The Cyber and Critical Infrastructures Nexus: Interdependencies, Dependencies and Their Impacts on Public Services
December 27, 2017
Rae Zimmerman (rae.zimmerman@nyu.edu)

I. Introduction

Background

Critical infrastructures (CI) provide fundamental services in ways that are essential to the social and economic fabric of society. These infrastructures are apparently becoming increasingly interconnected with one another (Saidi et al. 2018: 1), and these interconnections appear in the form of interdependencies and dependencies.[1] Information technologies or information and communications technologies (ICT)[2] are often a major location point for that interconnectivity and have been increasingly so for some CI sectors, not only within single infrastructure sectors, subsectors, or subsector components, but also among different infrastructure sectors. When ICTs are disabled either intentionally or unintentionally, the impact can potentially be extensive given the capacity for ripple effects beyond the initial systems disrupted. The extent of damage often depends on the particular characteristics of the infrastructure, the threat, and environmental or contextual considerations. Important threats and environmental or contextual factors include extreme weather events and attributes of climate change. These are increasing (NOAA 2017; Walsh et al. 2014) often targeting infrastructure in particular. The U.S. DOE (2017: S-12) for example points out that the main cause of electric power outages is extreme weather and earlier studies analyzed weather as a factor as well (Simonoff, Zimmerman, and Restrepo 2007). Climate change is increasingly being studied as a contributor to extreme events (National Academies 2016). Similarly, government assessments and the financial support for infrastructure following extreme weather events also address the effects of these extreme conditions upon transportation, water and wastewater, and communications infrastructure. Given the dependency of society on such systems and increasingly so, the impacts of extreme events are often transmitted through infrastructure services. Thus, extreme events both intentional (e.g., terrorism) and unintentional (weather and geological activity) provide a lens through which CI-ICT linkages and their impacts can be understood.

[1] The term interconnectivity is used here as a broader term to encompass interdependencies and dependencies. Both interdependencies and dependencies are defined and addressed in Section II.

[2] The term information and communications technology used here encompasses information technology as well. "Information technology (IT) is the application of computers to store, study, retrieve, transmit and manipulate data [footnote 1: citing Daintith (2009)] "or information, often in the context of a business or other enterprise" [footnote 2: citing the FOLDOC computing dictionary, foldoc.org]. "IT is considered a subset of information and communications technology (ICT)" (Wikipedia December 1, 2017). "Information and communications technology (ICT) is an another/extensional term for information technology (IT) which stresses the role of unified communications[footnote 1: citing Murray 12/18/2011] and the integration of telecommunications (telephone lines and wireless signals), computers as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information.[footnote 2: citing the FOLDOC computing dictionary, foldoc.org 9/19/08]" (Wikipedia December 26, 2017).

Several issues related to these interconnections are examined along with their implications for infrastructure policy. One issue pertains to the way interconnections among CIs are configured and how the introduction of ICT can influence those relationships. A second issue is that under conditions of infrastructure disruptions, interconnections in the form of dependencies and interdependencies among infrastructures could result in longer recovery times than if the infrastructure was isolated. A potential implication of longer recovery times is greater damage and human impact. If these interconnections are increasing, the negative implications for recovery increase as well unless mitigating actions are undertaken. A third issue (related to the second issue) is that where information technologies are a key aspect of the interconnections among CI that are already interdependent, the recovery time from intentional or unintentional disruptions could increase if they are unexpected and not planned for. Recovery is one aspect of the impact of disruptions and infrastructure resilience. Definitions that expand upon the recovery concept and its relationship to resilience have been extensively coverage elsewhere, for example in terms of what state and level of service is aimed for and the distributional aspects of benefits and costs of different levels of recovery (see for example Zimmerman 2016 for a summary of some recovery and resilience literature related to infrastructure). Prior to introducing the concept of recovery, the major portion of the paper is devoted to analyzing the structures and other characteristics of CI interconnections with and without ICT.

Scope

The themes outlined below address the objective of characterizing the interconnections of ICT to CI in terms of interdependencies and dependencies. The focus is on a set of about a half dozen "lifeline" infrastructures in the energy, transportation, communications, and water and wastewater sectors.[3] It should be recognized, however, that sectors other than lifelines interact with and are interdependent with lifelines, including those that provide inputs to lifelines and to which the lifeline sectors produce outputs. For example, manufacturing both provides inputs and is the recipient of outputs connected with lifeline sectors. The chemical and metals sectors do likewise.

