

Critical Infrastructures and Challenges for Enhanced Security and Network Management

Dr. Ioannis Chochliouros
Evangelos Sfakianakis

17th INFOCOM World Conference 2015

Athens, Greece - November 24, 2015

OTE
GROUP OF COMPANIES

SECCRIT

SEcure Cloud computing for CRitical infrastructure IT

(Ασφαλής υπολογιστική νέφους για κρίσιμες υποδομές τεχνολογιών πληροφορικής)

Grant Agreement No.312758.

Contents

Introduction – Essential Conceptual Framework

Discussion upon Critical Infrastructures and about essential concerns of the related European policy

CI - *Conceptual definition* (I)

The term* "Critical infrastructure (CI)"** implicates for a **particular asset -or a system-** which is necessary for the **maintenance** and the **continuity** of ***vital societal functions.

The **damage** to a critical infrastructure, its **destruction** or **disruption** ***by natural disasters, terrorism, criminal activity or malicious behaviours***, *may have an important negative impact for the security of the EU and the well-being of its citizens.*

The ***term "infrastructure"*** *usually describes the underlying basis of an organization or system (for example a country) and* ***includes****, in principle:*

- *Information and Telecommunications Systems;*
- *Banking and Financial Institutions;*
- *Water, Electricity, Oil and Gas supplies;*
- *Transportation and Logistics structures, and;*
- *Health and Emergency services.*

The ***word "critical"*** is more appropriate than *"infrastructure"*, **for making a conceptual distinction** between ***normal operating procedures*** and ***strategic security policy*****.**

CI - *Conceptual definition* (II)

Actual European challenges:

- **The reduction of CIs' vulnerabilities and weaknesses *in parallel with effort to "improve"/"raise" their resilience,* is one among the *well defined* objectives of the present and the contemporary EU policy.**

- **An acceptable level of protection has to be provided and guaranteed, *while harmful effects of disruptions on the society and/or upon the citizens need to be reduced!***

CI - *Conceptual definition* (III)

CIs comprise those physical resources, services, and IT facilities, networks and infrastructure assets which, ***if disrupted or destroyed***, would have a severe impact and influence on the *health, safety, security or economic well-being of citizens or the effective functioning of European or local governments.*

There are three types of "corresponding" infrastructure assets:

- **Public, private and governmental infrastructure assets and interdependent cyber & physical networks.**
- **Procedures and *-where relevant-* individuals that exercise control over critical infrastructure functions and/or operations.**
- **Objects having cultural or political significance as well as "soft targets" *which may also incorporate mass events* *(i.e.: sports, leisure and cultural).***

European Critical Infrastructures (I)

The term **European Critical Infrastructure (ECI)**

implies those specific physical resources, services, and IT facilities, networks and infrastructure assets, which,

if disrupted or destroyed,

would have a serious impact on the **health, safety, security, economic or social well-being**

of two or more Member States (MS).

European Critical Infrastructures (II)

- The **pure definition** of ***"what may constitute an EU critical infrastructure"*** **is given by its cross-border effect,** which ascertains *whether an incident could have a serious impact beyond two or more MS national territories*.

***This is conceived as "the loss of a critical infrastructure element", and is rated by the following criteria*:**

- **Extent of the geographic area** *which could be affected by the loss or unavailability of a critical infrastructure element beyond three or more Member State's national territories.*
- **Effect of time** *(i.e. the fact that a for example a radiological cloud might, with time, cross a border).*
- **Level of the so-called *"interdependency".***

European Critical Infrastructures (III)

"*Interdependency*" is a bidirectional relationship between two infrastructures, through which ***the state of each infrastructure influences or is correlated to the state of the other*** *(for example, an electricity network failure in one MS affecting another).*

There are four types of interdependencies for critical infrastructures:

- ***Physical:*** *The operation of one infrastructure depends on the material output of the other.*
- ***Cyber:*** *Dependency on information transmitted through the information infrastructure.*
- ***Geographic:*** *Dependency on local environmental effects, simultaneously affecting several infrastructures.*
- ***Logical:*** *Any kind of dependency not characterized as Physical, Cyber or Geographic.*

European Critical Infrastructures (IV)

According to the context of the ***Council Directive 2008/114/EC***, **an EU critical infrastructure is** *an "asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".*

The scope of the Directive was originally limited to the energy and transport sectors…

- However, it has constituted the **"first step",** *in a step-by-step approach*, to detect, identify and then designate ECIs and so assess the need to improve their protection.
- ***The Directive outlined the approach all Member States would be required to follow*** **to identify, designate, and protect ECIs in the energy and transport sectors**, ***while indicating the ICT sector as a priority for possible future expansion of its scope.***
- The majority of Member States have implemented the provisions of this Directive by incorporating them within their national legislative and regulatory frameworks, *through a variety of approaches.*

Critical Infrastructure Protection (I)

CIs can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity & malicious behaviour.

