ARES project
CONSOLIDER-INGENIO 2010 CSD2007-00004
Workpackage 5

Yearly Legal Reports

November 16, 2011

Preface to the yearly legal report.

GIDET/Universitat Illes Balears

Attending to the valuable remarks of the external committee, this year we have introduced some changes to the juridical deliverables. First of all, it should be noted that the way to work in the field of engineering and in the legal field is totally different. The former are more used to work in teams, while the latter usually perform research in a more individual way. It is also different the way to publish the results of the research. In the case of technical, and for curricular effects, are often considered only those international journals and conferences with a proper impact. In the legal sphere, international publications tend to have less prestige for personal resume, as the legal field tends to be more "local", with each country's own laws and regulations. We must also bear in mind that ARES is a highly technical project, and that the jurists were expected to support the engineers for juridical aspects, but very specific contributions in their field of research were not expected. We mean that the consulting work being done by jurists, and the documents produced for the ARES project are of a high internal interest (and for those who face similar situations), but are difficult to publish in prestigious journals for jurists. The same would happen if the technicians should produce documents understandable by jurists: they would have a high value for jurists, but they would have no interest (or very low) in the journals where we publish regularly.

ARES project is nearing its end, and at this late stage in which we are entering, transfer of technology to the productive sector is a special concern. In this way, it was considered that it would be interesting to have short documents that let we view that apart from providing a good technical solution, engineers must be aware that these technical solutions must form part of a system where a legal framework must be respected.

Here we present an overview of juridical aspects related to critical infrastructures, and the result of collaboration between engineers and jurists to provide a solution for signing contracts by electronic means. The latter will be updated and prepared for submission to some conference.

Contract Signing: a Protocol in accordance with Legal Framework

Apol·lònia Martínez Nadal and Josep Lluís Ferrer Gomila

Civil Law and Mathematics and Computer Science Dept.
University of Balearic Islands

Abstract. Electronic contracting is an essential service to develop electronic commerce. But this service is not very used because merchants and consumers do not trust in contracting by electronic means. For time we already have technical solutions that should allow to give trust to the actors implied in this new scenario. But the lack of international standards and of an appropriate juridical mark, suppose a serious restraint to the contracting by electronic means. However we can observe some legislative initiatives in the European Union to give full juridical effect to electronic contracting. With these two elements already in course, we believe that a last step will be necessary: to assess the adaptation of the technical solutions regarding the enacted legislation. In this work, juridical and technical analysis of contract signing protocols is carried out. Besides, we present a modified version of a previous optimistic fair protocol for contract signing.

1 Introduction

The World Wide Web, e-mail, EDI, etc., have proven to be very effective in e-commerce environments (in their multiple alternatives: B2B, B2C, A2C, etc.). Contract signing becomes an essential electronic service, to be used by governments, private companies and consumers. It is clear that it speeds up the commercial transactions, reduces errors, bears (to half term) a saving, etc. But even with all these advantages, potential users (e.g., merchants and consumers) are reluctant to use these new means.

This distrust can be due to a sensation of insecurity in these new contracting means. It is necessary to approach two issues in order to provide security to users. On one hand, we need technical solutions allowing to get the same (or better) level of security that the one obtained in transactions on paper at present. But technical solutions are not enough for security in a broad sense. It is absolutely necessary a juridical mark giving full effect to the electronic contracting, and allowing eliminating any reticence.

Electronic contract signing is one service offered to users, when they want to obtain a signed copy of a contract from another party. Protocols for contract signing have to provide enough evidence to parties to prove, at the end of the exchange, if the contract is signed and the terms of the contract. We can handle contract signing as a fair exchange of values: the originator has an item (the text of a contract and a non-repudiation of origin token) to be exchanged for a recipient's item (a non-repudiation token bounded to the text of the contract). An exchange is fair if at the end of the exchange, either each player receives the item it expects or neither player receives any additional information about the other's item [2]. Well then, in the technical literature, and even in the market, we already find proposals to solve the problem of electronic contracting.

On the other hand, different international organisms (e.g., UNCITRAL) and different States have enacted or are elaborating laws to give effect to electronic contracts. The European Union enacted the Directive 2000/31/EC, dated 8th of June of 2000, that pointed (see considering 7) that "in order to ensure legal certainty and consumer confidence, this Directive must lay down a clear and general framework to cover certain legal aspects of electronic commerce in the internal market". The different Members States of the European Union, according to first point of article 22, shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 17th of January of 2002. Nowadays, many countries have enforced a law on electronic commerce (in the European Union, and outside the European Union).

The European Directive, in first point of article 9, establishes that Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.

Therefore we observe that, a priori, there is no reason for not using electronic means for contracting. But we believe that it is necessary to carry out a last step: to verify if technical solutions are in accordance with legislative initiatives. This is one of the objectives of this work: to analyse different generic solutions of electronic contract signing, in order to observe their technical and juridical adaptation.

2 Juridical Aspects.

From a juridical point of view, there are two especially important issues to be resolved. The first one is the time of contract formation, that is to say, when is an electronic contract considered to be signed? The second issue has to do with the evidence, that is to say, what elements have the contracting parties to be provided in the event of litigation in relation to a signed (or not signed) contract by electronic means?.

In different phases of the discussion of the European Directive on electronic commerce, several mechanisms were settled down in relation to the two previous issues (we will not analyze those stages of the discussion of the Directive, although it is very interesting). In its final writing, and for the sake of getting the consent of the Member States, the proposal was reduced to the minimum. This way, first point of article 11 establishes: "Member States shall ensure, except when otherwise agreed by parties who are not consumers, that in cases where the recipient of the service places his order through technological means, the following principles apply:

> - the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means,
>
> - the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them."

