IDENTIFICATION OF SOURCES OF FAILURES AND THEIR PROPAGATION IN CRITICAL INFRASTRUCTURES FROM 12 YEARS OF PUBLIC FAILURE REPORTS

H. A. Rahman, K. Beznosov, J. R. Martí

Members of the I2C Group
Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, Canada

Introduction

Modern Communication and Information Technology Infrastructure (CITI) provides key links and services to many other critical infrastructures [1], such as telecommunication, electricity, water supply, oil and gas networks, transportation, financial services, etc. Over the years, integration of these infrastructures with CITI has become pervasive, extensive, and complex. As such, failure in CITI, either due to an accident or caused by a malicious attack, can propagate to other infrastructures and can degrade or disrupt their functionalities. Conversely, failures in other infrastructures can also propagate to CITI and hence disrupt the operation of many of these interconnected systems. Such disruptions may lead to huge disturbances in the public life of modern nation states. Volatile world situations increase these threats even further. As a result, there are enormous concerns for secure and reliable operation of different critical infrastructures [1, 2]. One of the prerequisites for smooth operation of these interconnected infrastructures is to gain understanding of their interdependencies. By studying the origin of the infrastructure related failures and their propagation patterns, we can develop a better understanding of their interdependencies. Such understanding can be useful for decision makers and infrastructure operators for policymaking and system design [3].

Since 1992, US telephone companies are required to submit major failures information to the US Federal Communications Commission (FCC). Using FCC outage reports, a study was done on the failure pattern of Public Switch Telephone Networks (PSTN) [4]. According to our knowledge, no other critical infrastructure providers in North America are obliged to disclose their failure related information. However, such data could help the research community to develop good understanding of failure patterns and their interdependencies among different critical infrastructures. Data from infrastructure service providers is especially helpful, because they may give detailed information about the systems' states, their control parameters, input and output specifications, operating assumptions, back-up facilities, management procedures and practices, and other physical and environmental constraints [5]. Unfortunately, both public and private infrastructure operators are reluctant to share this information with the research community [6]. The FCC Outage Report mentioned above is accessible only to the users of FCC and the US Department of Homeland Security (DHS) [5].

Given this reality, one possible alternative is to use public domain infrastructure failure reports, such as newspaper or mass media reports to develop an understanding of infrastructure interdependencies. There are two major difficulties in this approach; i) normally these failure reports have only brief amounts of information, and ii) they do not have any regular structure. However, even though individual reports may not give much information about a specific failure, by studying a large number of cases we can trace common trends among similar classes of failures. To address the second obstacle, we classify these reports based on their failure type and extract meaningful information through some critical attributes. We have collected 347 cases of 12 years failure data (1994 to 2005) from the Association for Computing Machinery's (ACM) RISKS forum [7], which is the largest known public repository of this kind of reports. Posting to this forum is moderated, which ensures a certain level of quality and reliability. Since the reported cases to this forum are only a fraction of the actual events, there may be a concern about the usefulness of the statistics we can derive from our analysis. However, since the trend of reporting to this forum is related to the public perception of risks, research shows that despite partial information public perception of risks is fairly accurate [8, 9]. To ensure authenticity of our selected cases, we give special importance to the verifiability of our selected report's sources. For instance, we give preference to the newspaper reports than to reports by private individuals. Our methodology is discussed in detail in Section 3.

In this work, we have identified interdependencies between CITI and other infrastructures based on some key factors, such as, origin of failures, impact of failures in spatial and temporal dimensions, affect of failure on public safety and their propagation from CITI to other critical infrastructures and vice versa. More specifically, we would like to answer questions such as, what are the main causes of infrastructure failures, what is the nature of their impact; what

locality is affected by them and their geographical locations, how their fatality changed over time, and how infrastructures are related to each other. In the absence of any formal model of interdependencies between CITI and other critical infrastructures, our findings should give useful ideas to the policy makers, practitioners and researchers. In Related Work section, we discuss previous works to classify and interpret infrastructure related failures. In Approach and Methods section, we give a brief overview of our own methodology. In Failure Database section, we give a brief description of our failure database. In Results section, we summarize the results of our analysis. Finally, in Conclusions section, we discuss the contributions of this research and future research directions.

Related Work

There have been three major approaches to classify and interpret infrastructure related failures. The fist approach focuses on the failures and their impacts related to CITI [4, 11, 13]. The second approach focuses on understanding of failures in any computer-based system and is not limited to CITI [10, 14]. The third approach classifies failures and interdependencies among the critical infrastructure in a general system agnostic way [15].

Richard Kuhn [4] analyzes public switched telephone network (PSTN) failure data based on six failure categories. These are human errors, acts of nature, hardware failures, software failures, overloads and vandalism. Using this scheme, he analyzed two years of PSTN failure data (1992-1994) from the US Federal Communication Commission (FCC). His analysis shows the impact of different types of failures on PSTN operation. John Howard [11] proposes a taxonomy based on attack types in computer networks and uses that taxonomy to perform frequency analysis of more than 4000 security related incidents reported to Computer Emergency Readiness Team Coordination Center (CERT/CC). From the results of this analysis, he proposes a set of recommendations for government, vendors, CERT/CC, and individual users to improve security practices. Howard and Longstaff [12] further extend this taxonomy by incorporating additional terms, such as additional objects and attributes like site name, attack date, reporting time, etc. Chakrabarti and Manimaran [13] propose a taxonomy to classify Internet infrastructure security failures. Their classification is based on a survey of different intrusion detection and prevention techniques. They classify Internet infrastructure failures into four categories: DNS hacking, routing table poisoning, packet mistreatment, and denial of service attack.

