View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by DepositOnce

DE GRUYTER PIK 2014; 37(3): 205–210

Simone Wurster*

Ethics and Privacy Issues of Critical Infrastructure Protection – Risks and Possible Solutions Through Standardization

Abstract: Recent studies propose a paradigm shift in standardization strategies and research and the use of ethical aspects as an additional factor to explain standardization success. This article goes one step further. It focuses on specific ethical and privacy standards and introduces privacy as a new dimension of the interplay between standards and innovation in the fields of civil security and the protection of critical infrastructures. Based on a survey, it represents mainly German and European perspectives. The article finishes by giving recommendations for new privacy standards which may help to raise acceptance for several new security solutions.

Keywords: privacy, standards, security technologies, public security, critical infrastructures

DOI 10.1515/pik-2014-0018

1 Introduction

Life in modern democratic societies requires security measures and there is a need for protecting critical infrastructures (CIs) in particular (see CRN, 2011; EC, 2004; Wurster, 2013[1]). Several recent studies also highlight the need for security-related standards, e.g. ECORYS (2009), ESRIF (2009), EC (2008, 2011) and Sáez et al. (2009).

CIs comprise all physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact for the relevant country (see EC, 2004, p. 2). They include for example energy systems, communications and information technology, water supply systems as well as transportation systems including airports, ports, the railway system and mass transit networks (see EC, 2004, p. 2). The focus of this article is on transportation infrastructure.

The EC's perception of security relates to public security and includes among others, protection against threats by terrorism and severe and organized crime (see EC, 2011, p. 1). Three kinds of civil security-specific settings can be distinguished: private places (e.g. privately owned houses or company buildings), public places (e.g. public parks, schools etc.) and semi-public places like airports, train stations; ports etc. (see Wuerttemberger, 2012).

Many semi-public areas represent CIs and are used by millions of people every day worldwide. Therefore their protection has great importance but security technologies bear ethical and privacy-specific risks (see Article 29 DPWP, 2007) which can impede the acceptance of new security solutions (see e.g. Hempel & Toepfer, 2004, and Wuerttemberger, 2012).

A definition of privacy is given in Wilkins & Christians' (2008) book: '(Privacy is) the condition of being protected from unwanted access by others – either physical access, personal information, or attention' (Wilkins & Christians, 2008, p. 277).

Principle privacy-related rights are defined by the Universal Declaration of Human Rights (UDHR), Article 12 and in Europe, for example, by the EU Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Article 8.

According to Craig & Ludloff (2011) and Wilkins & Christians (2008), privacy has two dimensions: physical freedom and having control over personal information. Privacy goals and security-related goals may contradict each other. Regarding CIs, security has specific importance and fulfilling both goals bears challenges. Specific standards may offer solutions and raise the acceptance of innovations in the security field but privacy-related standards for CI protection are missing (see e.g. ESRIF, 2009, and EC, 2011). Therefore, this article has four objectives: 1.) showing which security technology solutions bear special ethical or privacy-specific risks, 2.) identifying specific ethical and privacy risks, 3.) showing needs for standards and 4.) deriving implications for further research.

1 This article builds on Wurster (2013). 'Security technologies for the protection of critical infrastructures – ethical risks and solution offered by standardization', presented at the 5th ITU Kaleidoscope Conference, Kyoto Japan, 22–24 April 2013.

* Corresponding author: Simone Wurster:
E-Mail: simone.wurster@tu-berlin.de

Bereitgestellt von | Technische Universität Berlin
Angemeldet
Heruntergeladen am | 27.10.17 15:41

2 European & International Standards

A standard is 'a publication that provides rules, guidelines or characteristics for activities or their results, for common and repeated use' (CEN, 2014a). Our focus is on formal standards that have been adopted by one of the three European Standardization Organisations (ESOs) CEN, CENELEC and ETSI or by one of the three international organisations ISO, IEC and ITU. Their most popular deliverables are European Norms (ENs) and international standards (ISs), respectively.