Regarding this point it is necessary to point out some technical and juridical considerations. In the first place, the Directive doesn't make an explicit pronouncement about the time of contract formation, neither about the evidence mechanisms. In the second place, it introduces an imprecise time issue when it compels to send an acknowledgement of receipt "without undue delay". In the third place, we believe that to consider that an information has been received (the order or the acknowledgement of receipt) when the parties are able to access to them is frankly dangerous (the legislator, probably, was thinking about depositing messages in electronic mailboxes). To end up, and especially important for the content of this work, the Directive points to a model of electronic contracting in three phases:

- a company carries out an offer by electronic means (a product or a service that it puts for sale)

- a consumer (or another company) carries out an order by electronic means (in relation to the previous offer, that it can be named acceptance in juridical terms)

- the first company must send an acknowledgement of receipt of the acceptance that the consumer (or second company) sent.

We have said that the Directive only points to the previous model, and in fact, it doesn't establish explicitly the obligatory nature of the three steps, although it can be deduced from the writing of the first point of article 11. On the other hand, some of the legislation (and bills or draft bills) of the Member States make explicit the obligatory nature of following the three steps: offer, acceptance and acknowledgement of receipt of the acceptance. It is the case of the Spanish bill, the law of Luxembourg, etc.

Nevertheless, this legislation differs in one of the two issues mentioned at the beginning of this section: the time of contract formation. All the legislation of the European Union, according to the Directive, establishes the obligatory nature of sending an acknowledgement of receipt. It will be part of the evidence that the consumer (or the second company) will be able to provide as a proof of the signature of the contract. But regarding the time of contract formation, some legislation (for example, Spanish bill) establishes that the contract is signed when the consumer (or the second company) sends its acceptance, while other legislation (for example, Luxembourg law) establishes that the contract is signed when the consumer (or second company) receives the acknowledgement of receipt (the third step). The first type of legislation doesn't diminish the importance of the acknowledgement of receipt. In fact they establish considerable sanctions for companies that don't send such an acknowledgement of receipt; probably because they observe that the company is leaving the consumer or second company without proof of the contract.

From technical and juridical points of view, we think that solutions based on the three steps model, but considering that the contract is signed when the consumer has received the acknowledgement of receipt, are better, because they provide higher security to the commercial traffic. This way the time of contract formation is linked to the availability of evidences to be used in the event of litigation.

Once we have made an approach to juridical issues of the electronic contracting, in the following section we will carry out a brief analysis of the different types of technical solutions that have been proposed to date.

3 Juridical and Technical Analysis of Contract Signing Protocols

A first kind of solutions (for electronic contract signing) is based on the gradual release of secrets (parties exchange non-repudiation tokens "simultaneously"). This approach [5, 10] achieves fairness by the gradual release of information over many rounds: some knowledge about the non-repudiation evidence is revealed during each round. From a technical point of view, this approach seems to be too cumbersome and inefficient for actual implementation, due to the high communication overhead. Moreover, fairness is based on the assumption of equal computational power. This assumption is unrealistic in practice and undesirable from a theoretical point of view [3]. From a juridical point of view, it's clear that this kind of solutions does not follow the offer / acceptance / acknowledgement (ACK) model. On the other hand, to convince a judge, about if a contract was signed or not, would be difficult.

A second kind of solutions are third party protocols (parties exchange items, assisted by a TTP). We can find some fair exchange protocols using a trusted third party [1, 2, 4, 7, 9, 11]. First question a jurist asks is: who can act as a trusted third party? The first answer can be a Public Notary (obviously we mean an Internet server in the name of a Public Notary, with or without human intervention, but with a Public Notary in charge of the proper working of the system). But, it is well known that Public Notaries, as a high qualified professionals, establish high fees for their intervention in paper world (and probably they will do the same in the electronic world). So we have to wonder if other entities (for example, Internet Service Providers, or ad hoc entities) can assume the role of trusted third party. We think so, but with one condition: TTP's intervention has to be verifiable. It's to say that if the TTP tries to cheat (when it has to intervene) then contracting parties will be able to prove the fraud in courts.

Contract signing protocols with TTP differ in the degree of the TTP's involvement in a protocol run. We classify this kind of protocols into two classes: with active TTPs (a TTP is actively involved in every protocol run) and with subsidiary TTPs or optimistic protocols [1] (a TTP only intervenes in case of exception, not in every protocol run). But solutions with TTP have drawbacks: the trusted third party can become a bottleneck. Besides, a TTP will want to charge for its intervention. Hence, from commercial and technical points of view, one of the goals of designing an efficient contract signing protocol is to reduce TTP's intervention.

So, "optimistic" protocols are especially interesting. Parties will exchange their items, following the sequence of steps specified in the protocol. They hope to receive the expected item from the other party, and this will be the case if the protocol ends successfully. Otherwise, if one party is trying to cheat (or there are communication failures) the other party may contact the TTP to solve the unfair situation. Of course a cheating party can contact the TTP or can conspire with the TTP, and so, good protocols have to foresee these possible situations.

Some formal requirements for fair exchange were stated in [2], and re-formulated in [11]: effectiveness, fairness, timeliness, non-repudiation and verifiability of third party. Two additional properties to be met are efficiency and privacy (this last one is optional for users). Now, from a juridical point of view, we have to add a new requirement: technical solutions must ensure legal fitting. So, we need a protocol for contract signing with three steps: offer / acceptance / ACK.

ASW [2] and GJM [8] protocols have, both, three sub-protocols: exchange, abort and resolve. The exchange sub-protocols have four steps in both cases. So, none of them follows the agreed model of the European Directive. In next section we adapt a previous solution [6] to observe the legislation.

Finally, we think that solutions have to be secure from a technical point of view, but as simple as possible. Some disputes will be solved in courts, and judges will have to evaluate evidence brought by parties involved in an electronic contract signing. Obviously, judges will have to be assisted by experts, but they (judges) must understand, at the end, conclusions given by those experts.

In next section we present a contract signing protocol with the following characteristics: effective, fair, asynchronous, with verifiable TTP and efficient. This protocol is better than previous solutions at least in three aspects. On one hand, the protocol has less steps than any other solution in the literature. On the other hand, it is easy to understand and so, it can be useful in situations that potentially will arrive to courts. Finally, the solution is adapted to the European Directive on electronic commerce.

4 A Contract Signing Protocol

We will begin describing the proposed protocol.

