2006

The risk of public data availability on critical infrastructure protection

Roba Abbas

*University of Wollongong, roba@uow.edu.au*

---

**Publication Details**

The risk of public data availability on critical infrastructure protection

Abstract
This paper examines the threat of freely available information on critical infrastructure protection (CIP) efforts. Critical infrastructure are the services required to maintain the stability and security of a country, and comprise both physical and cyber infrastructures. These interdependent entities must be protected from natural disasters, accidental errors, and deliberate attacks. The CIP process typically includes vulnerability assessment, risk assessment and risk management, and has been a global concern for many years; the concern now amplified in Australia due to a number of recent events such the 9/11 attacks, and the Bali bombings. The events have called into question the role of information and communication technologies (ICTs) in both preventing, and aiding such activities. ICTs, primarily the Internet, provide a means of gathering public data. Public data refers to ‘sensitive but unclassified’ information; that is, information that may not on its own appear harmful, but when compiled with other data can be truly revealing about an individual or critical infrastructure. The paper presents the risk of ‘sensitive but unclassified’ data being available in the public arena (on the CIP process). There is an evident need for increased awareness of this issue throughout Australia. Additionally, further research must be conducted into the topic, in an attempt to achieve a balance between providing data publicly and restricting access in the interest of national security.

Keywords
risk, public, data, availability, critical, infrastructure, protection

Disciplines
Physical Sciences and Mathematics

Publication Details

This conference paper is available at Research Online: http://ro.uow.edu.au/infopapers/1643
The risk of public data availability on critical infrastructure protection

Roba Abbas
School of Information Technology and Computer Science, University of Wollongong

Abstract

This paper examines the threat of freely available information on critical infrastructure protection (CIP) efforts. Critical infrastructure are the services required to maintain the stability and security of a country, and comprise both physical and cyber infrastructures. These interdependent entities must be protected from natural disasters, accidental errors, and deliberate attacks. The CIP process typically includes vulnerability assessment, risk assessment and risk management, and has been a global concern for many years; the concern now amplified in Australia due to a number of recent events such the 9/11 attacks, and the Bali bombings. The events have called into question the role of information and communication technologies (ICTs) in both preventing, and aiding such activities. ICTs, primarily the Internet, provide a means of gathering public data. Public data refers to ‘sensitive but unclassified’ information; that is, information that may not on its own appear harmful, but when compiled with other data can be truly revealing about an individual or critical infrastructure. The paper presents the risk of ‘sensitive but unclassified’ data being available in the public arena (on the CIP process). There is an evident need for increased awareness of this issue throughout Australia. Additionally, further research must be conducted into the topic, in an attempt to achieve a balance between providing data publicly and restricting access in the interest of national security.

Keywords: public data, information access, terrorism, critical infrastructure
1 Introduction

This paper examines the risk of freely available information on critical infrastructure protection (CIP) efforts. To establish a proper understanding of this subject, it is important to consider three fields of study. The areas to be independently assessed include critical infrastructure (a definition of the term, and why critical infrastructures are important), critical infrastructure protection (the steps in the protection process, and the impact of recent events), and public data availability (the nature of public data, the impact of information and communication technologies, and national security vs. open information access issues).

2 Critical infrastructure

Critical, by definition, refers to an entity that is essential or vital in nature (Bezerra et al., 2005). Critical infrastructures, more specifically, are the essential services that contribute to the stability and security of a country (Chakrabarty and Mendonca, 2004; Rinaldi et al., 2001).

From a historical perspective, critical services have been in existence since the development and growth of cities, which led to the need for water supplies (Mendonca et al., 2004). In the Australian context, critical infrastructure encompasses banking and finance, transport and distribution, energy, utilities, health, the food supply and communications (Attorney General’s Department, 2006; TISN, 2006). Throughout this paper, the term critical infrastructure represents the listed services.

In terms of the Australian situation, the Australian Security Intelligence Organisation (ASIO) provides a definition of critical services as:

“[t]hose physical facilities, supply chains, information technologies and communications networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia’s ability to conduct national defence and ensure national security” (ASIO, 2006).

