Prevention, protection and REaction to CYber attackS to critical infrastructurEs

PRECYSE

SEVENTH FRAMEWORK PROGRAMME

EUROPEAN COMMISSION

Title:	Document Version:
D 7.1 Review of ethical principles and their effect on CI and report on EU policy initiatives	Final

Project Number:	Project Acronym:	Project Title:
285181	PRECYSE	Prevention, protection and reaction to cyber-attacks to critical infrastructures

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type*-Security**:
February 2013	March 2013	PU

*Type: P: Prototype; R: Report; D: Demonstrator; O: Other.

**Security Class: PU: Public; PP: Restricted to other programme participants (including the Commission); RE: Restricted to a group defined by the consortium (including the Commission); CO: Confidential, only for members of the consortium (including the Commission). EU Restricted

Responsible:	Organisation:	Contributing WP:
Jennifer Betts	QUB	WP 7

Authors (organisation)
Jennifer Betts (QUB)

Abstract:
This deliverable investigates CI security relevant legal and ethical contexts, applying these to the work in the PRECYSE Project to facilitate the development of CI security technology which respects fundamental ethical requirements.

Keywords:
Ethics, privacy

PROJECT REVISIONS:

Revision	Date	Description	Author (Organisation)
0.1	20/03/13	First complete version of the report	Jennifer Betts (QUB)
0.2	27/03/2013	Final release after the modifications of the peer review team Nils Ullveit-moe (UIA) and Santiago Cáceres (ETRA)	Jennifer Betts (QUB)

CONTENTS

1 INTRODUCTION 4
1.1 Purpose of the Document 4
1.2 Scope of the Document 4
1.3 Structure of the Document 4
2 Critical Infrastructures 4
2.1 Definitions 4
3 Control Systems 6
3.1 Industrial Control Systems and SCADA Systems 6
4 CI Ethical Issues 8
4.1 Privacy 8
4.2 Ethical requirements for CI protection 9
5 Government Expectation 11
5.1 EU: Importance of CI protection and attitude to security 11
5.2 ENISA 12
5.3 EU Directives and Communications 13
6 Public Expectation 15
6.1 Of Privacy 15
6.2 Of Security 16
6.3 Public reaction in the UK and U.S. 17
7 Upholding Expectations: PRECYSE 18
7.1 Precyse methodologies 18
7.2 Insider threat 18
7.3 D 1.2 Use Specification - Scenario 8 19
7.4 Ethical principles relating to Precyse 19
7.5 Smart Grid 20
8 Summary and Recommendations 20
REFERENCES 22

1 INTRODUCTION

1.1 Purpose of the Document

This deliverable describes the background and ethical principles relevant to the protection of critical infrastructures. The purpose of this deliverable is to explain the background of ethical principles relevant to the protection of critical infrastructures (CI). CIs generally describe services and communication that are vital for society to function. Attacks on CIs can damage economies, cause natural disasters and lead to loss of life. As dependence on CIs is now integral to the functioning of societies, their protection is of paramount importance to governments and citizens.

1.2 Scope of the Document

The document will aim at producing an explanation of the ethical principles involved in securing CIs in the European Member States. It will analyse the European Communications, Directives and documents produced by the European Commission in relation to ethical considerations. These focus on citizens' right to privacy and the protection of their personal information while balancing the requirement to protect CIs from global threats. Specific reference will be made to the services delivered by the end-users in the Precyse Project: LINZ and Valencia Traffic Control Centre.

1.3 Structure of the Document

This document is structured as follows: Section 2 explains the basic elements of CIs; the IT and control systems and different priorities involved in their control. Section 3 examines how communication systems using open networks expose CIs to outside threats, for example from terrorists or hostile nations. Open networks highlight privacy concerns in general and ethical principles applying to CIs in particular. Section 4 goes on to focus on the ethical principles relating to privacy in general and ethical principles in relation to the balance between national security and individual privacy; the public good or public benefit debate. Section 5 examines the importance the European Commission places on securing CIs balanced with their level of concern for privacy. This involves analysis of Directives and Communications pertaining to the protection of CIs. Section 6 contrasts this with public attitudes towards CI security and privacy and in Section 7 there is a short review of Precyse methodology and technologies linked to ethics and a consideration of 'insider threat' and Smart Grids.

2 Critical Infrastructures

2.1 Definitions

1. Critical Infrastructure (CI) and European Critical Infrastructure (ECI) are defined in EC Directive 2008/114/EC [1] as:

- **Critical Infrastructure** (CI) 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 on a Member State as a result of the failure to maintain those functions"* and
- **European Critical Infrastructure** (ECI) is a "*…CI located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure".*

The Centre for European Policy Studies (CEPS) Taskforce [2] provides OECD definitions for the terms 'critical' and 'infrastructure' as follows:

The term "critical" refers to the infrastructure that provides an essential support for economic and social well-being, for public safety and for the functioning of key government responsibilities, such that disruption or destruction of the infrastructure would result in catastrophic and far reaching damage.