4.1 Protocol

The originator, A(lice), and the recipient, B(ob), will exchange messages and non-repudiation evidence directly. Only as a last recourse, in the case they cannot get the expected items from the other party, the TTP (T) will be invoked, initiating cancel or finish sub-protocols. In the following description, we have not included elements to link messages of an exchange, nor operations to achieve confidentiality, in order to simplify the explanation. The notation and elements used in the protocol description are as show in table 1.

The exchange sub-protocol is as follows:

1. A→B: offer, h_A
2. B→A: acceptance, h_B
3. A→B: ACK_A

If the protocol run is completed, the originator A will hold non-repudiation (NR) evidence, h_B, and the recipient B will hold non-repudiation evidence, h_A and ACK_A. So the protocol meets the effectiveness requirement.

Notation	
X,Y	concatenation of two messages X and Y
H(X)	a collision-resistant one-way hash function of message X
Sign_i(X)	digital signature of principal i on message X
i→j: X	principal i sends message (or token) X to principal j
Elements	
offer	message containing the offer
acceptance	message containing the acceptance
$h_A = \text{Sign}_A(\text{offer})$	message containing the offer
$h_B = \text{Sign}_B(\text{acceptance})$	signature of B on the acceptance
$\text{ACK}_A = \text{Sign}_A(h_B)$	signature of A on h_B; this is an acknowledge-ment that A knows that the contract is signed, and is part of the evidence for B
$\text{ACK}_T = \text{Sign}_T(h_B)$	signature of the TTP on h_B; this is an equivalent acknowledgement to the one that A should have sent
$h_{AT} = \text{Sign}_A[\text{H(offer)}, h_A]$	this token is an evidence that A has demanded TTP's intervention
h_B' = $\text{Sign}_T(h_B)$	signature of the TTP on hB to prove its intervention

Table 1. Notation and elements.

Observe that the protocol follows the model suggested in European legislation: the first company is compelled to send an acknowledgment of receipt of the acceptance. We have said that some legislation indicate that the contract is concluded when B sends the acceptance, while other legislations indicate that the contract is concluded when B receives the receipt. We think that it's better the second option because it allows to link the time of contract formation to the achievement of evidence for both parties.

But, what happens if A or B don't finish the execution of the exchange sub-protocol? For example, what happens if A does not send the receipt? A can allege that she sent the receipt and that it was lost. Whatever case, if B does not receive the receipt, he will not be able to prove that the contract is concluded (and A will be able to show or not to show evidences she has). To deal with this possible situations we have designed to sub-protocols (cancel and finish), with TTP's intervention. In order to simplify the sub-protocols descriptions, we assume that the information sent by A or B to the TTP is correct (otherwise the TTP should send an error message).

If B contacts the TTP before A, the TTP will send the NR token, ACK_T, to B:

2'. B→T: H(offer), H(acceptance), h_A, h_B, h_{BT}
3'. T→B: ACK_T

The TTP will store the NR token, h_B, in order to satisfy future petitions from A. If later A contacts the TTP, the TTP knows that it has finished the exchange for B, and it has to send the NR token, h_B, to A, plus a token in order that A can prove TTP's intervention, h_B':

1'. A→T: H(offer), h_A, h_{AT}
2'. T→A: h_B, h_B'

If A contacts the TTP before B, the TTP will send a message to A to cancel the transaction:

1'. A→T: H(offer), h_A, h_{AT}
2'. T→A: Sign_T(”cancelled”, h_A)

The TTP will store the exchange state (cancelled) in order to satisfy future petitions from B. If later B contacts the TTP, the TTP has cancelled the exchange for A, and it has to send a cancel message to B:

2'. B→T: H(offer), H(acceptance), h_A, h_B, h_{BT}
3'. T→B: Sign_T(”cancelled”, h_B)

So, A and B have a fair way to finish the contract signing (concluded or cancelled for both parties), and they always will have enough evidence to be used in case of dispute. As a conclusion, we have achieved fairness and non-repudiation, two fundamental properties to be met from a technical point of view. Observe that a ”conflicting” situation may occur. A can obtain NR evidence from B (h_B) and a cancel message from T, while B had obtained NR evidence from A (h_A, ACK_A). A can do it, for instance, invoking the cancel sub-protocol after the end of the exchange sub-protocol. It seems that A can affirm that the contract is signed or not signed, depending on her usefulness. But B possesses NR evidence that will prove that the contract is signed, and if A tries to use the cancel message she will be showing that she is a cheating party. As a conclusion, we repeat again that the protocol is fair and meets the non-repudiation requirement. Besides, observe that we have not established any restriction in regard to time for contacting the TTP, and so it can be proved that the proposed protocol meets the timeliness requirement.

To finish this section, we think that this protocol will be useful for "web based contracting". In accordance with UNCITRAL draft on electronic contracting [20], we think that "the offer of goods or services through automated computer systems allowing the contract to be concluded automatically and without human intervention is presumed to indicate the intention of the offeror to be bound in case of acceptance". A user (e.g., a consumer) will navigate through web pages selecting products. When he has finished, he will push a "check out" button, and as a consequence he will receive the offer, a web page containing the selected products with final prices (perhaps with discounts and gifts). If the user agree then he will press a button in order to send an acceptance, and he will receive a web page as an acknowledgment of receipt. The offer, acceptance and receipt are XML documents signed by the sender.

4.2 Verifiability of the Third Party and Confidentiality.

We have said that verifiability of the TTP is an important property to be met by proposed protocols, in order to allow that a private company (e.g., an Internet Service Provider) can be a TTP. The presented protocol satisfies this requirement. A TTP's possible misbehavior is: A receives h_B and h_B', while B receives the cancel token. If A uses h_B and h_B' to prove that B has signed the contract, B can use the cancel token to prove the TTP's misbehavior. If A received h_B and then (or before) she cancelled the exchange (and so she did not receive h_B'), and try to use h_B to prove that B received the evidence, and the TTP has the h_{AT} token, it is clear an A's misbehavior.

The other TTP's possible misbehavior is: B receives ACK_T while A receives the cancel token. If B uses h_A and ACK_T to prove that A has signed the contract, A can use the cancel token to prove the TTP's misbehavior. It should be noted that if B uses h_A and ACK_A to prove that A has signed the contract, A can not use the cancel token to prove the TTP's misbehavior, since the TTP did not issue conflicting evidence (it is obvious that A is misbehaving).