In addition, these organizations have developed different other types of deliverables to foster the diffusion of innovation via standardization. A suitable instrument on both a European and an international level is the 'Workshop Agreement' which is offered by CEN and ISO. The specific documents are called CEN Workshop Agreement (CWA) and International Workshop Agreement (IWA) (see Hatto, 2013; CEN, 2014b and ISO, 2014 for a description). Developed in 10 to 12 months, they are quickly available to address specific market requirements. There are two additional possible deliverables in ISO and one in CEN which offer interesting conditions for researchers (see Hatto, 2013). They are most suitable for topics which have not reached a sufficient state of maturity for more formal standardization. These are international Technical Specifications (TS), CEN TS as well as international Publicly Available Specifications (PAS) (see ISO, 2014 and CEN, 2014c).

3 Literature Review and Research Gap

Investigating privacy and security-related standards requires in-depth insight into standard-related and security issues. This chapter analyses four aspects: a) advantages of standards and public security standards, b) ethical and privacy aspects of public security solutions, c) ethical and privacy aspects in standards as well as d) ethical and privacy aspects in standards for public security and the protection of CIs.

a) advantages of standards and public security standards: Blind (2004, 2009), STAIR (2011) and Swann (2000) give overviews of the many benefits of standardization. General advantages include, e.g., its contribution to global market access for innovative solutions, economies of scale, cost savings as well as the facilitation of compatibility and interoperability. Standardization also 'raises the acceptance of innovations among customers and public procurers' and therefore 'helps to accelerate the diffusion of innovations' (Blind, 2009, p. 16). Blind (2008) provides innovation economic findings regarding the importance of (public) security standards but there is no work that covers privacy standards in the context of public security.

b) ethical and privacy aspects of public security solutions: Ethical and privacy issues of security technologies are investigated, for example, by Article 29 DPWP (2007), Hempel & Toepfer (2004), PRISE (2008), Wuerttemberger (2012) and Wright & de Hert (2011). All authors show that privacy problems can impede the acceptance of new security solutions.

c) ethical and privacy aspects in standards: Fens (2013), Wurster (2013) and van de Kaa (2013) are three of the first to investigate privacy issues in standardization. Fens (2013) and van de Kaa (2013) proposed a paradigm shift in standardization strategies and research to include privacy aspects as a new factor to explain standardization success. Van de Kaa (2013) even calls for a new research discipline that includes philosophy, ethics and standardization management. Besides the more practice-oriented paper by Wurster (2013), research on privacy and ethical aspects related to *formal* standards is rare. This article addresses this gap.

d) ethical and privacy aspects in standards for public security and the protection of CIs: Part b) showed the importance of privacy aspects in the public security field. Measures addressing concerns about CI and the physical safety of the population in particular usually have a substantial impact on privacy (see ICO, 2010). Specific privacy standards may help to overcome such problems, but there has been no scientific work which investigates standardization related to privacy issues of security technologies for CIs so far. One reason is the novelty of the field. In 2011 the EC described a need for public security standards (see EC, 2011). The report only includes a general note that privacy issues need consideration. This article helps to overcome the related research gap.

The investigation of these issues needs to consider all groups of security technology and security solutions, for example closed-circuit television (CCTV) and radio-frequency identification (RFID) technologies separately: 'It is crucial to clearly distinguish different types of detection technologies (i.e. CCTV, RFID tags, biometrics, etc.) in order to match appropriate data protection solutions to each of them separately' (Article 29 DPWP, 2007, p. 4).

Bereitgestellt von | Technische Universität Berlin
Angemeldet
Heruntergeladen am | 27.10.17 15:41

4 Survey in the German Security Research Program

In order to gain insight into ethical and privacy-related problems of security technologies and to identify possible solutions, a study in the German framework program 'Research for civil security' was done in summer 2012. It was a follow-up study to a survey on security research and standardization among the participants of the research program and included 23 participants[2]. Six out of ten questions were related to ethical and privacy-specific risks of security technologies. The survey took place in June and July 2012. The results are presented in chapter 5. Survey data was coded and clustered with the software Atlas.TI.

5 Ethical and Privacy Risks of Security Solutions

In response to question 1 four areas presenting ethical and privacy-specific problems were identified: detection technologies, processing of data, security services and additional topics (which only received two mentionings).

Ethical and privacy-specific risks of detection technologies are regarded as most important. Figure 1 describes their nature in more detail.