National definitions of "infrastructure" refer to physical infrastructure and often also intangible assets and/or to production or communications networks. These definitions are very broad, certainly broader than the notion of infrastructure commonly used in other fields of policy (e.g. the "essential facility" notion in competition law) and end up including not only the tangible assets, but also the intangibles that run with them (e.g. software, services, etc.).

OECD: Critical Information Technology as referring to:

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

Core CIs tend to be regarded as energy, water and transport systems, but also included are telecommunications, healthcare, pharmaceuticals, government, law enforcement and finance. Information Communication Technology (ICT) is now central to the functioning of these services, used in their control and delivery. The collection and handling of personally identifiable and often sensitive information would be more generally associated with healthcare, telecommunications, government services, financial services and law enforcement. The delivery of energy, water and traffic control are more readily associated with processes and moving parts. However, they also potentially involve the handling of personal data

whether in delivering services, for example payment information, or in implementing protection measures such as surveillance or for authentication purposes.

Different CIs result in different priorities and therefore different approaches. In an analysis of Critical Information Infrastructure (CII) protection in 14 countries [3], three protection typologies emerge. If CII protection is viewed in relation to economics the main actors come from the private sector, with continuity of business being the key issue. In protecting law and order, the main actors come from the law enforcement establishment to address issues ranging from technology enabled crime to crimes against individual computer users. However, where the issue is one of 'national security', the perception is that the whole of society and its core values are in danger due to their dependence on ICT. In this case the main actors involved come from the security establishment and action is taken at technical, legislative, organisational or international levels.

3 Control Systems

3.1 Industrial Control Systems and SCADA Systems

Industrial control systems (ICS) operate industrial infrastructures worldwide. These include power, water, oil and gas, pipelines, chemicals, mining, pharmaceutical, transportation, and manufacturing. Control takes place in a networked system. This can be internal to the operation site or can provide network links between remote facilities, sometimes in different countries. Impacts from a failure of the network communication can range from a minor disruption to service, adverse economic impact, to a major disaster and potential loss of life.

Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control CIs. Their primary purpose is to monitor, control and alarm remote plant or operating systems from a central location. The three main elements of a SCADA system are various Remote Transmission Units (RTUs), Information Communication Technology (ICT) and a Human Machine Interface (HMI). Each RTU collects data at the site and communicates the information to the central location with the HMI. From there information is communicated back to the RTU where necessary.

Information and data collection may take place over open networks, making them vulnerable to cyber-attack from outside threats such as denial of service attacks, malware, identity spoofing, eavesdropping and intruders trying to obtain information or control the system. An open network system is also vulnerable to insider threats from employees,

contractors and suppliers, particularly where workers have passwords to access the system remotely. The diagram below shows how SCADA systems control remote stations.