Finally, it is possible, and very easy, to conduct a confidential exchange between A and B, even for the TTP (in the case this one has to intervene). This is an important property to be in accordance with European legislation on privacy. If A and/or B want confidentiality then it has to be possible. A and B can exchange a secret key of a symmetric cryptosystem, k, using some key-exchange protocol (for instance encrypting k with the public key of B). Then, they can encrypt the offer and the acceptance of the exchange sub-protocol with that key k only known by them. Now we have to analyze the confidentiality of the exchange for two possible situations:

- the TTP has not intervened in the exchange: observe that only A and B can decrypt the encryption made with key k.

- the TTP has intervened in the exchange: observe that the TTP only needs a hash of the offer and/or of the acceptance to verify the correctness of the information given by A or B, and so, the TTP can not read the content of the contract, even if it intercepted the encrypted message (with k) in the communication channel between A and B.

5 Conclusions.

We have analyzed proposed solutions for electronic contract signing, from technical and juridical points of view, concluding that it is very important to bind time of contract formation and achievement of evidences related to that contract. We have presented a fair protocol for contract signing, following the model proposed in the European Directive: offer / acceptance / ACK. The fairness is guaranteed, provided the existence (and possible involvement) of a trusted third party, that plays a subsidiary role (only intervenes in case of exception). From technical and juridical points of view this role can be assumed by a private company without special or expensive requirements (only verifiability is required, and it is accomplished in our protocol).

References

1. N. Asokan, Matthias Schunter and Michael Waidner: "Optimistic protocols for fair exchange"; Proceedings of 4th ACM Conference on Computer and Communications Security, pages 7-17, Zurich, Switzerland, April 1997.
2. N. Asokan, Victor Shoup and Michael Waidner: "Asynchronous Protocols for Optimistic Fair Exchange"; Proceedings of the IEEE Symposium on Research in Security and Privacy, pages 86-99, Oakland, California, May 1998.
3. Michael Ben-Or, Oded Goldreich, Silvio Micali and Ronald L. Rivest: "A Fair Protocol for Signing Contracts"; IEEE Transactions on Information Theory, Vol. 36, n. 1, pages 40-46, January 1990.
4. Benjamin Cox, J.D. Tygar and Marvin Sirbu: "NetBill security and transaction protocol"; Proceedings of the First USENIX Workshop on Electronic Commerce, pages 77-88, New York, July 1995.
5. Ivan Bjerre Damgard: "Practical and provably secure release of a secret and exchange of signatures"; Advances in Cryptology - Proceedings of Eurocrypt'93, LNCS 765, Springer Verlag, pages 200-217, Lofthus, Norway, May 1993.
6. Josep Lluís Ferrer-Gomila, Magadalena Payeras-Capellà and Llorenç Huguet-Rotger: "Efficient Optimistic N-Party Contract Signing Protocol"; Proceedings of 4th Information Security Conference, ISC 2001, LNCS 2200, Springer Verlag, pages 394-407, Málaga, Spain, October 2001.
7. Josep L. Ferrer, Àngel Rotger and Llorenç Huguet: "Firma electrónica de contratos"; Proceedings of III Reunión Española de Criptología, Barcelona, Spain, 1994.
8. Juan A. Garay, Markus Jakobsson and Philip MacKenzie: "Abuse-Free Optimistic Contract Signing"; Advances in Cryptology - Proceedings of Crypto'99, LNCS 1666, Springer Verlag, pages 449-466, August 1999.
9. Oded Goldreich: "A simple protocol for signing contracts"; Proceedings of a Workshop on the Theory and Application of Cryptographic Techniques, Crypto'83, Plenum Press, pages 133-136, New York, 1984.
10. T. Okamoto and K. Ohta: "How to simultaneously exchange secrets by general assumptions"; Proceedings of IEEE Symposium on Research in Security and Privacy, pages 14-28, Fairfax, Virginia, November 1994.
11. Jianying Zhou, Robert Deng and Feng Bao: "Some Remarks on a Fair Exchange Protocol"; Proceedings of Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000, LNCS 1751, Springer Verlag, pages 46-57, Melbourne, Victoria, Australia, January 2000.
12. Austria: "Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt (E-Commerce-Gesetz - ECG) und das Signaturgesetz sowie die Zivilprozessordnung geändert werden".
13. Belgium: "Projet de loi sur certains aspects juridiques des services de la société de l'information".
14. European Council: "Directive 2000/31/EC of the European Parliament and of the Council of 8 June on certain aspects on information society services, in particular electronic commerce, in the Internal market ('Directive on electronic commerce')"; Official Journal L 178, 17/07/2000, pages 0001-0016.
15. France: "Projet de loi sur la société de l'information".
16. Germany: "Gesetzentwurf über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr - EGG".
17. Luxembourg: "Loi du 14 août relative au commerce électronique".

18. Spain: ”Proyecto de ley de servicios de la sociedad de la información y de comercio electrónico”.
19. UNCITRAL: ”Model Law on Electronic Commerce”.
20. UNCITRAL: ”Legal aspects of electronic commerce. Electronic contracting: provisions for a draft convention”, September 2001.

CRITICAL INFRASTRUCTURES (CIs) AND CRITICAL INFORMATION INFRASTRUCTURES (CIIs) PROTECTION.

Ana Isabel Cerezo Domínguez

Associate Professor in Criminal Law and Criminology
University of Málaga

Abstract. Critical Infrastructures are complex and highly interconnected systems that are crucial for the well-being of the society. Any type of failure can cause significant damage, affecting one or more sectors due to their inherent interdependency. Not only the infrastructures are critical, but also the information infrastructures that manage, control and supervise them. Due to the seriousness of the consequences, the protection of these critical (information) infrastructures must have the highest priority. It is the purpose of this report to review and discuss about Critical Infrastructures and Critical Information Infraestructures protection.