To save the lives and property of citizens being at any kind of potential risk in the EU territory from any cause (terrorism, natural disasters and accidents), **any disruptions or manipulations of CI should, *to the extent possible*, be brief, infrequent, manageable, geographically isolated and minimally detrimental *to the welfare of the Member States, their citizens and the European Union*.**

The effective CI protection implies for a proper level of communication, coordination, and cooperation nationally and at EU level, among all interested parties, *including:*

- *Owners and operators of infrastructure*,
- *regulators*,
- *professional bodies* and *industry associations* ,
- in collaboration with *all other sectors of government*, and *the wider public*.

Critical Infrastructure Protection (II)

Critical Infrastructure Protection (CIP) is about ensuring that services vital to the society continue to function, *even after the occurrence of any harmful event.*

It also implicates the **capability to *prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction***, *when some of these may appear and threaten the proper operation of the corresponding asset.*

The general European objective of CIP is to raise critical infrastructure protection capabilities across all EU Member States against all possible hazards.

*The **underlying rationale** is that disruption to infrastructures providing "key services" could harm the security and economy of the EU as well as the well-being of its citizens and so* **it is essential to work for proper prevention and/or counter measures**.

Critical Information Infrastructure (I)

The term ***"Critical Information Infrastructure (CII)"*** refers to *all ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, fibre optics, etc.).*

These infrastructures are necessary for the correct operation of most other CIs and compose a vital tool *for managing risk factors* and *for "returning infrastructures to order", after a breakdown occurs.*

Critical Information Infrastructure Protection (CIIP) **refers to the programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities**
which aim ***at keeping the performance*** *of critical information infrastructures in case of failures, attacks or accidents,* ***above a defined minimum level of services***
and also aim ***at minimising the recovery time and damage.***

CIIP is a shared responsibility ***among state, local, tribal, and territorial entities, and public and private owners and operators of critical infrastructure.***

European Strategic Framework (I)

- ***Basic Aim***

  The **assurance of a high degree of protection of EU infrastructures and the increase of their resilience** (*against all threats and hazards*), *so that to minimise the consequences of loss of services to society as a whole.*

- ***Two essential strategic frameworks***
  - ***Stockholm Programme (2009)***
  - ***EU Internal Security Strategy (2014)***

European Strategic Framework (II)

Stockholm Programme (2009)

- **Notification of the importance of critical infrastructure protection**. The EU has identified as one of its major objectives the reduction of critical infrastructure vulnerabilities.
- **Member States have been invited to draw up and implement policies** to improve measures for the protection, security preparedness and resilience of critical infrastructure, also including Information and Communication Technology (ICT) and services infrastructure.
- **Further analysis and review of the essential Directive 2008/114/EC,** in order to consider including additional policy sectors.

EU Internal Security Strategy (2014)

- **Critical infrastructure must be better protected from criminals who take advantage of modern technologies** and that the EU should continue to designate critical infrastructure and put in place plans to protect such assets, as they are essential for the functioning of society and the economy.
- **Threats to critical infrastructure require enhancements to long-standing crisis and disaster management practices in terms of efficiency and coherence.**
- **Focus on** better risk assessment **and** risk management.

European Strategic Framework (III)

The **objective of CI protection at the EU level is to provide satisfactory guarantee** *that there are*

- ***adequate and equal levels of protective security on CI***
- ***minimal single points of failure and***
- ***rapid, tested recovery arrangements***

throughout the EU.

The level of the ensured protection may not be equal for all potential sorts of and can be relevant to the impact caused by the potential failure of the CI.

The related European policy and strategy is a continuing process and it so implicates for systematic reviews to identify, assess and consider any new issues and/or related concerns.