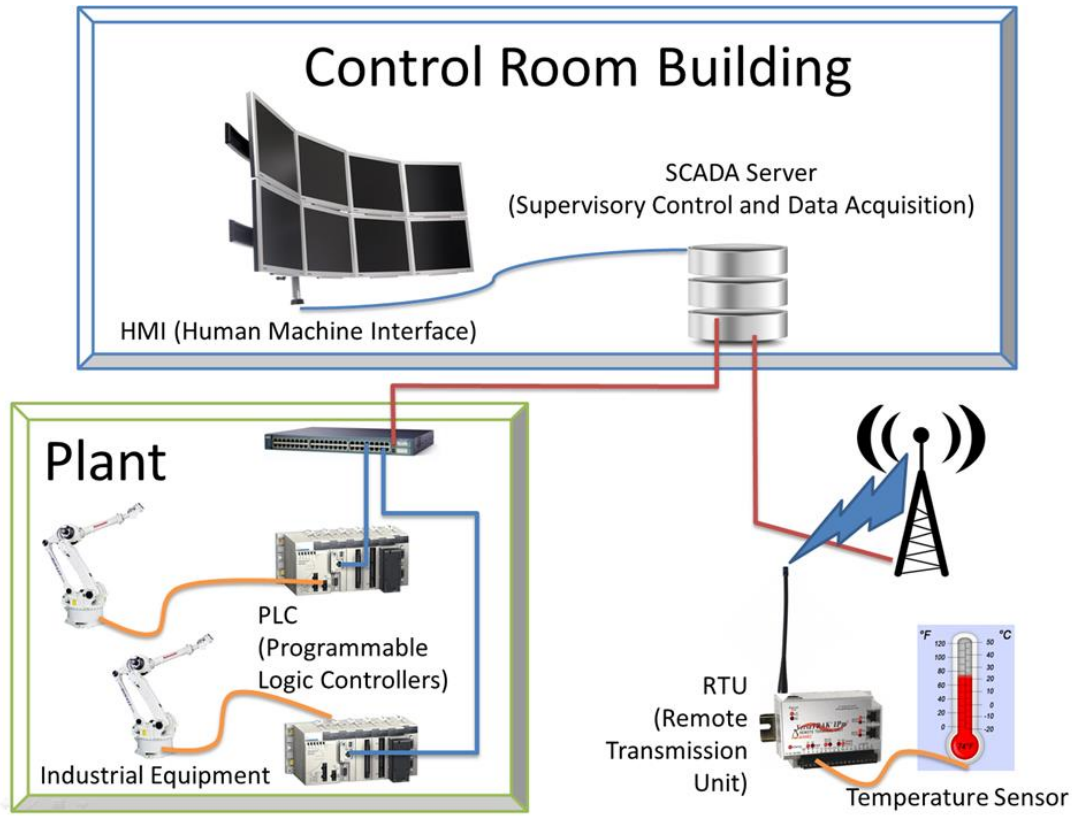

Figure 1: Example SCADA system

SCADA systems have evolved from stand-alone to networked systems using the internet to communicate with remote control sites and to deliver services to end-users. The systems and technologies are increasingly interdependent and the use of personal computing technologies means the production systems and ICT infrastructures are increasingly open to outside threats, such as the Stuxnet worm that was used to attack Iran's nuclear facilities. Measures adopted to protect CIs using open networks will involve the protection of personal data where service users are involved. This may be the case in both Precyse demonstrator models where personal information is involved in traffic management and power supply to prevent and manage leakage of data in the event of an attack on the network. Ethical issues around privacy and personal data protection are discussed in the next section.

4 CI Ethical Issues

4.1 Privacy

Michael Froomkin [4] wrote *"Both collecting and collating personal information are ways of acquiring power, usually at the expense of the data subject."* In 2000 Froomkin predicted a world that has now arrived when he said: *"As the cost of storage continues to drop, enormous databases will be created, or disparate distributed databases linked, allowing data to be cross-referenced in increasingly sophisticated ways."* He goes on to say, *"In this very possible future, indeed in our present, there may be nowhere to hide and little that can stay hidden."*

Opposing views of privacy argue that individual data privacy and protection should be paramount, while others believe that national security must take precedence in the public interest. Whatever perspective is taken, governments are accountable and have to address the various privacy concerns that privacy advocates have identified. Privacy advocates [5] suggest that it is the aggregation of accumulated data that causes privacy concerns and argue that data privacy laws have been written in the belief that anonymisation of data works [6].

The difference between personal and personally identifiable information is paramount to the debate around privacy. It can locate or identify a person. Historically it included names and addresses, phone numbers, date of birth, all easily identifiable as PII. However, technology has meant that other data, email addresses, IP addresses, social networking pages, Internet searches and logs can all be PII.

A criticism [6] of the use of anonymisation of data to protect individual privacy cites the well-known case of Netflix in the U.S. who shared their user database. Through the aggregation of the database with other personal data already in the public domain, it was possible to re-identify a particular individual. Ohm makes the case that previously no one would have classified zip code, date of birth and movie ratings as personally identifiable information (PII) and claims it is the death-knell for the assumption that we protect privacy by removing PII. *"In search of privacy law's new organising principle we can derive from re-identification science two conclusions of great importance: The power of re-identification will create and amplify privacy harms. Re-identification combines datasets that were meant to be kept apart, and in doing so gains power through accretion: Every successful re-identification, even one that reveals seemingly non-sensitive data like movie ratings, abets future re-identification."* [6].

An analysis of privacy [7] highlights the growing acknowledgement among

privacy scholars of its collective value to society. Daniel Solove argues that *"The value of privacy should be understood in terms of its contributions to society."* [5]. If this is the case, it makes an argument for the violation of privacy if it is in 'the public good' which can be usefully argued in relation to CI protection. Solove quotes Amitai Etzioni [8] *"...privacy is not an absolute value and does not trump all other rights or concerns for the common good."* However, in defending Etzioni's argument, Solove maintains that the individual will never win, unless the interest for society is trivial; *"…when privacy protects the individual, it does so because it is in society's interest."* [5].

Debates about privacy have been transformed with the arrival of new technologies and national security needs post 9/11. Add to this the reliance on CIs and the ICT that supports them, and we have come a long way from the first attempt to define privacy as 'the right to be let alone' [9].

4.2 Ethical requirements for CI protection

The security of critical infrastructures takes place within a framework that includes ethical principles in the form of internationally agreed fundamental rights. These include the right to privacy and the security of personal data. It is within this legally protected context that the security of CI has to operate. Ethical principles regarding privacy and the safeguarding of personal data has gained prominence as the control of CIs increasingly takes place over open networks. Open networks are susceptible to attack meaning that personal information may be at risk. This is the information that users provide, for example to pay online for a service. This may involve monitoring road use and toll payments. In the case of an attack on the network system, this information may be accessed or leaked. If this were to happen, the service users would have to be informed.