This definition is reflected in key Australian agencies that focus on critical infrastructures, and related protection campaigns such as the Attorney General’s Department and the Trusted Information Sharing Network.

2.1 Physical and cyber infrastructures

While critical infrastructure was traditionally described as the necessary physical services within a given community, the definition has been extended by a number of academics to encompass cyber infrastructures (Kun, 2002; Neumann, 2002; Overill, 2001). This is primarily due to the prominence of information and communication technologies (ICTs) in recent years, and the consequent increased reliance on computer networks.
De Bruijne (2004), and Chakrabarti and Manimaran (2002), state that the progression of information and communication technologies has created a situation where physical critical infrastructures heavily depend on the support and operation of cyber infrastructures. Similarly, Overill (2001) states that physical and cyber infrastructures are interdependent entities; in particular the prosperity of physical services such as power, water, electrical and emergency services is reliant on digital systems or infrastructures. These concepts are reinforced by Feglar and Levy (2004), who feel that computer communications underlie the global economy, and are required to ensure that physical infrastructures are properly functioning, as they are interrelated and interconnected.

2.2 Infrastructure interdependencies

In addition to the relationship between physical and cyber infrastructures, it is vital to consider the interdependencies existing between the individual infrastructures. These relationships are of particular importance, as critical infrastructures today do not exist in isolation; rather there are physical or logical connections between them. Mendonca et al. (2004) describe critical infrastructures as ‘systems of systems’; that is, they must be regarded as interdependent services. While a number of studies (such as that by Rinaldi et al., 2001) model or map such interdependencies, Mendonca et al.’s investigation assesses the impact of such interdependencies in a real world situation (that is, the impact of interdependencies on the events of 9/11). The research revealed that disruptions were dispersed across all eight infrastructures (as recognised by the US President’s Commission of Critical Infrastructure Protection).

Schainker et al. (2006) agree with this claim; that critical infrastructures should be viewed as inextricably linked entities. This is evidenced in the authors’ study of the electricity infrastructure, which revealed that a threat affecting one area would undoubtedly impact on the dependent critical services. This is particularly relevant to aid in grasping the complex environment in which these services exist, and the difficulties in maintaining reliable operations, and protecting against potential vulnerabilities.

As is evident by this body of literature, critical infrastructure relationships are complex, and difficult to define and manage. Therefore, any study on critical services must consider such interdependencies, as they ultimately impact on the critical infrastructure protection process.

3 Critical infrastructure protection (CIP)

Critical infrastructure protection (CIP) refers to safeguarding the identified services from potential harm, including physical and/or electronic attacks (ASIO, 2006; Schainker et al., 2006). Amin (2005) and Mendonca et al. (2004) identify the sources of infrastructure vulnerabilities as natural disasters, system complexities,
equipment failures, human errors and deliberate sabotage/attacks (which is the focus of this paper). Similarly, Kun (2002) recognises these sources in view of national security, economic stability and public safety concerns, highlighting the importance of the infrastructure protection process.

The value of the CIP process is also evidenced in a number of recently established initiatives supported by government and research bodies within Australia, but also internationally. For instance, the Australian Research Council (ARC) lists critical infrastructure protection as one of the major ‘Priority Areas for ARC Funding 2005-2006’ (ARC, 2006). Additionally, issues of threat detection and counter-terrorism (which can be considered subsets of the CIP process) are identified as essential by the Research Network for a Secure Australia (RNSA, 2006). This is also reflected in many nations, such as the US, which recognises critical infrastructure protection as one of its six mission areas (Yen, 2004).

Thus, the protection of critical infrastructure is a crucial issue for all countries, and chiefly aids in maintaining national security, an issue that has gained importance as a result of a number of events (particularly in recent history).

3.1 Recent events

CIP has been a global concern since the Cold War; however, the issue has gained increased exposure in Australia since the incidents of September 11, 2001 and Bali, 2002, in addition to the Y2K concerns of the late nineties (Rothery, 2005; Luijff and Klaver, 2004; Emergency Management Australia, 2003; De Bruijne, 2004). Such recent events, specifically 9/11, have raised public awareness of the vulnerabilities and risks existing in their surroundings, and the need for eliminating or mitigating these threats (Neumann, 2002).