The first four sections address interconnectivity characteristics and sections five through eight address impacts of interconnections.

Section I. ICT and CI connectivity issues are presented in the introduction above.
Section II. CI interconnectivity separate from ICT is first described and illustrated based on selected case literature as a foundation for a framework that introduces ICT connections to CI.

[3] Critical infrastructures (CI) have been categorized in a number of different ways. The U.S. Department of Homeland Security lists sixteen different sectors with reference to Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience (The White House February 12, 2013). They define the sectors as those "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." (U.S. DHS July 11, 2017). The lifeline sectors are included in that larger list. Although ICT is a critical infrastructure it is identified separately here for the purposes of analyzing its relationship to the other CI lifeline sectors.

Section III. Overall trends only for ICT deployment are then described primarily in terms of time trends as a context for the CI and ICT connections in Section IV.
Section IV. Interconnections between ICT and CI are presented based on analyses of some databases for selected lifeline infrastructures, primarily transportation and energy.
Section V. Impacts of interconnections among CI only are illustrated from case literature.
Section VI. Selected non-cyber attack impacts of ICT connections to CI are introduced associated with interconnections.
Section VII. The extent of cyber attacks as a type of impact is presented for a few data sources, and cases of ICT-CI interconnections follow to illustrate relationships of cyber attacks and interconnections.
Section VIII. Implications of interconnections and their impacts are illustrated for resiliency in terms of recovery time.
Section IX. Conclusions and policy implications are provided.

Ways of adapting to the threats are suggested from the analyses presented in terms of infrastructure management, for example, through design, planning, operations and detection technology including improved software and hardware fixes to prevent the adverse effects of the ICT-CI interface. The methodology and approach for the overall analyses are based upon databases and cases from publicly available information sources. Case databases are tabulated to construct data sets of typical cyber-CI failures and their characteristics, and where available, to identify successful solutions to reduce the threats.

II. CI Interdependencies and Dependencies

That infrastructures are interconnected with one another in the form of interdependencies and dependencies is reflected in a growing literature in this area. The literature generally points to the existence of such linkages and their increased diversity or variation, degree of concentration, and extent of interconnectedness. The means by which these insights have emerged include compilations of historical records and modeling of mechanisms to understand the structure of these linkages. Rinaldi, Peerenboom and Kelly (2001) and Petit et al. (2014) provided examples and typologies of ways in which infrastructures are related to one another at functional and spatial levels and flows among various sectors. Modeling approaches for interdependencies are very diverse (Ouyang 2014; Saidi et al. 2018; Varga and Harris 2015). Network models have been used as the basis for understanding these relationships (Ouyang 2014; Zimmerman 2014a; Zimmerman, Zhu and Dimitri 2017). Some models actually work at the component level of infrastructures (Verner, Petit, Kim 2017; U.S. DOE 2017; Varga and Harris 2015). Conceptual models have been developed to portray CI interconnections in a variety of settings for example for food systems (Zimmerman, Zhu and Dimitri 2016) and under conditions of extreme events (Zimmerman, Zhu, de Leon and Guo 2017).

Specific infrastructure sector dependencies and interdependencies have been highlighted in a number of government studies and are now imbedded in the U.S. DHS sector specific infrastructure plans. For example, in the water sector a sample of water purveyors conducted by the National Infrastructure Advisory Council (NIAC) (2016: 19) identified levels of impacts

based on self-assessments from the purveyors (results only lifeline sectors in this paper are cited) shown in Table 1.

Table 1 Assessment of Impacts of Water on Selected Infrastructure Lifeline Sectors

1. Lifeline Sector Reported as Dependent on Water	2. Percent of entities surveyed reporting dependency on sector given in column 1	3. Hours after impact (degrada-tion) felt	4. % of functions degraded (after hrs in column 3)
Transportation	88	8	34-66%
Wastewater Treatment	61	5	1-33
Electricity Generation	82	4	67-99

Source: Extracted and summarized from NIAC 2016, p. 19. The basis is a NIAC voluntary survey of 2,661 facilities (January 2011 to April 2014). Details are contained in the NIAC 2016 report.

During and following extreme events, water supply systems are often cited as being impaired due to a dependency on other systems, which in turn are dependent upon water supply.