There are debates in academia, government and the media about what precedence personal privacy should take when weighed against national security. This may appear ironic when the public divulge personal information over social network sites and online advertising can predict their next 'object of desire' based on the profile they have built from tracking their online activities. However, as Solove points out [10] the 'I've got nothing to hide' argument is only used in relation to government surveillance and data gathering based on the argument that if I have done nothing wrong, I have nothing to hide. This places privacy in the context of law and order basing it on the principle that government surveillance is carried out within the confines of criminality and terrorism. If an individual is not involved in these activities, it follows that no harm can come from government data gathering. However, all it takes is for the media to highlight a leak of information and the tide of opinion will rapidly change

leading to an association with government security initiatives and public panic. The problem is one of a perception of a loss of control of personal data, an issue that proposed EU data protection Regulation is keen to address.

Solove [8] uses the 'I've nothing to hide' argument in relation to government surveillance to illustrate how it reduces privacy to one concept. By demonstrating the plurality of privacy he shows how issues such as data mining can build a profile and eventually lead to harm or embarrassment, or at the least something people never intended to re-surface. His argument focuses on the aggregation of data and the length of time it may be retained. It involves the ethical issues surrounding the use of secondary data without the owner's consent. Solove maintains that this illustrates an imbalance of power. This is an accusation that is more often heard against government surveillance powers than commercial enterprises, making its consideration more relevant to protecting critical infrastructure and national security.

Solove argues that the law looks for harm or injury, when the problem is about loss of control over personal information that may not seem important until it is mined. This means that there is accumulated information in one place that the person is (probably) unaware of. Solove's focus on aggregation makes the argument that data subjects have divulged information over their lifetime that they never envisaged would be aggregated with each other to form the comprehensive profile that may have become a reality when so much information is now in the public domain.

Many are not concerned. The "I've got nothing to hide" argument and others like it are prevalent in modern discourse on privacy. Solove argues,

"Cast in this manner, the nothing to hide argument is a formidable one. It balances the degree to which an individual's privacy is compromised by the limited disclosure of certain information against potent national security interests. Under such a balancing scheme, it is quite difficult for privacy to prevail." [8].

However, contextualizing privacy may mean that in the context of national security, privacy should not expect to prevail;

"… from an ethical viewpoint, the concept of balancing is, one could argue, nearly self-evident as it derives from the concept of privacy whose scope has been ethically defined as non-absolute. Therefore, one needs to draw the limits of the concept, eventually, by balancing it against other values, as is the case in political and societal, or inter-subjective contexts. One has to assume, however, that the characteristics of the balancing will vary

depending upon the context within which it is performed." [7].

5 Government Expectation

5.1 EU: Importance of CI protection and attitude to security

The European Programme for Critical Infrastructure Protection (EPCIP) resulted from a European Council Consultation in 2004 [11], which endorsed the intention of the European Commission to create a European Critical Infrastructure Warning Information Network (CIWIN). The proposal for an EC decision [12] does not mention 'privacy', although the Impact Assessment [13] states that the preferred option would mean that data collected in the CIWIN system would be on a non-personalised basis giving examples of methodologies, risk assessment tools, CIP guidelines and imminent risks and threats. The only personal data intended for collection would relate to 'experts' in Europe and would consist of their employer's name and business address. It is also specified that any data collected would be protected in accordance with data protection rules and shared on a 'need to know' basis within Member States (in Section 7.1 'Respect for fundamental rights').

Priorities for policy research are contained in a report [14] from the Centre for European Policy Studies (CEPS) Taskforce. This highlights the need not only for communication and agreed standards across the EU Member States, but a comprehensive international policy for the protection of CIs. The report discusses the inter-dependence of CIs and the domino effect of failure in one region where the effects spread across local and often international borders. For example, failure of the power grid would lead to citizens having no light or heat, traffic disruption with traffic lights being out, and disruption of the Internet system affecting banking and financial institutions. This is particularly relevant for power grids and the Internet. The report states: *"There is no way to organise a meaningful CIP policy without involving the private sector, as CIs in Europe are mostly owned by private players, many of which are worldwide operating companies."* (Executive Summary, p.5) This is not an easy task. For example, the importance in the energy sector to provide affordable power to customers while ensuring a secure and uninterrupted supply is acknowledged, along with the need to assess evolving technologies and their effect on the resilience of CIs.

The recommendations contained in the Taskforce's report have to be negotiated in an increasingly privatised and international market. The report states:

"…the waves of privatisation and market liberalisation have made the protection of critical infrastructure more difficult to achieve by government alone, as most of the critical infrastructures (approximately 85%)[1] are owned by the private sector. Since private suppliers are growing in importance, especially in the ICT field, they must be kept in the picture when designing a policy for CIP."

Criticism of the privatisation of CIs [15] accuses the EU of allowing CIs to become the subject of experimentation with privatisation describing 'institutional restructuring' as 'experiments of privatization, liberalization and deregulation'. This has led to a paradox where CIs have become more complex and interconnected, but are increasingly 'institutionally fragmented'. The concern about the lack of central control is echoed in the Taskforce's report [2] which is critical of the lack of a single contact point where incidents can be reported and action taken.