Peter Neumann initiated the Association for Computing Machinery's (ACM) RISKS forum [7] in 1985 to compile computer related system mishaps which affect public life. Later Neumann published a book (1994) "Computer-Related Risks" [10], where he selectively compiled a large collection of RISKS forum reports based on problem sources. These include problem in requirement definition, system design, hardware implementation, software implementation, system use and operation, environmental problems, etc. Through this analysis, he draws attention to the safety and security issues associated with each type of failures. Avizienis et al [14] propose another generalized taxonomy based on computer systems reliability and security aspects. Their approach is to compile a few key definitions as a set of generalized concepts and to extend those concepts with extended sets of definitions. The main objective of this taxonomy is to use these concepts on a wide variety of cases.

Rinaldi et al [15] address classification of failures and interdependencies among the critical infrastructure in a system agnostic way. Their taxonomy is based on six functional dimensions to determine cross infrastructure interdependency issues. These are: types of interdependencies (e.g., physical, cyber, logical), infrastructure environment (e.g., business, economic, health care), coupling and response behavior (e.g., adaptive, loose, tight), infrastructure characteristics (e.g., temporal, spatial, organizational), types of failures (e.g., common cause, cascading, escalating), and state of operations. (e.g., normal, stressed, repaired). However, their failure source classification is very restrictive (e.g. common cause, cascading, escalating) and gives a very limited number of options to analyze the RISKS forum failure reports.

In our research, we have used Kuhn's [4] approach for CITI and related critical infrastructure failure classification. However, we have added two additional categories to Kuhn's original six. These are malicious logic fault and authorization violation fault. Even though these two are software related faults, due to their intentional and malicious nature, they are in separate categories. In recent years, these two faults have become of increasing concern for critical infrastructures management. Their remedial methodologies are also different from traditional software failures.

Approach and Methods

We have followed a four step methodology to collect and analyze failure reports. We started with a systematic collecting of failure cases from RISKS forum, we then categorized these reports based on their failure type, extracted useful information from these classified reports, and then we performed an analysis of the extracted information. The following sections discuss these steps in detail.

Data Collection: The RISKS forum covers a wide rage of issues related to computer related risks. These include system failure reports, conference announcement, book reviews, etc. The collection of

useful infrastructure failure reports from the huge volume of RISKS forum data (we scanned more then 10,000 records) was the most difficult but important step. During our selection process, we selected only those reports where the failure originated from CITI and affected other critical infrastructures (including CITI); or the failure originated from some other critical infrastructure and affected CITI. Failure is defined as the inability of a system or component to perform its required functions within the specified performance requirements [16]. Failure may be the result of one or many faults. Fault is a defect in a hardware device or component; or an incorrect step, process or data definition in a computer program [16]. In our study, failure is attributed to critical infrastructures. The following infrastructures are considered as critical infrastructures based on a US Congress document [1] on critical infrastructures identification:

- IT Infrastructure
- Telecommunication Infrastructure
- Water Supply
- Electrical Power System
- Oil and Gas
- Road Transportation
- Railway Transportation
- Air Transportation
- Banking and Financial Services
- Public Safety Services
- Healthcare System
- Administration and Public Services

We collected a unique report for each incidence. However, in cases of wide spread failure, we collected unique reports from different affected sites. One example of such wide spread failure is an Internet wide worm attack. The apparent simple task of selecting appropriate sets of reports became quite complicated due to the subtleties associated with each of the reports. The following three examples explain this intricacy. A selected report was as follows:

> *On November 19, 1994, Iowa City's US West telephone system shut down at about 3:30 p.m., local time, and service was gradually restored between 7:30 and 9:30 p.m, affecting about 60,000 people. Analysis showed that a new switching system had been installed in July 1994. In removing the old system, an electrical grounding cable had been inadvertently removed. Iowa City Press Citizen, November 22, 1994, RISKS (16, 58)*

The above example clearly shows that a fault in the electrical power system due to human error caused a failure in the telecommunications infrastructure. The report has a clear reference to a newspaper source. In contrast to the above report, the following is an example of a report that was not selected:

> *I suppose I shouldn't be surprised, but the power went out for 17,000 here in our small town (38,000) last week. The local newspaper first reported that the power company didn't know why it went out, but that it "may be related to someone digging in their back yard". A week later they fixed the blame. A phone call (by the power company), supposedly to one substation, (completely automated judging by the tone of the article) went instead to a different substation (for unexplained reasons) and shut that substation down. It was down for 1.5 hours. Make a Call, Turn Off the Power, RISKS (17, 4)*

In the above report, the failure in the electrical power system is not clearly related to CITI. There is no clear reference to where it happened and there is an undefined term 17000 in the report. Similarly, we have avoided survey reports, as they are not attributed to any particular failure case. The following is an example:

> *The Federal Trade Commission says that complaints of Internet-related identity theft more than tripled last year, to 2,352 last year from the year before. Jay Foley of the Identity Theft Resource Center says, "Online fraud is becoming as big an issue for eBay and AOL as security is for Microsoft." Typically, eBay covers buyers or sellers for up to $200 (or $500 for some listings) if an item is not delivered or is in bad condition, though there is a $25 processing fee. USA Today, 24 Oct 2003; RISKS (22, 98)*

Fault Classification: Our next step was to categorize collected reports based on the nature of the failure. As explained, we used eight fault classes, most of which were derived from the taxonomies proposed by Kuhn [4]. The major advantage of Kuhn's approach is that the failure sources are orthogonal and as such, they can be dealt with independently. A similar approach for software defect classification was studied by Chillarege [19]. For instance, risk of hardware faults can be minimized using redundant physical channel, redundant backup power supply, etc. [17], which is independent of other types of fault consideration. Similarly, for malicious logic fault, different kinds of protection techniques can be used. These include secure routing protocols, secure domain name systems, firewall and anti virus tools [13]. Sometimes failure management can be infrastructure dependent and more specialized tools and techniques are required. For instance, air transportation services require specialized hardware and software tools for their systems' reliability [18]. Table 1 shows the different fault classes used in our study.

Faults that trigger infrastructure failure can be mapped to different Generic Fault Types. These generic faults belong to one of the eight fault classes mentioned above. As we analyzed failure cases and

identified the root cause of each failure, we tried to identify some generic fault source for each of these root causes. These generic fault sources are similar to Kuhn's decomposition of fault classes into finer detail, such as, failure of cable component, power supplies, software version mismatch, etc. Table 2 lists the generic faults and the fault classes they belong to.

Table 1: Fault classes related to Critical Infrastructures

Fault Name	Description
Hardware Fault	All fault classes that affect hardware.
Software Fault	Fault caused by an error in the software system.
Human Error	Non-deliberate faults introduced by a mistake.
Natural Fault	Physical faults that are caused by natural phenomena without human participation.
Overload	Service demand exceeds the designed system capacity.
Vandalism	Sabotage or other intentional damage.
Malicious Logic Fault	These include trojan horses, logic or timing bombs, viruses, worms, zombies or DoS attack.
Authorization Violation	Attempt by an unauthorized person to access or damage network resources, but does not exclude the possibility of authorized users who are exceeding their rights. This also includes unauthorized sharing of digital contents, like audio, video or software.

Feature Extraction: Once we categorized a failure report to a particular failure class, we extracted key features from each of these reports using a set of key attributes. Sometimes a judgmental approach has been taken. For example, Degree of Impact is a feature that intents to capture the severity of a failure. Reading the failure case, we tried to understand how many people or systems were affected and how that number affected the overall functionality of an organization. The degree of impact assigned to a rating "High" indicates a massive effect on the functionality of CITI and other critical infrastructures. Similarly, ratings of "Medium" and "Low" indicate moderate and low impacts, respectively. Clemen et al [20] show that in the absence of detailed information, a judgmental approach can be followed to predict risk. The following three examples illustrate the assignment of Degree of Impact by subjective judgment.

Degree of Impact - High (Report ID # 5) - *On November 19, 1994, Iowa City's US West telephone system shut down at about 3:30 p.m., local time, and service was gradually restored between 7:30 and 9:30 p.m, affecting about 60,000 people. Analysis showed that a new switching system had been installed in July 1994. In removing the old system, an electrical grounding cable had been inadvertently removed.*

Table 2: Generic Faults related to each Fault Class

Fault Class	Generic Fault
Hardware Fault	Physical link failure.
	Hardware design or implementation flaw.
	Failure due to external operating environment exceeds predefined limit.
	Device failure due to lack of backup power supply.
	Device failure due to lack of proper maintenance.
	Device failure, origin unknown.
Software Fault	System failure due to software glitch.
	Software design or implementation flaw.
	Protocol stack design or implementation flaw.
	System failure due to software configuration or update error.
	System failure due to weak encryption algorithm.
Human Error	System design or implementation flaw.
	Inadequate safety measures.
	Careless mistake.
	Data entry error.
	Lack of proper user training or documentation.
Natural Fault	Natural Calamity.
	Resource allocation problem.
	Resource unusable due to natural cause.
Overload	User request failed due to inadequate system capacity.
Vandalism	Intentional breakage of physical links or devices.
Malicious Logic Fault	System failure due to malicious logic.
	Misguiding using malicious logic.
	System performance degradation due to malicious logic.
Authorization Violation	Unauthorized access by the outsider.
	Access right violation by authorized user.
	Unauthorized use of technology for malicious intension.
	Identity theft through authorization violation.
	Unauthorized capture or sharing of digital contents.

Degree of Impact - Medium (Report ID # 3) - *MCI's inbound Internet gateways were saturated*

during July 1994, resulting in days of delay in delivering e-mail to MCI customers. A fix was considered to be months in the offing.

Degree of Impact - Low (Report ID # 8) - *A software glitch on March 10, 1995, caused Prodigy's e-mail system to send 473 e-mail messages to incorrect recipients and to lose 4,901 other messages. The system had to be shut down for five hours*

For the first report, telephone service of 60,000 people was affected, which was an important consideration to assign it as a high impact case. For the second report, even though email service was delayed; but since there were other means of communication available, it was assumed gateway saturation was a moderate inconvenience for the MCI customers. So, the report was assigned as a medium impact case. For the third report, it seems that after five hours the email service was fixed and misdirected emails were re-dispatched to the recipients. Since people did not check their email very often and the number of recipients was less than 473, we considered this failure modestly affected the users. So, a low degree of impact was assigned.