1 Introduction and objectives

Critical Infrastructures (CI) are complex and highly interconnected systems (transportation systems, power plants, financial facilities, hospitals, defence systems, etc.) that are crucial for the well-being of the society[1]. According to the European Commission, Critical Infrastructures consist 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 citizens or the effective functioning of governments in the Member States"[2]. On the other hand, the United States consider Critical Infrastructures as "those 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

[1] Metzger, J.: The Concept of Critical Infrastructure Protection (CIP). In: Business and Security: Public-Private Sector Relationships in a New Security Environment, pp. 197- 209. Oxford University Press, Oxford, 2004

[2] Commission of the European Communities: Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism, COM (2004) 702 final, Brussels (2004)

debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"[3].

But not only the infrastructures are considered critical. Information and Communication Technologies (ICTs) are increasingly intertwined in our daily activities. Some of these ICT systems, services, networks and infrastructures form a vital part of the world economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. They are typically regarded as critical information infrastructures (CIIs) as their disruption or destruction would have a serious impact on vital societal functions. Recent examples include the large-scale cyber-attacks targeting Estonia in 2007 and the breaks of transcontinental cables in 2008. Not only the potential risk of existing threats is of importance, it is also significant to measure whether a certain infrastructure is more critical than others. For the EU, the selection criteria of what infrastructures are critical and their different degrees of criticality depends on the following three factors:

- Scope: The loss of a critical infrastructure element is rated by the extent of the geographic area, which could be affected by its loss or unavailability.

- Magnitude: The degree of the impact or loss can be assessed according to the following criteria: public impact (population affected), economic (significance of economic loss, present and future), environmental (impact on the location), interdependency (between other critical infrastructures), and political (regarding the confidence on the government).

- Time: This criterion ascertains at what point the loss of an element could have a serious impact, and at what point it would be possible to recover the functionality of that element.

The risks to CIIs due to man-made attacks, natural disasters or technical failures are often not fully understood and/or sufficiently analysed. Consequently, the level of awareness across stakeholders is insufficient to devise effective safeguards and countermeasures. Cyber-attacks have risen to an unprecedented level of sophistication. The recent large scale cyber-attacks on Estonia, Lithuania and Georgia are the most widely covered examples of a general trend. The huge number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam confirm the severity of the problem.

[3] Congress of the United States of America: USA PATRIOT ACT. Public Law, 107-156, Washington, D.C., 2001

The protection of critical infrastructures is a priority for homeland and corporate security. The development of the information society has caused a vast majority of such infrastructures to critically depend on the correct operation of the information systems that control them. Indeed, the interruption of such an operation or, even worse, the destruction of those information systems as a consequence of an accident or a terrorist attack can result in huge financial, material or even human losses[4]. So, the high dependence on CIIs, their cross-border interconnectedness and interdependencies with other infrastructures, as well as the vulnerabilities and threats they face raise the need to address their security and resilience in a systemic perspective as the frontline of defence against failures and attacks. Due to the seriousness of the consequences, the protection of the critical (information) infrastructures (CII) must have the highest priority[5].

2 European legal instruments on Critical Infrastructure protection.

2.1 Background

In June 2004 the European Council asked for the preparation of an overall strategy to protect critical infrastructures. In response, on 20 October 2004, the Commission adopted a Communication on critical infrastructure protection in the fight against terrorism (COM (2004) 702 final) which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

On 17 November 2005 the Commission adopted a Green Paper on a European programme for critical infrastructure protection (COM (2005) 576 final) which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network (CIWIN). The Green Paper on the European Programme for Critical Infrastructure Protection clearly foresees a number of funding sources for activities related to the protection of critical infrastructures in Europe. The Commission is prepared to participate in the funding of CIP-related measures including relevant studies and the development of specific methodologies. Funding for concrete hardware updates, however, would have to

[4] Javier Lopez, Cristina Alcaraz, Rodrigo Roman. On the Protection and Technologies of Critical Information Infrastructures. On Foundations of Security Analysis and Design IV, LNCS 4677, pp 160-182, Springer.

[5] Dunn, M., Abele-Wigert, I.: The International CIIP Handbook 2006: An Inventory of Protection Policies in 20 Countries and 6 International Organizations (Vol. I) (Zurich, Center for Security Studies, 2006)

be found from other sources. The responses received to the Green Paper emphasised the added value of a Community framework concerning critical infrastructure protection. The need to increase the critical infrastructure protection capability in Europe and to help reduce vulnerabilities concerning critical infrastructures was acknowledged. The importance of the key principles of subsidiarity, proportionality and complementarity, as well as of stakeholder dialogue was emphasised.

2.2 The European Programme for Critical Infrastructure Protection (EPCIP)

In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a European programme for critical infrastructure protection (EPCIP) in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders while welcoming the efforts of the Commission to develop a European procedure for the identification and designation of European critical infrastructures ('ECIs') and the assessment of the need to improve their protection. The European Programme demands that the Commission produces an annual communication to take stock of progress made and challenges ahead. This will integrate the various analyses and measures across the different sectors of the economy. Member-state governments would continue to develop and maintain databases of significant critical infrastructure on a national basis and would be responsible for developing, validating and auditing relevant plans to ensure continuity of services in case of an attack under their jurisdictions.

2.3 The Critical Infrastructure Warning Information Network (CIWIN)

In October of 2008, the European Commission (EC) proposed legislation to create the Critical Infrastructure Warning Information Network (CIWIN), a system designed to strengthen information sharing on critical infrastructure protection (CIP) between EU Member States (see COM(2008) 676 final).

CIWIN will bring together member-state CIP specialists to assist the Commission in drawing up programmes to facilitate exchange of information on shared threats and vulnerabilities and appropriate countermeasures and strategies. The USA has a similar system known as Critical infrastructure Warning Information Network (CWIN), operational since 2003.

The CIWIN consists of the two following functionalities (article 4):

(a) an electronic forum for the CIP related to information exchange; (b) a rapid alert functionality that shall enable participating Member States and the Commission to post alerts on immediate risks and threats to critical infrastructure.

The electronic forum shall be composed of fixed areas and dynamic areas.