The 2012 Joint Communication on a Cybersecurity strategy for the EU [16] acknowledges the need for the development of capabilities and co-operation within and between member States and public and private sectors.

5.2 ENISA

Regulation (EC) No 460/2004 [17] established the European Network and Information Security Agency (ENISA) in 2004. Its duration was extended in 2011 [18]. ENISA's function is to support and enhance the capability of the EU Member States and the business community to respond to network information and security problems. Computer Emergency Response Teams (CERTs), more recently referred to as Computer Security and Incident Response Teams (CSIRTs). CSIRTs within and outside of the EU Member States collaborate to share information on security incidents and response, with ENISA's role being that of facilitator and information broker. Collaboration on Cybersecurity requires a high level of trust as information will be shared between private and public organisations operating CIs and across borders. It will also involve the sharing of information with countries outside the EU.

ENISA collects and analyses data on security incidents and provides advice on the security of network infrastructures. ENISA's role is to advise the private and public sectors on the protection of CIs. Its Mission Statement [19] sees networks and information systems "*… becoming as indispensable as electricity or water supply.*" ENISA's role is to encourage cooperation between public and private sectors at national and EU level.

[1] As of 2010.

In October 2012 ENISA organised its first Annual Privacy Forum to address gaps between research in the area of privacy and relevant policy initiatives. The subsequent report [20] does not mention CI or national security in relation to privacy or data protection. Nor are these topics mentioned in an ENISA study [21] on data collection and storage in the EU. However, an ENISA publication [22] on the resilience of networks states that resiliency from an operational culture will 'usually' encompass "*… the ability to protect business, information and customer data from external attack or internal security breaches.*"

5.3 EU Directives and Communications

On privacy it is noteworthy that the purpose of data protection in the EU is to support the free flow of information, rather than to restrict it [7]. Although the EU places high importance on personal data protection, proposing more stringent regulation for its protection, nonetheless, there is clear evidence that the protection of CIs and national security would take precedence of individual data protection. The European Charter on Human Rights (Article 8) provides a fundamental right to the protection of privacy. However, it subjects the right to certain limitations and exemptions:

There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Pointing out [7] that data protection and privacy are different, although related, the European Court of Human Rights has developed criteria to determine whether an issue of data protection relates to privacy (as set out in art. 8 ECHR). It is based on whether the data concerns the private life of the data subject. If the data are not 'essentially private' then it will depend on the extent of the processing; whether data is systematically stored, if there is a focus on the data subject and if the data subject would not reasonably have expected the data processing? Data protection (Directive 95/46/EC) applies every time personal data is processed, even where privacy (protected by art. 8 ECHR) is not necessarily affected [7].

The CEPS Taskforce acknowledges the trade-off that will have to take place in relation to privacy and personal data if, for example, deep packet inspection is to be used for Internet traffic and surveillance is to be used to protect CIs. Nevertheless, the 2011 Communication from the EU Commission on CI protection [23] does not mention either 'data protection' or 'privacy'.

Sharing of information will be required, not only between governments but between public and private CI providers. These will differ in relation to geographical spread. For example, traffic regulation will be local and national, whereas energy supply will be virtually borderless. While trust may be less of an issue within the EU, it will be more difficult to achieve on a global level. The taskforce reached the conclusion that in order to build trust there should be balance "… with effective privacy and personal data protection." However, this is in relation to intra-government and intra-industry rather than personal data of citizens. In asserting the importance of CI protection the Taskforce believes "… it must be effectively mainstreamed into the policy-making process of EU and national institutions." [2].

The European Programme for Critical Infrastructure Protection, COM(2006)786 [24], in discussing information sharing processes for CI protection stated that relationships of trust would be required and, as such, *"the proprietary, sensitive or personal information that has been shared voluntarily will not be publicly disclosed and that sensitive data is adequately protected. Care must be taken to respect privacy rights" (Section 4.4).* This is the only mention of 'privacy' contained in the document. It does not make it clear whether it relates to corporate information or the personal data of individual citizens. Although specifically mentioning 'sensitive data', again this could be interpreted as applying to sensitive corporate data. The Communication does not refer to 'personal data' or 'data protection' at any point.

In some ways discussion of privacy is redundant in relation to national security, synonymous with the secure functioning of CIs. European policy on national security is clear in that security will take precedence over the privacy of individual citizens in any trade-off. For example, the EU proposed General Data Protection Regulation [25] on the "processing of personal data wholly or partly by automated means" states in Article 2 (2) that "*This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security*".

Each country within the EU will have discretion in protecting their national security. Hence the British Government's proposal for legislation that led to a similar reaction from the British public as the US giving some indication of what public feeling would be and is discussed below.