The CIP literature to date has a common element in that a majority of the studies cite these occurrences (that is, events of the past forty years) as creating a heightened need for protecting infrastructure networks (Amin, 2005; Amin 2002). Therefore, a situation presently exists where nations are developing the strategies and stages of the CIP process, in order to avert situations such as those identified.

3.2 The CIP process

As with the definition of critical infrastructures, the CIP process inevitably varies between nations. This process, whether referring to physical or cyber infrastructures, is constrained by a number of factors, such as social, political and economic aspects, in addition to a country’s specific environment (Bezerra et al., 2005).

The first stage in the CIP process involves assessing the context in which the infrastructure exists (including consideration of the previously mentioned factors). A paper by Bezerra et al. (2005) suggests that a country’s unique context affects the CIP strategies implemented, using Brazil’s telecommunications infrastructure as a case example. This stage is followed by measuring the threats to the identified
critical services, the establishment of security controls, the creation of an ideal scenario and finally a comparison with the actual situation (providing necessary recommendations).

Similarly, a study by Luiijf and Klaver (2004), deals with the various phases in the CIP process. They focus on the ‘Quick-scan’ phase, which identifies the critical assets that require protection. An essential outcome of this study is the need for a multi-tiered approach to CIP; that is, providing protection at the strategic, tactical and operational levels. Other authors (Jones et al., 2003) identify risk assessment (identifying the risks, sources, interdependencies and developing threat scenarios) and risk management (cost evaluation, and conducting a trade-off analysis when selecting a response option) as core phases of the CIP process, which follow the identification of the critical infrastructure.

Whilst CIP efforts are typically focussed on the protection of physical infrastructures, the importance of safeguarding cyber critical services is gaining recognition. Threats to cyber infrastructures can be just as damaging, and reach a greater population, as an attack may be perpetrated from across the globe, on multiple sites (Elbert, 2003). Feglar and Levy (2004) propose an independent process for protecting cyber critical infrastructures which includes scope definition, asset identification and valuation, threat and vulnerability assessment, risk analysis and risk management. Throughout the cyber protection process Shainker et al. (2006) state that an important element in maintaining cyber security is to understand that the infrastructure (as a whole) is only as secure as its ‘weakest link’. This also holds true for physical infrastructures, due to the interdependencies discussed in section 2.2. Additionally, the elements of the cyber protection process can be aligned with the physical CIP phases, as a general pattern in both models emerges.

For instance, Australia’s national guidelines for protecting both physical and cyber infrastructures involves risk assessments, public information and media management, prevention and preparedness, and response and recovery (Attorney General’s Department, 2006).

Although minor variations exist between the CIP phases internationally, the typical steps in the CIP process can be regarded as vulnerability assessment/scanning, risk assessment, and risk management (Luiijf and Klaver, 2004; Jones et al., 2003). This paper aims to introduce the potential risk posed by public data availability to the CIP process, an issue that has not been adequately addressed in the literature.

4 Public data availability

Public data is concerned with ‘sensitive but unclassified’ data that may be obtained through open or freely available outlets. This refers specifically to information that may be unclassified when used independently, but when combined enables inferences or previously unconsidered patterns to emerge, which may prove harmful to the CIP process (Thuraisingham, n.d.).
Givens (n.d.) states that public records (or data) may be provided in two ways, either freely or commercially. Even though the latter requires a fee for access, it remains available in the public arena and can potentially be obtained by all individuals.

Hariharan et al. (2005) extends the issue of data availability to focus on integrating geographic information system (GIS) data from disparate sources in order to improve the means in which data (particularly commercial) is accessed in CIP campaigns. This study marks a shift in focus from personal to geopatial data. For example, authors such as Givens (n.d.) focus on personal data, that is, information concerned with an individual, such as health and legal records. However, the focus of Hariharan et al.’s paper is on location specific data with regards to critical services.

Since the events of 9/11, a direct link has been drawn between data collection facilitated by information and communication technologies (ICTs) and the act of terrorism (Davies, 2002), or threats to critical infrastructure protection endeavours. The various aspects of ICTs in relation to CIP are examined.