According to the figure, two specific areas of detection technologies were identified: detection from a distance and obtrusive detection. Technologies which allow detection from a distance comprise all kinds of video surveillance (CCTV) solutions including intelligent CCTV as well as identification technologies, for example remotely identifying license plate numbers. The second cluster, 'obtrusive detection' includes body scanners, biometric devices as well as solutions for access control which allow the identification of people. In question 2, the participants were asked to rank a selection of the products and technologies they had listed in the previous question according to their ethical and privacy-specific risk potentials. Similar to the results from question 1, detection from a distance is regarded as bearing the most ethical and privacy-specific risks. Question 3 and 4 addressed specific ethical and privacy risks. Three groups of problems became apparent: restrictions to freedom, abuse and discrimination.

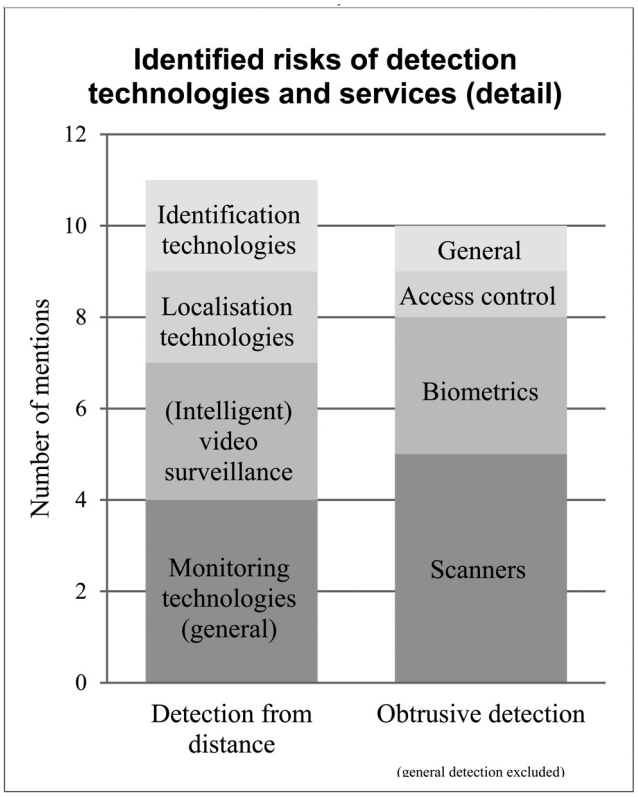

Figure 1: Ethical risks of detection technologies.

Questions 5 and 6 focused on the need for standards to better address ethical and privacy specific aspects in the development and use of security solutions and services. Based on the answers, six fields with specific needs for standards to reduce ethical risks were identified: biometrics, security-specific sensor solutions, video surveillance (CCTV), data storage, access control and security services. Furthermore, a need for a regulative document was unveiled in the specific area of intelligent CCTV.

In our further investigations we will examine aspects of access control within the analyses in the biometrics field. Suggestions regarding security services gathered by our survey mainly focused on the work of security service firms. These issues will be excluded from further analyses because they do not represent specific technology topics. The remaining fields will be investigated in the next two chapters. In addition, some responses unveiled in particular a need for certifications for ethic-friendly security products. We will refer to this issue in the next chapters, too.

2 6 experts from supplier companies of security-related products and services, 5 from research organizations, 8 from universities, 1 expert from an industry association and 3 experts representing the end user.

Bereitgestellt von | Technische Universität Berlin
Angemeldet
Heruntergeladen am | 27.10.17 15:41

Table 1: Suggestions for new working items for new standards.

Area	Suggestion by participants in the survey	Investigation of current standards (general and regarding CIs)		Remaining standardization needs for the protection of CI	
biometrics	matching of biometric records, conditions and limitations of the procedure	*ISO/IEC 15944-8*, CWAs 16113, 15499, Part I + II, 15262, 15263, 15292	ISO/IEC 19784-2, 19785-1, 19792, 24745, 24761 and ISO/IEC TR 24714-1	protection of (semi-public) CI, particularly airports and ports	use of biometric data in the context of public security
security-specific sensor solutions	ethic and privacy standard in general		no appropriate standard available		ethic and privacy standards for security sensors and security-specific sensor solutions
video surveillance	specification of the storage period, specifications for intelligent CCTV		ISO 22311, IEC 62676 series, particularly IEC 62676-1-1, EN 62676 series, div. European + national laws		general requirements for the processing of video data as suggested by ISO 22311
data storage	neutral supervision, a specification of the storage period and the type of data		EN 15713, ISO/TR 15801, ISO/TS 21547, div. European and national laws		definition of the kind of data stored for security reasons, rules for the matching of data for security reasons