Objectives:

- *Development of a commonly accepted framework towards achieving, to the extent possible, a common level of protection.*
- *Avoiding negative impact or consequences between member states, in particular due to the high expansion of modern Future Internet (FI)-based technologies and applications, in parallel with current market liberalisation initiatives.*
- *Sufficient protection implicates for communication, coordination, and cooperation nationally, at EU level (where relevant), as well as internationally.*

European Strategic Framework (IV)

Principles taken into account in order to compose the essential framework for CI protection:

- Subsidiarity
- Complementarity
- Confidentiality
- Stakeholder Cooperation
- Proportionality
- Sector-by-sector approach

European Strategic Framework (V)

Subsidiarity: Explicit priority is given for the CI protection and **the related action becomes an action of national responsibility**. **Thus, the national governments need to work together with any involved "market actors" *(i.e., owners and/or operators*) according to a well-defined and common context.**

Complementarity: **The proposed set of measures and/or actions has to complement any previously existing measures**. In case where there are specific contexts already established and/or validated, these have to remain active in order to support the overall performance of any new action.
Complementarity also needs to be ensured with other Community and Union programmes and related initiatives *(i.e.: European Union Solidarity Fund and the Civil Protection Financial Instrument, **Horizon 2020** and the Structural Funds).*

Confidentiality: **Any necessary action for information sharing about CI has to be done in a way to provide sufficient guarantee about trust and confidentiality**.
This implicates that that CIP information has to be classified accordingly, and that access has to be granted only on a need-to know" basis.
For the IT sector, an effective information sharing procedure can enable the success of the related sector's public-private partnership model, by ensuring that all partners have relevant situational awareness to protect IT and critical functions.

European Strategic Framework (VI)

Stakeholder Cooperation: **All stakeholders** *(European Authorities, MS, industry and business associations, standardisation bodies and owners, regulators, operators and users)* **have a major role to play in protecting CI.**

These actors need to work together to effectively contribute to the development/validation/implementation of a modern and efficient EPCIP (European Programme for Critical Infrastructure Protection), according to their specific roles and responsibilities.

State Authorities have to afford leadership and coordination in developing and implementing a nationally reliable approach to the CI protection within their jurisdictions.

Owners, operators and users would be actively involved at both the national and EU level.

Proportionality: **Any proposed protection strategies and/or related measures have to be "proportionate" to the level of risk involved, *as not all infrastructures can be protected from all threats*.**

By applying fitting risk management techniques, priority can be given to those sectors implying for highest risk, by considering the nature of the threat, any comparative criticality, cost-benefit ratio, the level of protective security and the efficiency of existing mitigation strategies.

Sector-by-sector approach: As numerous sectors of the market environment already possess specific experience, expertise and requirements with the CIP issue, **the corresponding *EPCIP* will be structured on an explicit *sector-by-sector basis* and will be implemented by following an approved list of CIP sectors.**

European Strategic Framework (VII)

Prevention implicates the range of deliberate, critical tasks and activities *required to shape, sustain, and expand the operational capability* to prevent, protect against, respond to, and recover from an incident.

It also encompasses effort to recognize and classify potential threats, define vulnerabilities and identify necessary resources *for such kind of purposes.*

Prevention also implicates for suitable measures to protect lives and property.

"Prevention" involves applying intelligence and other data to a variety of actions that may include:

- *Countermeasures as deterrence operations;*
- *heightened inspections;*
- *improved surveillance and security operations;*
- *investigations to determine the full nature and source of the threat;*
- *public health and agricultural surveillance and testing processes;*
- *immunizations, isolation, or quarantine; and*
- *appropriate specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice.*

Some Essential Concerns about CIs

During the latest years, the appearance of CIP studies and programs at the European level constitutes an increasing trend…

EU Member States have provided substantial initiatives and have selected and promoted appropriate measures for crisis management cooperation through supranational institutions, to ensure a globally accepted character of the proposed measures.

This sort of dynamic development implicates a qualitatively novel role for the EU, much further beyond pure economic management.

A "European protection policy space" is gradually emerging.
This protection space intersects several policy sectors and EU institutions, thus comprising all activities, mechanisms, resources and other means to deal with potential trans-boundary crises.

The Information Technology (IT) Sector as part of the CI protection policy in the modern EU context

General concerns (I)

The Information Technology (IT) sector conducts operations and services *that provide for the design, development, distribution and support of corresponding products (HW/SW)* and operational support services that are necessary & critical to the assurance of national and economic security and public health, safety and confidence.