Another key feature of a failure report is the Report Accuracy, where based on the source type we assigned an accuracy rating on a scale of 10. For each of these reports, the information source was given. If the information was released from an official source and had other supporting references for validation, we assigned 9 or 10 points to it. If it was from an official source, but no further details were given, we assigned 7 or 8 points to it. All newspaper reports have 5 or 6 points. Reports from individuals, which were difficult to verify, were normally given less than 5 points. Higher ratings were given to reports of a particular class if the reports fulfilled most of our additional criteria. For instance, if a newspaper report had most of the information required, such as severity, duration, financial impact, description of fault origin, etc., then it was given 6 points. Otherwise, it was given 5 points. In the future, we would like use this accuracy rating for reliability analysis of the collected cases. Table 3 lists the extracted key features of a failure report and their meanings.

Table 3: Extracted features and their meaning

Feature Name	Meaning
Title	Title of the report. Most often this is the same as the original report.
Date	Date of the failure report.
Country	Country where fault incident originated. For global fault, it is World.
Impact Scale	Size of area affected. It could be an Organization, a City, a Region (a big part of the country), a Country, a Continent, or the whole World
Degree of Impact	Failure impact. Could be High, Medium or Low
Simulation	Indicates if the fault conditions can be simulated within a lab environment using NS2 [21] or a similar network simulator.
Fault Intent	Fault could be Intentional, due to deliberate and malicious attempts by any individual or groups, or Unintentional due to human error or system flaw
Duration	Time from the start of the fault to its full recovery.
Financial Impact	Amount of financial loss in Million USD
Public Safety	Any public safety concern associated with a particular fault incident, such as failure of 911 service, medical emergency service, fire rescue service or police service.
Affected Sites	Number of sites or locations affected by a particular fault incident.
Description	Description of the failure (report text)
Report Source	Reference of the report collected from RISKS forum and referred as RISKS (i, j) where i is the volume number and j is the issue number within the volume.
Report Accuracy	Based on the source type we assign an accuracy rating on a scale of 10.
Fault Class	Fault type is one of the eight types mentioned in Table 1
Generic Fault	A qualitative assessment about the origin of the fault
Source Infrastructure	Is one of the critical infrastructures discussed in Data Collection section.
Affected Infrastructures	Is one of the critical infrastructures discussed in in Data Collection section.
Affected	Description of the industry

Industry Sectors	sectors affected by the failure
Comment	Comments on specific interesting aspects of these faults.

Many of these features intent to capture the extent of the failures, their impact in spatial and temporal dimensions, the effect of these failures on public safety, and the propagation of the failures from CITI to other critical infrastructures and vise versa. Table 4 groups these features into different categories according to the intended use.

Table 4: Features that capture different failure dimensions

Analysis Dimension	Feature Names
Extent of failure	Fault Class, Degree of Impact, Fault Intent, Fault Type
Impact (spatial)	Country, Impact Scale, Affected Sites
Impact (temporal)	Date, Duration
Public safety	Public Safety
Failure propagation	Source Infrastructure, Affected Infrastructures

Data Analysis: Many of the public domain failure reports we collected had missing attributes. For example, duration of a failure and number of sites affected by any such failures was not clearly specified for almost half of the cases. Financial impact of failures is mentioned in less than 10% of the cases. As a result, we could not use concepts like "Customer Minutes" (product of average number of customer affected and average outage duration) as used by Kuhn [4] to measure the severity of failures in PSTN networks. Use of such concepts was possible for FCC report, as each FCC report has to include date, time, failure duration and the number of affected customers [4]. Unlike FCC, however, our failure reports did not have such uniformity and universal impact dimensions. To compensate for this, we used a frequency-based approach to quantify results from the extracted features of the failure database (Section 4). This way, we tried to answer the most likely cause of infrastructure failure, types of localities affected, and the implications on public safety. As mentioned before, due to the absence of clearly specified values for many key attributes, we had to use our own judgment to guess some of the values of these key attributes. Doing so, we were limited by the description of the data. There were no mechanisms for getting further detail.

Failure Database

The collected cases and their extracted features were compiled in a MS Excel database. A sample record from this database is shown below (Figure 1). Each record represents a single row in the MS Excel spreadsheet. The analysis performed on these records is done in another sheet within the same MS Excel file.

5	Ground-cable removal blows Iowa City phone system upgrade			
Date	**Country**	**Impact Scale**	**Deg of Impact**	**Simulation**
11/19/1994	USA	City	High	Unsure
Fault Intent	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	6 hours	Unknown	Yes	Unknown
On November 19, 1994, Iowa City's US West telephone system shut down at about 3:30 p.m., local time, and service was gradually restored between 7:30 and 9:30 p.m, affecting about 60,000 people. Analysis showed that a new switching system had been installed in July 1994. In removing the old system, an electrical grounding cable had been inadvertently removed.				
Report Source	Iowa City Press Citizen, November 22, 1994; see discussion by Douglas W. Jones, RISKS (16, 58)			
Report Accuracy	6			
Fault Class	Human Error			
Generic Fault	Inadequate safety measures.			
Source Infrastructure	Electrical Power System			
Affected Infrastructures	Telecommunications Infrastructure			
Affected Industry Sectors	All kinds of industries in Iowa City			
Comment	Fault in electrical system due to human error.			