6 Reducing Ethical and Privacy Risks in CI Protection by Standardization

Database and document analyses were done to compare the need for privacy standards in the field of public security expressed in the survey with existing standards and other relevant documents. An important European document related to **privacy in general** is the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Concerning public security, the directive includes specific passages on safeguarding e.g. national and public security. But permanent CI protection is not specifically covered by the directive.

Current activities in Europe focus in particular on the creation of a new General Data Protection Regulation which will supersede Directive 95/46/EC. The draft was released in January 2012 (EC, 2012). The European Parliament adopted a modified Directive in March 2014, while its implementation is expected to be finished in 2016.

The regulation does not include specific technology-related passages. More **technology-specific documents** regarding privacy are, for example, provided in **Europe** by CEN, though most documents are Workshop Agreements (CWA)[3] like CWA 16113, 15262 and 15499, part I and II. The documents are shown in table 1. An important player in the **international** arena is the ISO/IEC Joint Technical Committee (JTC) 1/Sub Committee 27/Work Group 5, 'Identity Management and Privacy Technologies'. Its focus in the privacy field includes topics such as 'A Privacy Framework', 'A Privacy Reference Architecture', 'Privacy infrastructures', 'Anonymity and credentials', 'Specific Privacy Enhancing Technologies (PETs)' and 'Privacy Engineering'. Privacy standards developed by the work group include, in particular, ISO/IEC 29100, ISO/IEC 29101 as well as ISO/IEC 29115.

Problems of ISO/IEC 29100 concerning public security and the protection of CIs are in particular its principles 'consent and choice', 'participation and access' and 'transparency and notice' because they can hinder investigations of irregular behavior which might endanger the population in a relevant area.

CWA 16113 and *ISO/IEC 15944-8* pay specific attention to privacy in the context of **public security** but specifics of the permanent protection of (semi-public) CIs (e.g. ports and airports) are not covered and managers of these infrastructures are expressing a need for action.

Further analyses were dedicated to specific technology areas. According to table 1, there are six documents which have specific importance in the **biometric** field. But there are limitations. *ISO/IEC TR 24714-1* offers, for example, no applications for the protection of CIs, public and semi-public areas and the specific use of data in contexts of CI protection. Specific privacy issues in the field of **sensors** are for example related to sensor tunnels, wireless sensor networks and sensor data fusion[4]. Our analysis

3 The adoption of CWAs is voluntary in the European member states.

4 See e.g. the German survey InfraNorm (2013). Sicherheitsethik, Privacy und Normung, available via the author.

Bereitgestellt von | Technische Universität Berlin
Angemeldet
Heruntergeladen am | 27.10.17 15:41

showed that ethical aspects in these areas are not represented appropriately yet. Suitable standards are not available. Specific aspects of **video surveillance** (CCTV) are covered by *ISO 22311*. It calls for monitoring access to the data, a mandatory storage time and an appropriate deletion of data after a relevant period, minimal masking techniques as well as training of staff in dealing with sensitive data. In addition, it includes a comment recommending implementing privacy specifications as fast as possible. The participants of our survey mentioned specific risks regarding intelligent CCTV. While conventional systems record all events during a monitoring period, intelligent CCTV systems only document detected events that deviate from the 'ordinary'. Resulting problems are in particular risks of abuse, discrimination risks and possible intimidation effects (see Wuerttemberger, 2012). Specific aspects related to these technologies are not included in the current version of ISO 22311. Documents on **data storage** include, for example, the European Standard *EN 15713* as well as the ISO report *ISO/TR 15801*. Recommendations for data storage which specify a specific period are not available but this field is also covered by many national laws and in Europe also by European regulation. Regarding video data the need for action is stressed by the ISO standard 22311. It calls for a mandatory storage time for such data but does not specify the storage period.