IT sector provides, *among others,* **critical control systems and related services/facilities, physical architecture and any relevant Internet infrastructure.**

All involved actors *(corporate entities, authorities, research and academic organizations, public users)* **depend on the proper establishment and the operational functionality of the corresponding resources.**
***Such kind of physical or virtual functions can create and offer hardware, software, and information technology systems and services, under various concepts*.**

General concerns (II)

The **high complexity of the underlying environment implicates difficulties**
- **upon identification and assessing threats *or***
- **upon the evaluation and management of vulnerabilities.**

The procedure for **vulnerability assessment** normally considers the people, process, technology, and physical vulnerabilities that, *if exploited by a certain kind of threat*, **could exercise effects and "modify" certain essential features of critical functions** *(such as confidentiality, integrity, or availability).*

Although IT technology infrastructure has a convinced level of intrinsic resilience, its interdependent and interconnected structure creates challenges and opportunities *for coordinating public and private sector preparedness and protection activities.*

Cooperation is needed between the public and the private sector,
with the pure aim of promoting commonly accepted concepts & methodologies.

Risk Management in the IT sector (I)

The IT Sector risk management context concentrates on two major levels:

- the **individual enterprise level**, *and;*
- the **sector -or the national- level**.

- ***Private sector entities structure their approaches on business explicit objectives**, such as shareholder value, efficacy, and customer service.*
- ***Public sector entities base their approaches on ensuring mission effectiveness or providing a well-defined and conceived public service**.*

*Enterprise-level risk management methodologies regularly include **cybersecurity initiatives** and **measures to preserve the well-being of information security programs and of the necessary infrastructures** to fulfil that purpose.*

Corresponding examples may comprise, among others:

- **Physical vulnerability mitigation measures** *(e.g., physical access control and surveillance)*
- **Human vulnerability mitigation measures** *(e.g., security training and awareness)*
- **Cybersecurity measures** (*e.g., encryption; behavior monitoring and management technologies)*
- **Business continuity planning.**

Risk Management in the IT sector (II)

- **The area of ICT security has developed extensively within the EU,** ***over the past few years.***
- **There is a large body of EU legislation, regulation and programs aimed at the protection of telecommunications, media and IT** *(the Commission addresses these infrastructures in combination).*

Network and Information Security – NIS (I)

The EU promotes specific ***network and information security (NIS) measures*** **via a regulatory framework for electronic communications** *(which also addresses issues of privacy and data protection)* **and via measures against cyber crime.**

- ***NIS is increasingly significant to our economy and society.***
- ***NIS is also an important precondition to generate a reliable environment for worldwide trade in services.***

Lack of NIS can compromise vital services depending on the integrity of network and information systems.

Lack of NIS can:

- ***Harm or terminate businesses functioning;***
- ***generate substantial financial losses for the economy, and;***
- ***negatively affect societal welfare.***

Network and Information Security – NIS (II)

The current European regulatory framework requires only telecommunication companies-operators to adopt risk management steps and to report serious NIS incidents.

However, many other sectors rely on ICT as an "enabler" and should be concerned about NIS as well.

Several infrastructure and service providers are particularly vulnerable, due to their high dependence on appropriately functioning NIS.

Security the underlying systems is of specific importance to the functioning of the market, *especially for several sectors like:*

Banking, stock exchanges, energy generation, transmission and distribution, transport (air, rail, maritime), health, Internet services and public administration).

Network and Information Security – NIS (III)

The European Commission has focused attention on prevention, preparedness and awareness and has defined a plan of immediate actions to strengthen the security and resilience of CIIs.

This focus was consistent with the challenges and priorities for NIS policy *and the most appropriate instruments needed at EU level to tackle them.*

The proposed actions were also

- **complementary** to those to prevent, fight and prosecute criminal and terrorist activities targeting CIIs

  and

- **synergetic** with current and prospective EU research efforts in the field of NIS, *as well as with international initiatives in this area.*

Network and Information Security – NIS (IV)

Areas & activities in the European regulatory and strategic policy framework

- Support of the right to privacy and of the right to the protection of personal data
- Creation of common specifications on, *for example*, personal integrity and user control, *and for developing a secure infrastructure*.
- Measure to improve robustness of networks and of information systems, *against accidents and criminal attacks*.
- Development of rules to secure electronic communications *(e.g., via measures for electronic signatures and the data protection legislation for e-communication).*
- Establishment of a bureau for information security: **the *European Network and Information Security Agency (ENISA)***

Network and Information Security – NIS (V)

Promotion of a *Directive on Network and Information Security* ***(COM(2013) 48 final, 07.02.2013)*** **to strengthen national resilience and to increase cooperation on cyber incidents.**

This is to be achieved

- **By requiring member states to increase their preparedness and improve their cooperation with each other**,
  and
- **by requiring operators of critical infrastructures,** *such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc.), as well as public administrations,*
  to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.