Fixed areas shall be included in the system on a permanent basis. While their content may be adjusted, the areas may not be removed, renamed or new areas added. The Fixed areas shall be comprised of the following:

(1) Member State Areas, offering each participating Member State the possibility to create its own area in the CIWIN portal. The organisation, administration and the content of this area will be the sole responsibility of Member States. The area will be accessible exclusively to users from the respective Member State.

(2) Sector Areas, with 11 separate sectors: Chemical Industry; Energy; Financial; Food; Health; ICT; Nuclear fuel-cycle industry; Research facilities, Space, Transport; and Water. There will also be a cross-sector sub-area for generic topics and issues of relevance to multiple sectors.

(3) CIWIN Executive Area, serving as a strategic coordination and cooperation platform designed to promote and enhance the work and communication as far as Critical Infrastructure Protection is concerned. This area will be accessible to CIWIN Executives exclusively.

(4) EU External Co-operation Area, focusing on raising awareness of external cooperation in Critical Infrastructure Protection and of Critical Infrastructure Protection standards outside the EU.

(5) Contact Directory, to facilitate the search for contact details of other CIWIN users or Critical Infrastructure Protection experts.

Dynamic areas shall be created upon demand, and shall serve a specific purpose. Their existence shall be terminated upon fulfilment of their initial purpose. The dynamic areas shall be the following:

(1) Expert Working Group Area, to provide support to the work of CIP Expert groups;

(2) Project Area, containing information on projects financed by the Commission;

(3) Alert Areas, which may be created in the event of an alert being triggered in the RAS, and will constitute the channel of communication during CIP-related activities;

(4) Special Topics Area, to focus on specific topics.

The CIWIN shall be established as a secure classified system, and shall be capable of handling information up to the level of RESTREINT UE (article 7) The Commission shall decide on the most appropriate technological platform for CIWIN and users shall meet the technical requirements established by the Commission.

The security classification of the CIWIN shall be upgraded as appropriate. Users' rights to access documents shall be on a "need to know" basis and must at all times respect the author's specific instructions on the protection and distribution of a document.

Member States and the Commission shall take the necessary security measures:

(a) to prevent any unauthorised person from having access to the CIWIN;
(b) to guarantee that, when using the CIWIN, authorised persons have access only to data which are within their sphere of competence;
(c) to prevent information on the system from being read, copied, modified or erased by unauthorised persons.

The uploading of information onto the CIWIN shall not affect the ownership of the information concerned. Authorised users shall remain solely responsible for the information they provide and shall ensure that its contents are fully compliant with existing Community and national law.

Finally, the Commission shall review and evaluate the operation of the CIWIN every three years, and shall submit regular reports to the Member States (article 10). The first report, which shall be submitted within three years after the entry into force of this Decision, shall, in particular, identify those elements of the Community network which should be improved or adapted. It shall also include any proposal that the Commission considers necessary for the amendment or adaptation of this Decision.

2.4 EU New Directive 2008/114/EC.

The Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology ('ICT') sector. The primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures. There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures. Such ECIs should be identified and designated by means of a common procedure. The evaluation of security requirements for such infrastructures should be done under a common minimum approach. Bilateral schemes for cooperation between Member States in the field of critical infrastructure protection constitute a well established and efficient means of dealing with transboundary critical infrastructures. EPCIP should build on such cooperation. Information pertaining to the designation of a particular infrastructure as an ECI should be classified at an appropriate level in accordance with existing Community and Member State legislation.

Identification of ECIs (article 3). The Directive requires Member States to identify and designate European Critical Infrastructure (ECI) providers. To qualify as critical, disruption of the infrastructure has to have a cross-border dimension. The Commission has identified an indicative list of priority sectors. ECI designation is also subject to a severity test and the comitology procedure.

The cross-cutting criteria shall comprise the following:

(1) casualties criterion (assessed in terms of the potential number of fatalities or injuries);

(2) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);
(3) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

The cross-cutting criteria thresholds shall be based on the severity of the impact of the disruption or destruction of a particular infrastructure. The precise thresholds applicable to the cross-cutting criteria shall be determined on a case-by-case basis by the Member States concerned by a particular critical infrastructure. Each Member State shall inform the Commission on an annual basis of the number of infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds.

The sectoral criteria shall take in into account the characteristics of individual ECI sectors. The Commission together with the Member States shall develop guidelines for the application of the cross-cutting and sectoral criteria and approximate thresholds to be used to identify ECIs. The criteria shall be classified. The use of such guidelines shall be optional for the Member States.

The sectors to be used for the purposes of implementing this Directive shall be the energy and transport sectors. The subsectors are identified in Annex I.

ENERGY

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

TRANSPORT

4. Road transport
5. Rail transport
6. Air transport
7. Inland waterways transport

8. Ocean and short-sea shipping and ports

Therefore the list of ECI sectors in itself does not generate a generic obligation to designate an ECI in each sector.

Designation of ECIs (article 4) Each Member State shall inform the other Member States which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI. Each Member State on whose territory a potential ECI is located shall engage in bilateral and/or multilateral discussions with the other Member States which may be significantly affected by the potential ECI.

A Member State that has reason to believe that it may be significantly affected by the potential ECI, but has not been identified as such by the Member State on whose territory the potential ECI is located, may inform the Commission about its wish to be engaged in bilateral and/or multilateral discussions on this issue. The Commission shall without delay communicate this wish to the Member State on whose territory the potential ECI is located and endeavour to facilitate agreement between the parties.

Operator security plan (article 5) Once identified and designated, a common approach will be applied to assess how the protection of the infrastructure should be improved. The proposed common approach requires the owner or operator of the relevant infrastructure to establish an Operator Security Plan (OSP) and to review this plan against the Directive methodology within two years after the Directive comes into force. More detailed European Union sector specific requirements may be adopted by comitology. Member States must ensure adequate and regular supervision of each OSP and its implementation, in line with the risk and threat assessment.

Annex 2 of the ECI Directive provides the minimum contents of such OSPs including:

(a) identification of important assets;
(b) a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact shall be conducted.
(c) identification, selection and prioritization of counter-measures and procedures with a distinction between:

- Permanent security measures, which identify indispensable security investments and means which cannot be installed by the owner/operator

at short notice. This heading will include information concerning general measures; technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.
- Graduated security measures, which are activated according to varying risk and threat levels.