As mentioned in the previous chapter, several participants in the survey described a need for appropriate certification schemes to show the fulfillment of specific privacy-related requirements. Privacy Impact Assessments (PIAs) were invented to handle privacy issues in different fields (see Wright & de Hert, 2011, for an overview). Currently, PIAs for systems used for the protection of public and semi-public areas also suffer from a research gap. Important additional solutions to address ethical questions are offered by Privacy Enhancing Technologies (PETs) but most areas investigated in this article, for example sensors, are not covered by existing standards in this field (see ETSI, 2011).

Furthermore, no standard for PETs exists which particularly addresses specific security solutions for public and semi-public areas. In summary, the needs expressed by the participants of the survey are not appropriately met by current standards.

7 Suggestions for new Standards

In section 5, needs for various privacy standards in the security context were expressed. In section 6 they were analysed in detail. Table 1 summarized the results. First of all, our analyses showed the shortage of privacy rules in the context of public and semi-public security and the need for privacy standards that meet the specific requirements of CI protection and the security of public transportation infrastructure. In addition, figure 1 showed that the risk potential of detection from a distance including CCTV was top-ranked in our survey and ISO 22311 describes the need to implement as fast as possible privacy specifications published by ISO/IEC JTC 1/SC 27. Based on all results, six new working items for new standards were suggested: 1) a privacy standard for the protection of (semi-public) CI, particularly airports and ports, 2) a general standard defining the kind of data stored for security reasons, 3) rules for matching data for security reasons, 4) the use of biometric data in the context of public security, 5) privacy-related standards for security sensors and sensor solutions and 6) general requirements for the processing of video data as suggested by ISO 22311.

Besides the identified topics to be considered in new standards, the need for a regulative document covering privacy-related issues of intelligent CCTV which may be followed by specific standards was described. In addition, section 5 showed that the current need for action regarding privacy in the civil security field has merely caused the development of CWAs, specifications or technical reports in many areas in Europe. Several current CWAs relate to Directive 95/46 EC. The General Data Protection Regulation may require the development of new related standards. Furthermore, the development of formal standards based on selected CWAs and technical specifications and reports from the three ESOs is recommended. In the international arena comparable privacy-related standards and even workshop agreements are missing in many fields. Therefore these European documents may offer a stable foundation for future standardization activities in this broader context, too.

Earlier, we identified privacy as a new area in which standards can raise the acceptance of innovations. Recommendations to overcome privacy problems through standardization were formulated but standardization alone does not guarantee the realization of specific privacy-related requirements. As mentioned by several participants in our survey, appropriate certification schemes and procedures are necessary to ensure the implementation of the desired levels of privacy. The new European project CRISP (Evaluation and certification schemes for security products – Capability Project, 2014–2017) is addressing this gap.

Bereitgestellt von | Technische Universität Berlin
Angemeldet
Heruntergeladen am | 27.10.17 15:41

8 Summary and Further Directions

Blind (2009) and STAIR (2011) showed the importance of standards for raising the acceptance of innovative solutions. Fens (2013) and van de Kaa (2013) illustrated the novelty of investigating ethical and privacy aspects in standardization research. Based on a survey, we identified topics for new ethical and privacy standards which may support the acceptance of new security solutions. A remaining question is in which way and to what extent privacy and ethical standards raise the acceptance of security solutions. We recommend further in-depth studies focusing the different security fields and privacy dimensions. In addition, more research in general is needed to measure the importance of ethical and privacy aspects as an explaining factor for standardization success.

References

Article 29 DPWP [Article 29 Data Protection Working Party] (2007). Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law. Enforcement, Customs and other Security Authorities www.dataprotection.ro/servlet/ViewDocument?id=227.

Blind, K. (2004). The Economics of Standards: Theory, Evidence, Policy. Cheltenham 2004.

Blind, K. (2008). Standardization and Standards in Security Research and Emerging Security Markets. 3rd Security Research Conference Karlsruhe, 2008, 63–72.

Blind, K. (2009). Standardisation: a catalyst for innovation. Inaugural Address Series. Research in Management. Erasmus Universiteit. http://repub.eur.nl/res/pub/17558/EIA-2009-039-LIS.pdf.