***Figure 1**: A Sample Database Record*

Each record in this database has a report ID. A report ID is a sequential number assigned based on the incidence date. Other fields have their own set of valid values. Table 5 summarizes acceptable values for each of these attributes.

Table 5: Legal values for Failure Database

Field Name	Legal Values
Report ID #	A sequential number assigned based on the report's date.
Title	Text String
Date	MM/DD/YYYY
Country	Country Name / World
Impact Scale	Organization / City / Region / Country / Continent / World
Degree of Impact	High / Medium / Low
Simulation	Yes / No / Unsure
Fault Intent	Intentional / Unintentional / Unknown
Fault Class	One of the eight fault class (Table 1)
Generic Fault	Origin of the fault that belongs to one fault class (Table 2)
Duration	# Hour
Financial Impact	# Million USD
Public Safety	Yes / No / Unknown
Affected Sites	# / Unknown
Description	Text String
Report Source	Text String
Report Accuracy	#
Fault Origin	Text String
Source Infrastructure	One of the infrastructure from Data Collection section
Affected Infrastructures	One of the infrastructure from Data Collection section
Affected	Text String

Industry Sectors	
Comment	Text String

Results

We collected 347 cases corresponding to an observation period of 12 years (1994 to 2005). Figure 2 shows that the reporting frequency of infrastructures failure to the RISKS forum changes during this period. The trend is nearly linear, except for the year 2003. The linear increase of CITI and other critical infrastructures failure reports can be inferred to imply that these infrastructures are increasingly becoming more dependent on CITI services. However, the sudden rise of failure cases during 2003 was due to a significant escalation of malicious attacks against IT infrastructure (Figure 7). These included different kinds of worm attacks (Slammer, MSBlaster, Nachi) and DoS attacks. We also observe a significant number of Authorization Violation cases (22 reports) in this year. These included a fake US government organizations showing its presence in the Internet (Report ID# 167), major identity thefts (Report ID# 172, 183), unauthorized digital content sharing (Report ID# 189, 208), change of stock market index using malicious techniques (Report ID# 199), online auction frauds (Report ID# 207), and similar others. The trend was worldwide and was visible in the remote parts of the world (Report ID# 211, 217). One explanation of this large number of failures during this period is that corporate cyber security mechanisms were not mature enough to compete with the power and availability of automated hacking tools.

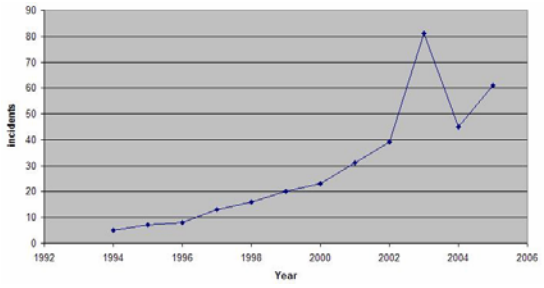

Figure 2: *Reported failures over time.*

Failure by category: Figure 3 shows percentages of failure based on fault classes. One interesting fact from this figure is that software related failures constitute more than 65% of all reported failures (if we include malicious logic and authorization violation within this group). The most common cause of software failure was software glitches (53 cases), with software design or implementation flaws (36 cases) being the next cause. Software glitch is a generic term we used to indicate software failure due to unknown reasons. Most of these cases were related to design or implementation flaws. A high percentage of failures due to software design and implementation defects implies, that better software engineering practices are essential to increase the CITI infrastructure safety and reliability.