6 Public Expectation

6.1 Of Privacy

There is no definition of privacy and therefore it is a subjective area. It can mean different things to different people at different times and in different contexts. A problem in relating privacy to a particular area, such as CI protection is that it will not be clear before the event that a perception of privacy violation has been created. However, once it has, it is difficult for the perceived violator to repudiate and defend. Paradoxically, public expectations differ radically when applied to government. Happy to exchange personal information in a trade-off for internet services, public outcry occurs when government is perceived to be gathering personal information, even when national security is threatened.

When privacy is viewed as a series of trade-offs and balances, [15] it offers some understanding of the willingness to trade personal information for a perceived reward. However, public perceptions of a balance between security requirements and privacy violation do not necessarily incorporate the immediate gratification that makes the trade-off palatable. Ubiquitous technology means that even the reluctant user is gaining a familiarity with technology and an awareness of the value of personal information. Where privacy and security, both determined to be 'social values', are analysed through a legislative lens, privacy is seen to be weakened by the need for protection against crime and terrorism. It has been argued that if security is to be balanced against privacy, the value of privacy to society as well as the individual has to be taken into account [7].

It is difficult to separate the ethical and social meanings of privacy, since society sets the agenda for what is ethical, or what it feels is morally wrong. Often this cannot be foreseen and, in any case, there will not necessarily be agreement. This is the case where there are differing views on the balance between individual privacy and national security; i.e. personal demands for privacy versus public interest and protection. In defining the difference between privacy and data protection, data protection controls how data is processed, but *"privacy shields the individual."* [7]. Proportionality in relation to privacy is emphasised by privacy scholars, particularly in relation to national security and is not proscriptive. Judgement will be required on an individual scenario basis taking consequences and security needs into consideration.

An article [26] on EU citizens' perceptions of data protection and privacy is a reminder that reactions to privacy and data protection when they impact national security are not necessarily 'informed'. Perhaps it is the lack of understanding found in various surveys in the article that allows the media

in many instances to set the agenda for public reaction.

6.2 Of Security

The 2012 Joint Communication on a Cybersecurity strategy for the EU [27] addresses personal data and privacy stating:

Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field.

The Communication goes on to state that security is a shared responsibility that needs to be recognised by public authorities, the private sector and individual citizens (p.4, para.4). The Communication also calls for product manufacturers to incorporate both security-by-design and privacy-by-design principles in products.

Citizens' familiarity with ubiquitous technologies such as smartphones and social networking means the public are increasingly aware of online security and privacy threats. There is a perceived lack of control in relation to personal information that is fuelled by media coverage of incidents of data breaches by government departments and agencies. It is against this background that CI and national security policies and protection measures are consulted on and agreed. Public acceptance can be gained through greater knowledge and information sharing. However, handling of personal information must be a primary concern. Each incidence when personal data is leaked is what will be remembered when public co-operation is required. Reactions to proposed security policies in the UK and U.S. outlined below demonstrate the need for public co-operation.

Shifting the 'meaning' of a terrorist attack on critical infrastructure captures the social and psychological effects that may be the main influence on how the public view their privacy in relation to protecting CIs. Burgess [28] conceptualises CIs and their protection in terms of 'social values'. In doing so he focuses on the value of CIs and shifts the emphasis from the actual CI to the effect its destruction has on the psyche of citizens, both in the areas affected and globally. His main argument is that a terrorist attack on a critical infrastructure has less to do with the disruption and even loss of life this may cause, but rather the loss of confidence of people in their CIs and the reality of future attack to engender fear and uncertainty. The value for the terrorist is in the fear they create rather than the material value of the CI. It is this element of

fear that may influence attitudes toward the protection of privacy in light of the need to protect national security and CIs.

6.3 Public reaction in the UK and U.S.

Empirical evidence shows that strong public resistance to the gathering of personal data exists, even in the U.S. in the aftermath of 9/11 [10]. In 2002 a proposed data mining project called Total Information Awareness (TIA) was not funded by the U.S. Federal Government due to a public outcry about privacy. The aim of TIA had been to gather financial, educational, health and other personal data in order to have profiles for national security purposes. It is suspected that components of it are still taking place in government agencies in a less systematic and more surreptitious form [10]. Similarly, in February 2013 Bill C-30, containing government surveillance powers was dropped by the U.S. Federal Government, again on the strength of public outrage.

Attitudes toward privacy were further demonstrated in reaction to the UK Government's Draft Communications Data Bill introduced in April 2012. It proposed to force Internet Service Providers to store details for a year of the online activity of UK citizens including emails, instant messaging, social media activity, web browsing and VoIP. GCHQ would monitor activity and the police, Serious Organised Crime Agency, HM Revenue and Customs and the Home Office would have access to the data. Sir Tim Berners-Lee said that such government surveillance would be a "destruction of human rights" and privacy advocates described it as 'Orwellian'. The Government Joint Review Committee found that the Draft Bill showed "*insufficient attention to the duty to respect the right to privacy, and goes much further than it need or should.*" The Bill is currently undergoing a second draft.