CEN (2014a). European Standards. www.cen.eu/cen/products/en/pages/default.aspx.

CEN (2014b). CEN Workshop Agreements. www.cen.eu/cen/Products/CWA/Pages/default.aspx.

CEN (2014c). Technical Specifications (TS). www.cen.eu/cen/Products/TS/Pages/default.aspx.

Craig, T., Ludloff, M. (2011). Privacy and Big Data. Bejing, Cambridge, Farnham etc. 2011.

CRN (2011). CRN Report. Focal Report 6. Risk Analysis. Resilience – Trends in Policy and Research. www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/dokumente/Unterlagen_Risiken.parsys.19839.downloadList.95833.DownloadFile.tmp/crnfocalreport6resilience.pdf.

EC (2004). Critical Infrastructure Protection in the fight against terrorism (COM/2004/0702). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF.

EC (2008). Towards an increased contribution from standardisation to innovation in Europe. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0133:FIN:en:PDF.

EC (2011). Programming Mandate Addressed to CEN, CENELEC and ETSI to Establish Security Standards. ftp://ftp.cencenelec.eu/CENELEC/EuropeanMandates/M_487.pdf.

EC (2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

ECORYS (2011). Security Regulation, Conformity Assessment & Certification. Final Report. http://ec.europa.eu/enterprise/policies/security/files/doc/secerca_final_report_volume__1_main_report_en.pdf.

ESRIF (2009). ESRIF Final Report. http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf.

ETSI (2011). Technical Report Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436. www.etsi.org/deliver/etsi_tr/187000_187099/187020/01.01.01_60/tr_187020v010101p.pdf.

Fens, T. (2013). Smart metering in the realm of smart grids. Presented at the 5th ITU Kaleidoscope Conference, Kyoto Japan, 22–24 April 2013.

Hatto, P. (2013). Standards and Standardisation. A practical guide for researchers. European Union 2013.

Hempel, L., Toepfer, E. (2004). CCTV in Europe. Final Report. Urbaneye Working Paper No. 13 (August 2004).

ICO (2010). Privacy Impact Assessment Handbook 2.0. www.ico.gov.uk/upload/documents/pia_hand-book_html_v2.

ISO (2014). ISO deliverables. www.iso.org/iso/home/standards_development/deliverables-all.htm?type=pas.

PRISE (2008). Legal Evaluation Report. http://prise.oeaw.ac.at/docs/PRISE_D3.2_Legal_Evaluation_Report.pdf.

Sáez, A. C., Urech, A., Pereira, J. (2009). Current status of Security in Mass Transport. DEMASST Deliverable 3.1, November 2009.

STAIR [CEN/CENELEC WG STAIR] (2011). An Integrated Approach for Standardization, Innovation and Research. www.cencenelec.eu/news/publications/Publications/STAIR.pdf.

Swann, P. (2000). The Economics of standardisation. Final Report for Standards and Technical Regulations Directorate Department of Trade and Industry. Manchester 2000.

van de Kaa, G. (2013). Responsible innovation and value sensitive design and its application to ICT standardization. Presented at the 5th ITU Kaleidoscope Conference, Kyoto, Japan, April 2013.

Wilkins, L., Christians, C. G. (2008). The handbook of mass media ethics. New York, 2009.

Wright, D., de Hert, P. [eds.] (2011). Privacy Impact Assessment. Law, Governance and Technology Series, Vol. 6. Dordrecht 2011.

Wuerttemberger, T. (2012). Rechtswissenschaftliche Begleitforschung zur intelligenten Videoueberwachung. BMBF-Innovationsforum 'Zivile Sicherheit'. www.bmbf.de/pubRD/B1-I_Wuerttemberger_Redemanuskript.pdf.

Wurster, S. (2013). Security technologies for the protection of critical infrastructures – ethical risks and solution offered by standardization. Presented at the 5th ITU Kaleidoscope Conference, Kyoto, Japan, April 2013.

Simone Wurster: TU Berlin – Innovationsökonomie, Müller-Breslau-Str. 15, 10623 Berlin, Germany

Bereitgestellt von | Technische Universität Berlin
Angemeldet
Heruntergeladen am | 27.10.17 15:41