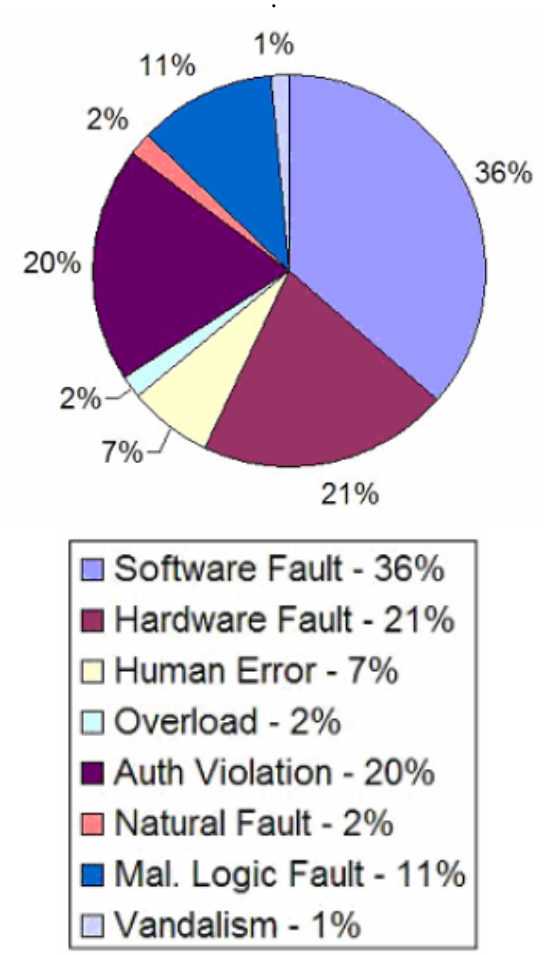

Figure 3: *Faults those lead to infrastructure failure*

Impact of Failure: The failure reports revealed that the root cause of most of the CITI and related infrastructure failures can be attributed to unintentional or accidental causes (Figure 4). Critical Infrastructures are the lifelines of modern societies. As such, even though the root causes may be unintentional, their impact is high (Figure 5). Accidental causes include hardware or software faults, configuration problem, human error, etc. In contrast, malicious logic faults, authorization violation attempts and vandalism account for less than 33% of the cases. This illustrates the subtle fact that system reliability deserves more attention than it is getting now as compared to system security. An example is the air transportation industry. We have 27 air transportation failure cases reported, out of which 26 were due to various non-malicious hardware and software faults of air traffic control system. One such case (Report ID # 83) says:

On 17 Jun 2000, thousands of would-be passengers were stranded when the main air-traffic control computer collapsed. The National Air Traffic Services computer was fixed later in the day, but the resulting congestion caused many people to spend the night at airports around the UK, and many flights were cancelled the next day as well. Heathrow and Gatwick were hardest hit, although other UK airports experienced severe delays. This was the second time in a week that the computer system had failed

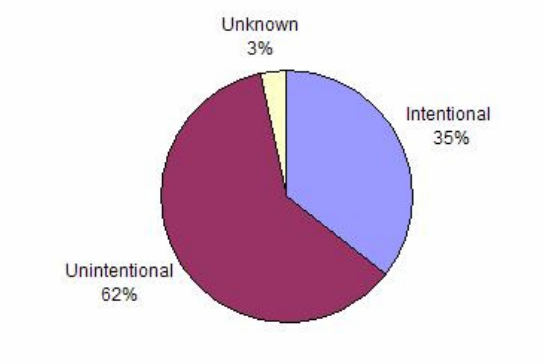

***Figure 4**: Failure type distribution*

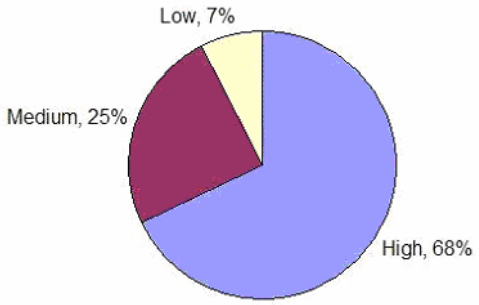

***Figure 5:** Infrastructure failure impact distribution*

Public Safety Concerns: Public safety is a major concern for critical infrastructure failure. Although our study shows that a majority of failure cases do not have public safety implications (Figure 6), we observed that in nearly 20% of the cases the failure affected public safety in some degree. Many times, these failures were due to improper design or set up or public safety related devices, lack of backup power supply, etc. Since infrastructure failures are on the rise, there are increasing concerns for public safety. An example can be given from the 911 systems (Report ID # 230):

Houston has deployed a new 911 emergency response system which has had a number of failures since it went "live" a week ago. Pictures of the new facility look somewhat like Mission Control - large consoles with multiple displays in front of each operator. It sure looks nice, but the system does not appear to work reliably. The latest incident occurred during the day when technicians were working on the link between the computers and units within the cars. To quote: When the system started slowing, technicians reverted to the backup, which crashed within minutes. From 9:50 a.m. to 10:30 a.m., dispatchers resorted to dispatching by radio instead of by computer. Without the computer's locator system, they frequently had to ask emergency workers to volunteer for individual assignments rather than assigning them to calls. Another notable quote is But city officials say the only way to test the system was by going "live."

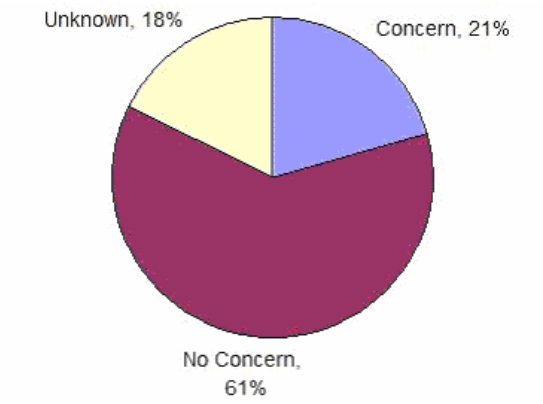

***Figure 6**: Public safety impact distribution.*

Change of Degree of Impact over Time: Figure 7 shows that the frequency of high impact infrastructure failure is on the rise. Figure 8 shows that many of these failures are due to malicious intention. Examples of origin of failure include DoS attack against the Internet infrastructure (Report ID # 156), worm or virus attack (Report # ID 163, 166) and identity theft (Report # ID 172). From 2001 on, failures due to intentional cause are showing a significant rise. This is largely due to the emergence of automated and high-speed worms (e.g., Code Red), the increased deployment of off the self software systems for critical infrastructure management (e.g., MS SQL Server), and an inadequate number of expert manpower to manage more complex interconnected infrastructure systems. The following example shows how health care system can be affected due to its dependency on computerized prescription systems that depended on electrical power systems (Report ID # 186)

Thousands of patients could have received the wrong prescription drugs after a power outage at Kaiser Permanente's computer center in Southern California knocked the pharmacy's labeling system out of sync -- printing the wrong labels on filled prescriptions. There were no reports yet of patients suffering from adverse reactions. About 4,700 patients from Fresno to the

Oregon border were affected, including those ordering prescriptions by telephone. After the error was discovered on 14 Mar 2003, hospital officials attempted to contact the affected patients, although by 17 Mar, 152 remained uncontacted -- including those for whom they had only PO-box addresses.