These public reactions may seem ironic given that, as already pointed out, advertisers know our shopping habits, what we like to buy, read and view and online businesses hold and trade our personal data. However, it provides an illustration of the subjective nature of ethics in relation to privacy, even when the security of critical infrastructures, national security and public safety is at stake.

The UK Cyber Security Strategy [29] acknowledges the place of ethics in its 'Guiding Principles' stating:

1.13 Cyber security poses particular challenges in meeting the tests of necessity and proportionality, as the distributed, de-centralised form of cyber space means that a wide range of tools must be deployed to tackle those who wish to use it to harm the UK's interests. A clear ethical

foundation and appropriate safeguards on use are essential to ensure that the power of these tools is not abused.
1.14 The programme of work outlined in this Strategy cannot and should not be progressed in isolation from these issues, and will require ongoing consultation with a variety of groups and organisations that work to safeguard our civil liberties and protect the privacy of the individual.

7 Upholding Expectations: PRECYSE

7.1 Precyse methodologies

Council Directive 2008/114/EC [1] concentrates on energy and transport. It is the first legal instrument on the subject of CI protection and focuses only on energy and transport sectors, but documents the need to include, in particular, the ICT sector. The Directive places the ultimate responsibility for protecting these CIs on their operators and owners.

The Precyse methodology has to address the handling of personal data relevant to users of the services supplied by the two demonstrators. Consideration also has to be given to the confidentiality of the processes and findings of the research. Precyse will fulfil expectations through building 'privacy-by-design' into the project from the start [30]. The necessity for this has been identified through the need for information sharing with semi-trusted third parties.

7.2 Insider threat

Insider threat will be addressed at Phase 2 of Precyse. Malicious threat from insiders has been found to be the most common type of threat to CI. The method of attack is normally not technically sophisticated, but involves insider knowledge. This threat may come from disgruntled staff or contract or agency staff.

An incident was reported in the U.S. [31] where both common and sophisticated malware was found in the industrial control system environment of a power plant facility. The malware was found on a USB drive regularly used by an employee to back up control system configurations within the control environment. The private firm reported the incident to the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS – CERT). This is an example of a non-malicious insider threat. This type of threat is addressed through technical security measures and staff training and awareness-raising.

7.3 D 1.2 Use Specification - Scenario 8

Privacy and data protection will apply to any surveillance that involves the monitoring of traffic in the Valencia demonstrator. Where car registration and licence plates are used in monitoring and/or recording of traffic flow, this will be regarded as personally identifiable information and subject to data protection.

Ethical privacy issues may be raised by any monitoring and surveillance of employees in, for example, a scenario where data collected through surveillance cameras recording those entering the building for authentication purposes. This may expose instances where the visual identification, building access identification and computer log on details are incompatible. However, this would be an issue that should be accounted for in contracts employees agree to and would be extended to contract, supply and agency staff.

7.4 Ethical principles relating to Precyse

The Precyse methodology specification will address and evaluate security, privacy, resilience and trust in critical information infrastructures. It therefore addresses the points previously raised in relation to ethical considerations.

Economical restrictions will also be accounted for in providing a security and management system, particularly relevant in the supply of energy to service users in an affordable manner.

The project will address privacy issues of the demonstrator partners and their consumers by separating confidential information related to the project and data protection for the personal information of service users. Where private or confidential information is stored it will be protected using cryptographic means and safely deleted when no longer required. This is in line with data protection legislation and satisfies ethical considerations where the collection of data should not be disproportionate to the needs of the project and will not include sensitive data.

The specific demonstrators involved in Precyse are service driven. In relation to ethical considerations, largely focusing on 'privacy', many of the arguments that pertain to general services provided by technology apply. The legal obligations in data handling are laid out clearly, although with exemptions for issues of national security. It is interesting to note that both Precyse demonstrators are functioning in CIs that also provide services, bringing the 'trade-off' principle into play where people are gaining a service in exchange for providing personal information. This is an exchange model the public are familiar with in their online activities and is generally

regarded differently from supplying personal details for government administration or monitoring purposes.

7.5 Smart Grid

If Smart Grid was to be adopted in the future the handling of personal data would become a major consideration. Information passing between the power provider and the consumer will include an unprecedented flow of information. Much of this will be a security as well as privacy issue as patterns of behaviour and home occupancy will be indicated by the patterns that emerge. These will be associated with physical and IP addresses, both of which are PII.

Non-trusted third parties could gain access to real time data containing personal information. They would be doing this with the permission of customers in order to provide services. This is an area that will test trust relationships and privacy by design technology.