Cloud Computing as an means to support NIS for essential CI protection and operation

Cloud Computing for managing CIs (I)

IT Systems used for managing CIs require large resources ***and thus*****, CI providers often host their own infrastructure and possess own data centers.**

However, due to virtually unlimited scalability of resources and performance, as well as noteworthy improvement regarding maintainability, **evermore organisations will incorporate cloud computing into their computing environments.**

Thus, we argue that cloud computing will eventually reach ICT services that are operating critical infrastructures (CI).

Cloud Computing for managing CIs (II)

Cloud computing ("CC") is a "style of computing" where elastic IT-related capabilities are provided as optimized, cost-effective, and on-demand utility-like services to the corresponding customers, *mainly by using Internet-based technologies*.

Cloud computing, *in simplified terms*, can be understood as the storing, processing and use of data on remotely located computers, *accessed over the Internet*.

This means that

- **"users" can command almost unlimited computing power "on demand",**
- **they do not have to make major capital investments to fulfil their needs, *and;***
- **they can get to their data from anywhere, *simply with an Internet connection*.**

Cloud Computing for managing CIs (III)

Cloud computing has gained tremendous momentum **and started to revolutionize** ***the way enterprises create and deliver IT solutions*****.**

Cloud computing ***has the potential to***

- *slash users' IT expenditure and*
- *enable many new services to be developed.*

As more and more sectors adopt cloud services in their computing environment,
the trend also reaches ICT services operating critical infrastructures (CIs) such as transportation systems or infrastructure surveillance
which are two quite characteristic and modern examples.

Cloud Computing for managing CIs (IV)

Cloud services provide competent access to large IT infrastructures that benefit from the economy of scale.

- **It would extremely advantageous to preserve irrecoverable and valuable data obtained from CIs, *within secure cloud infrastructures*.**
- **But hosting CI services in the cloud brings with it security and resilience requirements, that existing cloud offerings are not "well placed" to deal with for all related cases.**
- **Any attempt to deploy, test and validate CI services in the cloud implicates difficulties and potential obstacles *-as well as risks and threats-* focused around technical issues but also being dependent upon legal or business issues.**

With a minimum tolerance to any security incidence or downtime,
a CI enforces much stronger requirements for security, reliability and resilience on cloud computing environments.

Cloud Computing for managing CIs (V)

The main concerns about cloud services are security, data location, applicable law and jurisdiction over data, *though on the last point it appears that most organizations in the EU market lack a full understanding of the complex issues.*

Data and application portability between cloud service providers does not appear to be a significant barrier to initial adoption, ***but becomes more important when the issue is deepening and extending the use of cloud in the enterprise.***

For the case where CIs are actually "running" inside the cloud environment, it should be expected to deploy countermeasures for attacks *(implicating for a detailed, in depth, analysis/assessment of all corresponding risks -upon a continuous and fully dynamic perspective)* **together with preventive and corrective measures** *whenever anomalies, deviations from proper level of operational behaviour or unexpected features may be observed.*

Cloud Computing for managing CIs (VI)

An example for the consideration and use of cloud computing for the support of IT of CI has been develpoed within the scope of the ***SECCRIT ("SEcure Cloud computing for Critical infrastructure IT")*** EU-funded project *(GA No.312758)*.

***SECCRIT*'s mission** is to **analyze and evaluate cloud computing technologies with respect to security risks in sensitive environments,** and to **develop methodologies, technologies, and best practices for creating a secure, trustworthy, and high assurance cloud computing environment for CI.**

SECCRIT's main objectives are prescribed as follows:

- *Identification of the relevant legal framework and establishment of respective guidelines, provision of evidence and data protection for cloud services;*
- *Understanding and managing risk associated with cloud environments;*
- *Understanding cloud behavior in the face of challenges;*
- *Establishment of best practice for secure cloud service implementations;*
- *Demonstration of SECCRIT research and development results in real-world application scenarios*

Thank you for your attention!

For further information:

Ioannis Chochliouros, Ph.D., M.Sc., ***ichochliouros@oteresearch.gr***
(Head of Research Programs Section, Fixed)

Evangelos Sfakianakis, M.Sc. ***esfak@oterseearch.gr***

Research Programs Section, Fixed
Hellenic Telecommunications Organization S.A.
1, Pelika & Spartis Str.
15122 Maroussi Athens
Greece
Tel. +30-210-6114651, +30-210-6114938
Fax. +30-210-6114650