Once an OSP has been created, each ECI owner/operator should submit it to the relevant Member State authority. Each Member State will setup a supervisory system concerning OSPs which will ensure that sufficient feedback is given to the ECI owner/operator concerning the quality of the OSP and in particular the adequacy of the risk and threat assessment.

Security Liaison Officer (SLO) The second obligation imposes on the owners/operators of those critical infrastructures consists on the designation of a Security Liaison Officer (SLO). Article 6 of the ECI Directive requires all CI owners/operators designated as ECI to appoint an SLO. The SLO would function as the point of contact for security issues between the ECI and the relevant CIP authorities in the Member States. The SLO would therefore receive all relevant CIP related information from the Member State authorities and would be responsible for providing relevant information from the ECI to the Member State.

Reporting (article 7) Member States must conduct an industry wide risk and threat assessment in relation to their critical infrastructure and report to the Commission on the types of vulnerabilities, threats and risks in each sector using a common template. The Commission will then assess on a sectoral basis where additional measures are needed, and may develop, on the basis of comitology, common methodologies for assessing risks

2.5 Air traffic control

Security of Aircraft in the Future European Environment (the SAFEE project) was begun in 2004 with the aim of improving security on commercial aircraft. It addresses classic hijacking situations, September 11-type scenarios and futuristic scenarios involving electronic jamming and hacking of computer systems. Sub-projects will address technical issues such as onboard-threat detection, threat assessment and response management plus flight protection.

2.6 The maritime sector

The International Ship and Port Facility Security, ISPS code, was introduced in July 2004. It requires ports and vessels to show that they have put adequate security systems in place - and vessels to show that they have been calling only at certified ports. The purpose of the code is to provide a standardized, consistent framework for evaluating risk.

2.7 The Critical Information Infrastructure Protection Policy (CIIP)

In april 2009, the EC created a Critical Information Infrastructure Protection policy, which focuses security efforts on information technology and communications systems. The Critical Information Infrastructure Protection (CIIP) policy proposed by the Commission focuses on prevention, preparedness and awareness and defines a plan for immediate actions to strengthen the security and resilience of CIIs (see COM/2009/149 final). The proposed actions complement existing measures in the area of police and judicial cooperation to prevent, fight and prosecute criminal and terrorist activities targeting CIIs. These proposals are also reflected in the EU research efforts in the field of network and information security and are in line with the international initiatives in this area. To achieve an enhanced level of awareness and preparedness throughout the EU, the Commission proposes the following set of actions:

> (1) Preparedness and prevention: to ensure preparedness by defining a baseline of capabilities and services of national/governmental Computer Emergency Response Teams, creating a European Public-Private Partnership for Resilience and a European Forum of Member States to share information and good policy and operational practices.
>
> (2) Detection and response: to provide adequate early warning mechanisms, by supporting the development and deployment of a European Information Sharing and Alert System, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems.

(3) Mitigation and recovery: to reinforce EU defence mechanisms for CII, via the development by Member States of national contingency plans and the organisation of regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination, and by strengthening the cooperation between national/governmental Computer Emergency Response Teams.

(4) International and EU wide cooperation: to promote EU priorities internationally, by driving a Europe-wide debate, involving all relevant public and private stakeholders, to define EU priorities for the long term resilience and stability of the Internet, by working with Member States to define guidelines for the resilience and stability of the Internet and by working on a roadmap to promote principles and guidelines at the global level, possibly leveraging strategic cooperation with third countries.

(5) Criteria for the ICT sector: to support future implementation of EPCIP, by continuing to develop, in cooperation with Member States and all relevant stakeholders, the criteria to identify the European critical infrastructures in the ICT sector.

3 The implementation of European Critical Infrastructures legislation in Spain.

It is under the text of the draft Royal Decree (”PRD”) being prepared by the Ministry of the Interior that aims to transpose into our domestic law the Directive 2008/114/EC of the Council of December 8, 2008, on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. That decree, upon approval, will complete and adapt existing Spanish legislation on the subject to the requirements of Directive 2008/114/EC and, particularly, the National Plan for Critical Infrastructure Protection, May 7 2007 and the National Catalogue of strategic infrastructure. In addition, approval will be a definite boost to the activity of the National Center for Critical Infrastructure Protection (”CNPIC”) established by the Council of Ministers Agreement dated November 2, 2007.

The ultimate goal pursued by the protection of critical infrastructure is, therefore, ensure continuity of essential public services or strategic for any eventuality or circumstance that may arise and affect normal operation. To this end, the first aim of PRD is to identify critical infrastructure, the responsible operator and the various security threats that affect each one of them. Only in this way may be established physical security measures and logic to counteract these threats and ensure service continuity in case of disaster.

According to PRD scope of critical infrastructure will be determined by the combination of horizontal and sectoral criteria criticality. The criteria refer provisionally horizontal criticality of an infrastructure based on the potential number of victims, the economic impact (both economic losses, including impairment of products and services, and environmental) as well as the public impact (the impact on confidence population, physical suffering and disruption of daily life, including the loss and the severe deterioration of essential services) in cases of non-performance of that infrastructure. As regards the sectoral lines, the PRD and the current National Plan for Infrastructure Protection, refer to the twelve sectors: Administration, Food, Energy, Space, Finance and Tax Systems, Water, Nuclear Industry, Industry Chemistry Research Facility, Health, Information Technologies and Communications and Transport. Noteworthy in this respect that the Spanish law, unlike the community-incorporated into Information Technology as one of these critical sectors.

The previous cutting and sectoral criteria used to determine the critical operations, ie, entities or bodies responsible for critical infrastructure. In any case, the operator must be duly informed critic, through CNPIC, the intention of being declared as such and have two months from the day following notification to submit comments. Of the obligations incumbent on the project critical operator should be highlighted:

The **development of an Operator Security Plan** within six months from designation as critical operations. This plan shall contain at least the identification of infrastructure located within the national territory as well as those that may impact at the community level and implemented countermeasures proposed for better protection. In any case, the CNPIC establish the minimum content and format to be followed for the preparation of the Plan, which must be previously approved by the CNPIC and updated annually.