4.1 The role of information and communication technologies (ICTs)

The importance and increased use of the Internet, and Information and Communication Technologies (such as biometrics, database processing, geospatial information exploitation, video processing and visualisations) have amplified the risks on critical infrastructures (Popp et al., 2004). These technologies provide outlets for data/information exchange, and have simplified the ability to transmit data. ICTs are providing tremendous opportunities for development. Kun (2002) describes the traditional technology focus, which has been on increasing the capabilities, productivity, and increasing the speed of technology whilst concentrating on digitising data, information and knowledge. The author feels that technology users have also become more proficient in utilising the available technology tools, and consequently accessing information. This proficiency in technology use also applies to individuals with a malicious intent (such as terrorist groups, for example).

An introductory study into the consequences of public data availability on critical services (in the US) states that there is an increase in the education levels of the individuals/groups attempting to penetrate critical services (Breeding, 2003). Breeding’s method involved assessing various online sources in an attempt to determine the threat posed by ‘sensitive but unclassified’ data availability to US physical security. The study found that terrorists’ use of technologies, and the availability of certain tools, has become progressively sophisticated, allowing room for the collection, use and duplication of ‘sensitive but unclassified’ information, to be used for ill purposes. In a book titled Terror on the Internet: The New Arena, The New Challenges, Weinmann (2006) describes terrorist use of the Internet for information warfare (or cyber terrorism) purposes, and data collection.

Information warfare is closely related to the issue of cyber terrorism, a term
that was first used in the 1970s, but became popular in 1996. According to Overill (2001), the phrase is generally defined as the premeditated attack on information activities and infrastructures, whilst preventing an attack on one’s own information resources. That is, information warfare involves employing both an offensive and defensive strategy simultaneously. This issue is particularly relevant due to the over-reliance on computer or cyber infrastructures, most notably the Internet. While authors such as Elbert (2003) feel that cyber terrorism is a recent, genuine concern for the protection of critical services, Weinmann suggests otherwise.

Weinmann’s studies found that it is highly unlikely that terrorists will use ICTs to launch cyber attacks; however, the Internet remains a repository for the collection of information/data about transportation, infrastructures and maps, for example (Cherry, 2005). It is believed that terrorists are increasingly using ICTs to further their cause, and carry out their preparations (Davies, 2002). Furthermore, the “intelligence information gained by cyber terrorist activities can be used to support the more traditional forms of terrorism” (Elbert, 2003, p.16/17).

Relevant to this concept of data collection is the chief idea that information and communication technologies can both aid, and hinder national security efforts, with particular reference to terrorist threats (Kun, 2002). Authors such as Yen (2004), Popp et al. (2004), Stout (2004), and Amin (2005) provide some insight into these issues.

Yen (2004) examines how ICTs can be utilised positively to advance the homeland or national security cause. Popp (2004) also shares the view that if used to their full potential, ICTs can ultimately assist in making informed decisions, and potentially prevent terrorist attacks. However, it is also important to address the negative implications. That is, that these technologies are also at the heart of the national security problem, and may be utilised negatively.

Stout (2004, p. 142) describes the present age as a “hybrid era”, in that it promises great potential for technological advancement within an uncertain context (referring primarily to terrorist activities). Technology was previously viewed in terms of its ability to provide safeguards, however, the theme of Stout’s paper is that technology alone cannot prevent acts of terrorism, and data misuse. This is based on the premise that information and communication technologies are revolutionising the area of communications, thus enabling improved information sharing, specifically through the use of the Internet. This signifies that the efficient and correct use, and understanding of these technologies will determine the success of both malicious activities, and national security operations (Stout, 2004).

Amin (2005) supports Stout’s claims, classing the protection of critical infrastructures largely as a technological problem or issue. The author feels that technology can serve two purposes; the first is to aid in penetrating or threatening a particular infrastructure, the second to provide protection mechanisms to safeguard the same services.

The conflicting roles of ICTs have been widely discussed in the literature;

Page 207
resulting in the requirement to review a number of issues such as national security (including CIP) in terms of censorship, open information access, and the related privacy concerns.