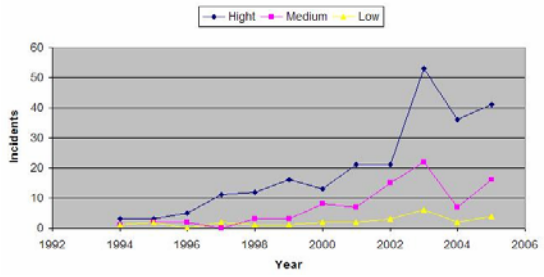

Figure 7: *Change of degree of impact over time*

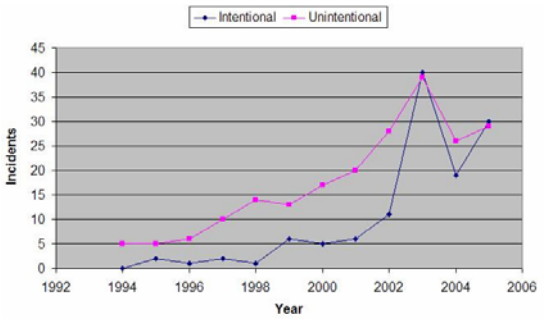

Figure 8*: Change of intentional and unintentional failure over time.*

Localities affected by CITI Failures: Figure 9 shows that almost half of the CITI and connected infrastructure failures propagate beyond organization boundaries (47%). Crossing the national boundary is relatively rare, unless an attack is targeted internationally. Figure 10 shows that North America (US/Canada) is the most vulnerable region for CITI infrastructure failure (63%). One possible explanation is that this region has a much higher proportion of computer uses than any other parts in the world. Figure 10 (left) includes worldwide failure cases (e.g., worm attack); whereas the figure on the right excludes those cases. In both figures most of the reported failures (above 60%) have taken place in North America (US/Canada). Inclusion or exclusion of worldwide failure does not change this pattern much.

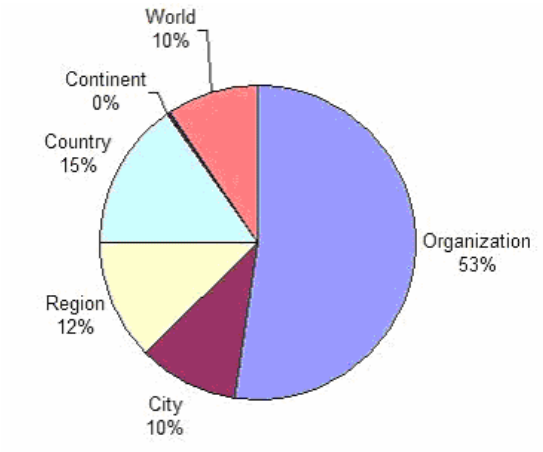

Figure 9*: Localities affected by infrastructure failures.*

Figure 10*: Failure location US and Canada*

Interdependencies between CITI and other infrastructures: Figure 11 shows that in most of the cases CITI failures originate from within the CITI infrastructure. The role of failures from other infrastructures was relatively minor. Figure 12 shows that most of the CITI failures affect the banking and finance services, the administration of public services, and the CITI infrastructure itself. A considerable part of the chart is also taken on by the general grouping of "all other individual infrastructures", indicating the wide reach of CITI failure problems. Since most of the CITI failure originates within CITI, improved techniques in CITI infrastructure design, implementation and management can ensure a greater stability in the operation of all connected infrastructures.

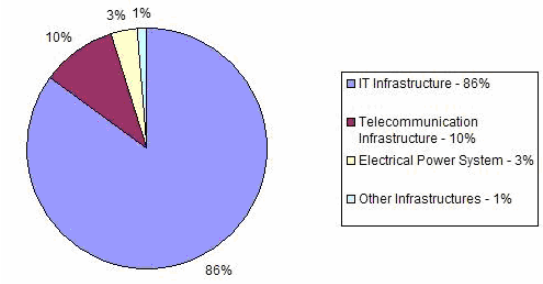

Figure 11: *Failure source those affect CITI.*

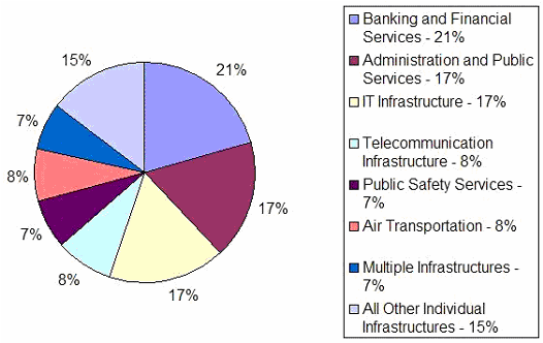

Figure 12: *Infrastructures affected due to CITI failures.*

Conclusions

Survival in our society relies on continued services from interdependent critical infrastructures. CITI failures are particularly pervasive in their penetration of all infrastructures and can have a very large impact in the workings of this fabric of society. Understanding and classifying patterns of CITI failures is an important step towards quantifying risk analyses in CITI-dependent infrastructure systems and identifying preparedness and mitigation strategies to ameliorate the impact of system-wide failures. In this research, we have used public domain data over a considerable time span (12 years) to understand CITI interdependencies. To our knowledge, this is the first attempt of this type of analysis in this area (using either public or privately owned data sources). In the analysis, we identified patterns for the origin of infrastructure failures, their propagation, their impacts on public life, and their historical trends. We have developed a CITI failure database that will be very useful for our Infrastructures Interdependencies Coordination (I2C) research group at UBC to set up realistic test case scenarios involving CITI failures during large-scale system failure situations involving multiple infrastructure interdependencies [22, 23].