8 Summary

The emergence of open networks in CIs has brought privacy and data protection issues into focus. The lack of references to privacy and security contained in EU policy documents on CI has been highlighted in this deliverable. What is acknowledged however is the need to establish trust in sharing information and data in order to protect CIs effectively. ENISA acknowledges the need for 'trust' as CIs are operated mainly by the private rather than the public sector. Exchange of information and data will take place between sectors and across national borders. Securing data will be paramount for the building of trust in information sharing that will be necessary to identify vulnerabilities and respond to any attacks.

In relation to public support for CI protection reactions to government monitoring and surveillance has been generally unfavourable. Public opinion tends to be shaped by media panic when public surveillance is proposed, or a data leak happens.

Recommendation 1: Priority needs to be given for the safeguarding of personal data of customers/service users in CIs in Europe.

Recommendation 2: Citizens should be educated in order to gain an understanding of the importance of CIs and the consequences of threats to their operation. In this way measures to safeguard them would be met

with co-operation rather than resistance. It should not be the media's role to set the agenda following a crisis or when security surveillance is proposed. An educated public will be equipped to provide a measured response to information about CI protection.

REFERENCES

[1] European Council Directive 2008/114/CE on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. [Online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[2] CEPS Task Force Report (2010) 'Protecting Critical Infrastructure in the EU'; Brussels.

[3] Myriam Dunn, 'The socio-political dimensions of critical information infrastructure protection (CIIP)'; *Int. J. Critical Infrastructures, Vol. 1, Nos. 2/3, 2005 (pp. 258-268).*

[4] Froomkin Michael A. (2000) The Death of Privacy; Stanford Law Review, Vol. 52, No:5, Symposium: Cyberspace and Privacy: A New Legal Paradigm? (May 2000), pp. 1461-1543.

[5] Solove, Daniel J., "Understanding Privacy"; Harvard University Press; Cambridge, MA, 2008.

[6] Paul Ohm (2009) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation; 57 UCLA Law Rev. 1701.

[7] PRESCIENT: Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment; Deliverable D1: Legal, social, economic and ethical conceptualisations of privacy and data protection (March 2011).

[8] Amitai Etzioni (1999) The Limits of Privacy, Basic Books; NY.

[9] Samuel D. Warren and Louis Brandeis, The Right to Privacy, 4 Harvard Law Review 193 (1890).

[10]Solove Daniel J. (2007) "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, *44 San Diego L, Rev. 745*, 768-72 (2007).

[11] COM(2004) 702 Critical Infrastructure protection in the fight against terrorism; Brussels 20.10.2004.

[12]Com(2008)676 Proposal for a Council Decision on a Critical Infrastructure Warning Information Network; Brussels, 27.10.2008.

[13]SEC(2008)2701 Accompanying document to Proposal for a Council Decision on creating a Critical Infrastructure Warning Information Network (CIWIN); Brussels, 27.10.2008.

[14] Protecting Critical Infrastructure in the EU, (2010) CEPS Taskforce Report [Online] http://www.ceps.eu/category/book-series/ceps-task-force-reports accessed 8.3.2013.

[15] Mark de Bruijne & Michel van Eeten (2007) Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment, Delft University of Technology.

[16]Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace; Joint Communication to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7.2.2013. [Online] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[17]Regulation (EC) No 460/2004 of 10 March 2004 establishing the European Network and Information Security Agency [Online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[18]Regulation 580/2011 [Online] http://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1

[19]ENISA Mission Statement [Online] http://www.enisa.europa.eu/about-enisa/activities/mission

[20]Report on Annual Privacy Forum (2012); ENISA [Online] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/report-on-annual-privacy-forum-2012

[21]ENISA: Study on data collection and storage in the EU [Online] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection accessed 12.3.2013.

[22]ENISA: Enabling and managing end-to-end resilience [Online] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/e2eres accessed 12.3.2013.

[23]COM(2011)163 on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber security; Brussels, 31.3.2011 [Online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF accessed 12.3.2013.

[24] COM(2006) European Programme for Critical Infrastructure Protection [Online]http://eur-lex.europa.eu/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

[25]COM(2012)11 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [Online] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[26] Dara Hallinan, Michael Friedewald, and Paul McCarthy, "Citizens' Perceptions of Data Protection and Privacy", *Computer Law and*

Security Review, Vol. 28, No. 3, 2012, pp. 263-272.

[27] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace; Joint Communication to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7.2.2013. [Online] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[28] J. Peter Burgess (2007) *Social values and material threat: the European Programme for Critical Infrastructure Protection* in Int. J. Critical Infrastructures, Vol. 3, Nos. 3/4, 2007.

[29] The UK Cyber Security Strategy (25 November 2011); Cabinet Office, London. [Online] https://www.gov.uk/government/publications/cyber-security-strategy accessed 15.3.2013.

[30] Nils Ulltveit-Moe, Terje Gjøsæter, Sigurd Assev, Geir M. Køien and Vladimir Oleshchuk "Privacy Handling for Critical Information Infrastructures" University of Agder.

[31] ICS – CERT Monitor October/November/December 2012 [Online] http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf accessed 8.3.2013.