III. Overall Trends in and Characteristics of ICT Use

Irrespective of ICT and CI connectivity, ICT activity and the reliance on ICT is in general occurring dramatically. Two indicators are used to illustrate these trends: Overall connection to the internet and the increased use of ICT products that support ICT connectivity.

Internet Connectivity

The "Internet of Things" (IoT) (Ashton 2009) popularized the notion of interconnected systems via information technology, in particular the internet. The U.S. DOE (2017: 1-10) has defined IoT as follows (citing Chiu, Loffler and Roberts 2010): ""The IoT is defined as "sensors and actuators embedded in physical objects—from roadways to pacemakers— [that] are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet."" Trends in ICT usage have been expressed in terms of internet use. For example, Gartner Inc. (February 7, 2017) estimated 8.38 billion interconnections in 2017 compared to the 2016 level of 6.38 billion, and estimated an increase to 11.2 billion in 2018 and 20.42 billion in 2020, valued at $2 trillion by 2020. This translates into about a 30-34 percent average increase per year from 2016 to 2018, which increases to an average of over 40% per year by 2020. While Gartner Inc. attributes the 2017 level to industry usage (including electric power) they indicate later uses are expected to be for building technologies that are indirectly connected to infrastructure. The FTC has also provided some insights into the interconnections. The U.S. DOE (2017: 1-10, quoting Federal Trade Commission (FTC) 2015) notes even higher connections: ""Six years ago, for the first time, the number of 'things' connected to the [global] Internet surpassed the number of people…Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion."" Other statistics are given by the U.S.DOE (2017: 1-10) that pertain primarily to usage of ICT by households and businesses.

ICT products

In addition to the internet itself, ICT enabling technologies are clearly increasing and supporting ICT connections to CI. Wireless technologies in particular cell phones are one of the backbones of such enabling technologies. CTIA notes the dramatic rise in cell sites that are pervasive in CI, and between 1986 and 2016 CTIA reported that the number of users ("wireless subscribers") increased from about 681,825 to 395,881,427 connections (CTIA 2017: 2) while the number of cell sites that send and receive signals to wireless equipment increased from 1,531 to 308,334 during that same period (CTIA 2017: 4). If one assumes that all of the subscribers are distributed across all of the cell sites, then the density of cell sites is also increasing. The number of cell units per site increased dramatically during an earlier period (Zimmerman 2012). Whether ICT is increasing or not in all CI sectors is difficult to assess, but in certain CI sectors it is clearly apparent, illustrated in Section IV.

ICT products including mobile wireless phones are increasing in diversity. Hilbert and Lopez (2011: 61) note for example the dramatic increase in storage capacity for information between 1986 and 2007 accompanied by substantial changes in the form of that storage from PC hard disks accounting for 5% in 2000 to 42% in 2007. Telecommunication they note for mobile phones alone accounted for only 1% in 1993 and increased to 97% by about 2005 (Hilbert and Lopez 2011: Figure 4).

These changes or trends have a number of effects. They can lead to unexpected and often uncertain routes by which connections are manifested. With respect to ICT, it can be difficult for ICT connections to adapt to infrastructure configurations in a comprehensive, consistent and timely way, given the speed of changes in the technology.

IV. ICT and CI Connection Characteristics and Trends

CI and ICT interconnections are increasing across many CI sectors, though CI specific ICT usage information is not easily obtained. The broader view of connectivity with the internet, computers and ICT in general previously described provides a good context to identify this.