Acknowledgements

The work presented in this paper is part of the effort currently in progress at the University of British Columbia, Canada, to better understand infrastructure interdependencies and their effects during large disasters. This work is being sponsored by the Joint Infrastructures Interdependencies Research Program (JIIRP) [3] of the Government of Canada. The UBC Infrastructures Interdependencies Coordination group (I2C) includes fourteen researchers from a number of disciplines in engineering, computer science, commerce, and psychology. CITI interdependencies are an important concern of this group.

References

[1] Critical Infrastructure and Key Assets: Definition and Identification
http://www.fas.org/sgp/crs/RL32631.pdf

[2] Executive Order on Critical Infrastructure Protection
http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html

[3] Joint Infrastructure Interdependencies Research Program (JIIRP)
http://www.nserc.ca/programs/jiirp_e.htm

[4] D. R. Kuhn, ”Sources of failure in the public switched telephone network,” IEEE Computer, v 30, n 4, April 1997, p 31-36

[5] FCC Network Outage Reporting System - User Manual
http://www.fcc.gov/oet/outage/nors_manual.pdf

[6] Eugene H. Spafford, Congressional Testimony, 10 October 2001http://www.house.gov/science/full /oct10/spafford.htm

[7] The RISKS Forum: http://catless.ncl.ac.uk/Risks

[8] Baruch Fischhoff, Paul Slovic, Sarah Lichtenstein,” Lay Foibles and Expert Fables in Judgments about Risk”, The American Statistician, Vol. 36, No. 3, Part 2: Proceedings of the Sixth Symposium on Statistics and the Environment. (Aug., 1982), pp. 240-255.

[9] Gene Rowe, George Wright, ”Differences in Expert and Lay Judgments of Risk: Myth or Reality?”, Risk Analysis, Volume 21, Number 2, April 2001, pp. 341-356

[10] Peter G. Neumann, Computer-Related Risks, Addison-Wesley Professional, October 18, 1994, ISBN: 020155805X

[11] John D. Howard,”An analysis of security incidents on the Internet 1989-1995”, Ph.D. Thesis, Carnegie Mellon University, 1997

[12] John D. Howard, Thomas A. Longstaff, ”A Common Language for Computer Security Incidents”, Sandia National Laboratories techinical report SAND98-8997, 1998.

[13] Anirban Chakrabarti, G. Manimaran,”Internet infrastructure security: A Taxonomy”, IEEE Network, v 16, n 6,Nov-Dec, 2002, p13-21

[14] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, ”Basic Concepts and Taxonomy of Dependable and Secure Computing”, IEEE Transactions on Dependable and Secure Computing, v 1, n 1, Jan 2004, p 11-33

[15] Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kelly,”Identifying, understanding, and analyzing critical infrastructure interdependencies”, IEEE Control Systems Magazine, v 21, n 6, December, 2001, p 11-25

[16] IEEE Standard Glossary of Software Engineering Terminology. IEEE Standard 610.12-1990, 1990

[17] Edward E. Balkovich, Robert H. Anderson, ”Critical Infrastructures Will Remain Vulnerable: Neighbourhoods Must Fend for Themselves”, International Journal of Critical Infrastructures, 2004 - Vol. 1, No.1 p. 8 - 19

[18] Barry Kirwan, ”The role of the controller in the accelerating industry of air traffic management”, Safety Science, v 37, n 2-3, 2001, p 151-185

[19] Ram Chillarege, Inderpal S. Bhandari, Jarir K. Chaar, Michael J. Halliday, Diane S. Moebus, Bonnie K. Ray, Man-Yuen Wong, "Orthogonal Defect Classification - A Concept for In-Process Measurements", IEEE Transactions on Software Engineering, Vol 18, No. 11, Nov 1992

[20] Robert T. Clemen, Gregory W. Fischer, Robert L. Winkler, "Assessing dependence: some experimental results", Management Science, v 46, n 8, Aug 2000, p 1100-1115

[21] NS2 - Network Simulator http://www.isi.edu/nsnam/ns/

[22] J.R. Martí, J.A. Hollman, C. Ventura, J. Jatskevich, "Design for Survival. Real-Time Infrastructures Coordination," Proceedings of the International Workshop on Complex Network and Infrastructure Protection CNIP 2006, Rome, Italy, March 28-29, 2006.

[23] J.A. Hollman, J.R. Martí, J. Jatskevich, K.D. Srivastava, "Dynamic Islanding of Critical Infrastructures, a Suitable Strategy to Survive and Mitigate Critical Events," To appear in Special Issue of the International Journal of Critical Infrastructures (IJCI).