4.2 National security (CIP), open information access and privacy

It has been asserted that the mentioned recent events (such as 9/11) could have been prevented if access to particular datasets in the public arena was limited (Kumagai, 2003). This accordingly raises the need for controlling access to ‘sensitive but unclassified’ data, in order to maintain national security. These concerns introduce the concept of censorship, or restricting access to information that may be used in an adverse manner. Davies (2002) notes that censorship in another era may have failed to be implemented or considered, as it attacks the basic principles underlying the right to privacy, free speech, and open source information. However, it is now a current issue, which must be resolved or addressed. The literature on the censorship of ICTs, particularly the Internet, agree that this task is difficult to achieve, and somewhat impossible.

Peace (2003) explores the issue of censorship in higher learning institutions, such as universities, measuring the importance of this area to heads of computer services departments. The study suggests that the issue of censorship is not a priority at present, and will unlikely be one in the near future. Universities are in conflict in terms of restricting undesirable information, whilst allowing legitimate Internet sourced to be accessed. This struggle perhaps exists due to the nature of ICTs, and particularly the Internet, which “defies censorship” because of its inherent structure, and characteristics, most notably its capacity to allow public access to information, and the creation and distribution of data (Ang and Nadarajan, 1996, p.74). These issues continue to be a topic of debate, with many views or solutions being offered by academics.

For instance, Shearer (1998) provides an alternative view to censorship, highlighting the need for establishing a ‘Code of Ethics’ to govern communications over the Internet. This is based on the need for the ‘responsible global citizen’ to overcome the negative aspects of Internet technology, requiring global community members to individually accept responsibility for their actions, and maintain basic human rights, environmental awareness, and global advancement. However, it must be noted that this paper was written in 1998, prior to a majority of the events discussed in section 3.1., after which the concept ‘public good’ has been generally disregarded in the literature. Instead, various governments, such as the Australian, have enacted technology-related (or censorship) legislation, such as the laws to intercept digital communications such as email.

While the discussion has focussed on censoring ICTs, a contradictory element exists in the literature, whereby there is the call for increased ‘intelligence’ or information access to assist with maintaining an appropriate level of national security.
In recent years, government agencies have expressed the need for information or data collection in the interest of national security.

Kumagai (2003) stresses the need for information access, with a focus on the FBI (Federal Bureau of Investigation), and its role in intelligence gathering and counter terrorism. The FBI is seeking to reform in a number of areas of intelligence gathering, such as increased data warehousing and data mining; that is, collecting data on individuals from various data sources and identifying patterns. In collecting such data, Kun (2002) raises concerns over data misuse, and its impact on civil liberties. This raises the issue of balancing privacy concerns with national security issues.

Privacy literature and concerns have been in existence for centuries, however, such concerns have now been exacerbated, and personal privacy has been applied to the technology arena (Walters, 2001).

Givens (n.d.) discusses the delicate act of balancing access to public data and maintaining personal privacy, with particular reference to legal records (such as court files and case indexes). Governments are increasingly providing such information online. Givens (n.d.) feels that the notion of e-government (and data provision) is primarily to allow the public to monitor the activities of the government. However, a number of negative consequences will inevitably arise due to public record access, most notably that the records will be used for secondary purposes (such as to make inferences, and to perform data mining activities).

As this body of literature has suggested, balancing national security, open information access, and privacy concerns is difficult. Therefore, when identifying the threat of public data availability, it is important to note that providing mechanisms to counteract the threat is a difficult task, and must be carefully considered in the interest of Australia’s national security.

5 Conclusion

This paper introduced the risk of public data availability on the critical infrastructure protection (CIP) process. This was achieved by amalgamating three bodies of literature including critical infrastructure, critical infrastructure protection and public data availability. The various factors surrounding and complicating the issue have been presented, raising the need for a detailed examination of the topic in terms of achieving a balance between public data access and maintaining national security in Australia. The awareness that freely available information can threaten the CIP process is a primary step in achieving this balance. However, it is very clear that further research into this field is required.

References