The **development of a specific protection plan** for each of the critical infrastructures within a maximum of eighteen months from designation as critical or operator of six months from the time that qualify as critical an infrastructure.

The **appointment of a Head of Security and Liaison**, who shall be appointed within three months from the appointment of the entity as critical operations. The Head of Security and Liaison will represent the critical operator to the competent authorities in all matters relating to the security of their infrastructure and the various specific plans, channeling operations and information needs that arise in this regard.

The **appointment of a Security Officer of the critical infrastructure** in the same period of three months. The Security Officer will be the operational link and channel information with the relevant authorities in all matters relating to specific security or critical infrastructure European critical infrastructure concerned, directing operations and information needs in this regard.

Finally, we note that all information contained in the Plans are considered classified and therefore their access will be restricted to the Security Forces and others expressly authorized. In this sense, goes an important part of the PRD to establish the security measures that should provide this information to prevent unauthorized access as well as their availability and integrity.

The resulting legal framework significantly affect the outsourcing of processes related to critical infrastructure and, above all, the relocation and virtualization of systems that may affect these facilities, so you have to take into account the critical responsibilities of operators contracting as well as the contractors concerned. At present, an estimated 80% of critical infrastructures are managed by private companies, to be expected that a significant proportion of these have networks, systems or equipment located outside our borders.

References

1. Definition of the word Infrastructure. Merriam Webster's Collegiate Dictionary (11th edn.), Springfield, MA (2003)
2. National Research Council, Dahms, L.: Infrastructure for the 21st century - framework for a research agenda. National Academy Press, Washington, D.C. (1987)
3. Critical Information Infrastructure Research Co-ordination (CI2RCO). Deliverable D12, ICT R&D for CIIP: Towards a European Research Agenda (April 13th, 2007).
4. Definition of the word Critical: Merriam Webster's Collegiate Dictionary (11th edn.), Springfield, MA (2003)
5. Commission of the European Communities: Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism, COM (2004) 702 final, Brussels (2004)

6. Congress of the United States of America: USA PATRIOT ACT. Public Law, 107-156, Washington, D.C. (2001)
7. Analysis and Assessment for Critical Infrastructure Protection (ACIP). Deliverable D1.1 (August 31, 2002)
8. Metzger, J.: The Concept of Critical Infrastructure Protection (CIP). In: Business and Security: Public-Private Sector Relationships in a New Security Environment, pp. 197-209. Oxford University Press, Oxford (2004)
9. Dunn, M., Abele-Wigert, I.: The International CIIP Handbook 2006: An Inventory of Protection Policies in 20 Countries and 6 International Organizations (Vol. I) (Zurich, Center for Security Studies, 2006)
10. Stoneburner, G., Goguen, A., Feringa, A.: Risk Management Guide for Information Technology Systems. In: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30, Washington, D.C. (2002)
11. Radvanovksy, R.: Critical Infrastructure: Homeland Security and Emergency Preparedness. CRC Press, Boca Raton (2006)
12. Rinaldi, S., Peerenboom, J., Kelly, T.: Identifying, understanding, and analyzing Critical infrastructure interdependencies. IEEE Control Systems Magazine 21, 11-25 (2001)
13. President's Commission on Critical Infrastructure Protection (PCCIP): Critical Foundations: Protecting America's Infrastructures. Washington, D.C. (1997)
14. Landau, S., Stytz, M.R., Landwehr, C.E., Schneider, F.B.: Overview of Cyber Security: A Crisis of Prioritization. IEEE Security and Privacy 03(3), 9-11 (2005)
15. Dunn, M.: Threat Frames in the US Cyber-Terror Discourse. In: Paper presentation at the 2004 British International Studies Association (BISA) Conference, Warwick (2004). On the Protection and Technologies of Critical Information Infrastructures.
16. Bologna, S., Setola, R.: The need to improve local self-awareness in CIP/CIIP. In: Proceedings of First IEEE International Workshop on Critical Infrastructure Protection (IWCIP 2005), Darmstadt, Germany, pp. 84-89 (2005)
17. Dunn, M.: Understanding Critical Information Infrastructures: An Elusive Quest. In: Dunn, M., Mauer, V. (eds.) The International CIIP Handbook 2006: Analyzing Issues, Challenges, and Prospects (Zürich, Forschungsstelle für Sicherheitspolitik, 2006), vol. II, pp. 27-53 (2006)
18. Critical Information Infrastructure Research Co-ordination (CI2RCO): Deliverable D1, Common Understanding of CI2RCO-Basics (March 1, 2005)
19. Henriksen, S.: The Shift of Responsibilities within Government and Society. In: CRN Workshop Report. Societal Security and Crisis Management in the 21st Century, Stockholm, pp. 60-63 (2004)
20. Dunn, M.: The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP). International Journal for Critical Infrastructure Protection 1(2/3), 258-268 (2005)
21. Krutz, R.L.: Securing SCADA Systems. Wiley Publishing, Chichester (2005)
22. Malcolm Pirnie: Why Malcolm Pirnie Can your Configuration Needs. White Paper (2000), `http://www.pirniecentral.com/Docs/MPI_Configure.html`
23. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Computer Networks: The International Journal of Computer and Telecommunications Networking 38(4), 393-422 (2002)
24. The Department of Homeland Security, Science and Technology Directorate: The National Plan for Research and Development in Support of Critical Infrastructure Protection. Washington, D.C. (2005)

25. Critical Information Infrastructure Research Co-ordination (CI2RCO). Deliverable D10, Gap analysis of existing CIIP R&D programmes at regional, national and EU level. (September 29, 2006)
26. Critical Information Infrastructure Research Co-ordination (CI2RCO): Deliverable D6, Report on the analysis and evaluation of CIIP R&D programmes (June 2, 2006
27. Lopez. J.; Alcaraz, C. and Roman, R.: On the protection and Technologies of Critical Information Infraestructures, In On Foundations of Security Analysis and Design IV, FOSAD 2006/2007, Springer, LNCS 4677, pp. 160-182, 2007.