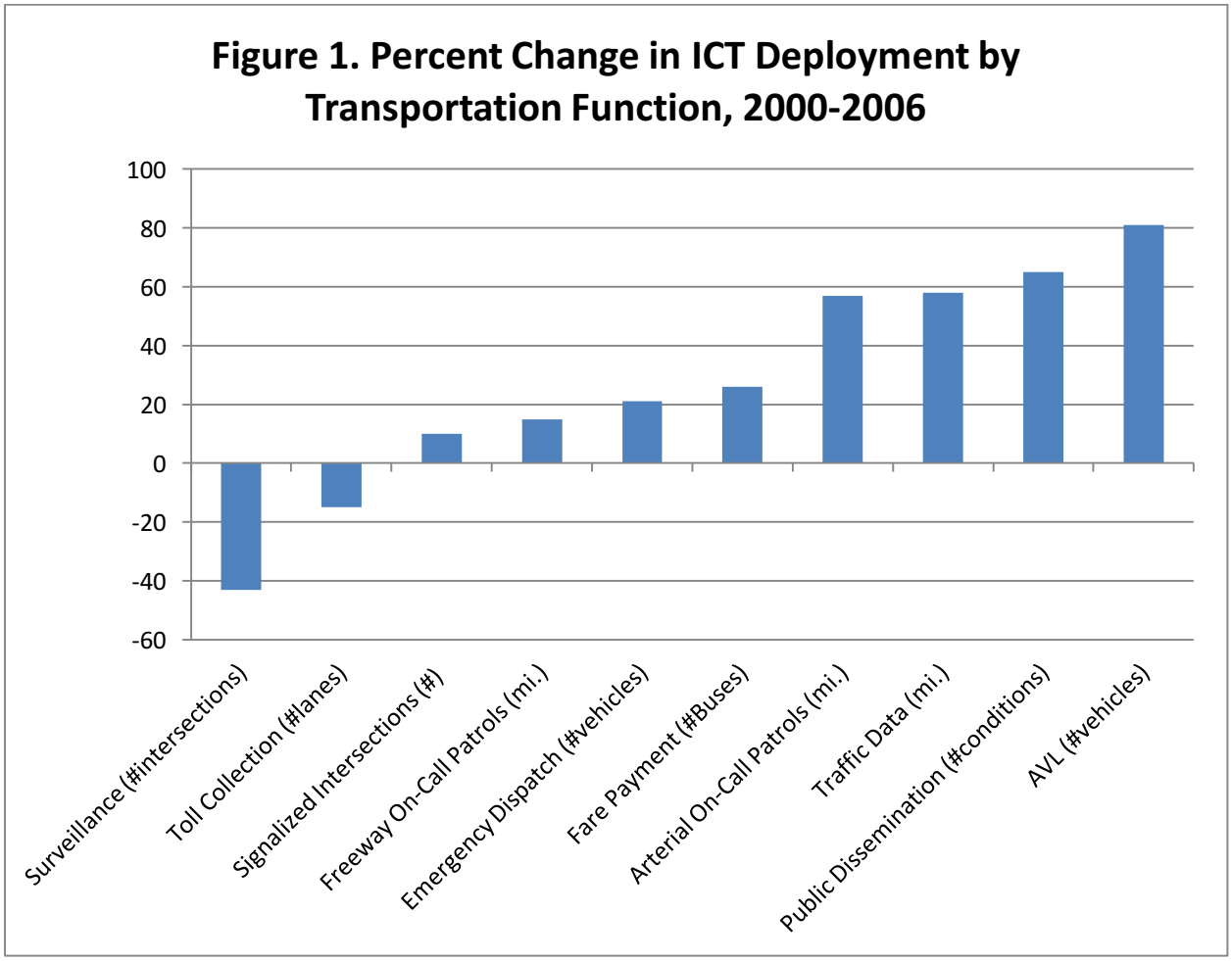
A number of phenomena are converging that provide benefits of ICT for CI yet potentially compromise the integrity of CI, given the trends described above namely increasing diversity, concentration and interconnectedness of infrastructures, increased use of ICT overall, and the dramatic transformation of ICT products. Specific patterns and trends for ICT deployment in CI illustrate these connections. Transportation and energy are used for illustrations and analyses.

Transportation

For *transportation infrastructure*, the U.S. DOT has surveyed ICT use across many functions that support road and rail travel noting that the use of IT has clearly increased across the following functions tracked for ICT deployment from 1997 through 2006 (U.S. DOT 2008: 2-18):

- “Freeway Miles with Real-time Traffic Data Collection Technologies
- Freeway Miles Covered by On-call Service Patrols
- Arterial Miles Covered by On-call Service Patrols
- Signalized Intersections Under Centralized or Closed Loop Control
- Toll Collection Lanes with Electronic Toll Collection Capability
- Fixed-route Transit Vehicles Equipped with Automatic Vehicle Location [AVL]
- Fixed-route Buses Accepting Electronic Fare Payment
- Highway-Rail Intersections Under Electronic Surveillance
- Emergency Management Vehicles Under Computer-Aided Dispatch
- Freeway Conditions Disseminated to the Public”

These functions varied considerably in the percentage ICT deployment in each of these functional areas over the time period as shown in the Figure 1 below.



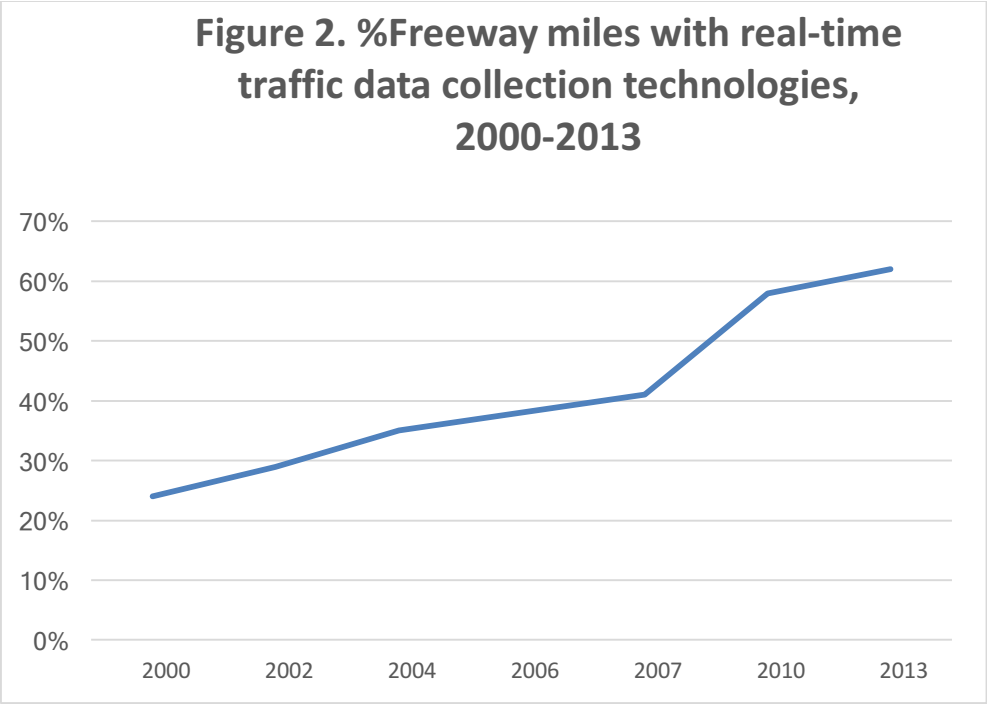
Source: Computed from data provided in U.S. DOT (2008: 2-18), and organized according to increasing level of deployment.

Time trend analyses presented in this section have the caveat that the number and percentage of reporting entities often varied over different time periods in the U.S. DOT surveys.

In its survey of 78 large metropolitan areas in 2008, the U.S. DOT (2008) noted that:

- The percent deployment of ICT in each category the U.S. DOT surveyed increased between 1997 and 2006.
- The leading transportation sectors for IT use were electronic toll collection and the dispatch of emergency vehicles which in 2006 showed over 80% use of IT which was about a doubling over the 1997 levels.
- The electronic fare collection on fixed route buses and certain types of signalized intersections ranked third and fourth in ICT deployment with 63% and 54% respectively, and the reliance of fare collection systems on ICT in 2006 more than doubled what it was in 1997.

The U.S. DOT continued the ICT deployment survey in 2010 and 2013. The U.S. DOT, however, particularly notes that reporting was much lower in the 2013 than in the 2010 survey, which they attribute to staffing problems that arose (U.S. DOT 2014: xi). Some standardization is done by reporting and comparing shares rather than absolute numbers. Among the notable findings was the intent of most agencies to continue ICT deployment in terms of expanding their current systems and investing in new ICT in 2010 (U.S. DOT 2011: 1-2) and again in 2013 (U.S. DOT 2014: 2) for road transportation as well as transit. Figure 2 was computed using the U.S. DOT data, and shows the change in time over one of the functions reported over the entire 1997-2013 time period, Freeway Miles with Real-time Traffic Data Collection Technologies, to illustrate the increasing deployment of ICT in the transportation sector.



Source: Computed from data provided in U.S. DOT (2008, 2011, and 2014).

The reliance of emergency services on ICT was particularly notable with such service reliance focused in the areas of navigation, vehicle deployment or dispatch, vehicle locating and communication including traffic signal preemption among emergency response agencies in 2010 (U.S. DOT 2011: 41-42) with continued interest in 2013 (U.S. DOT 2014: 33-34), however transportation agencies other than those specializing in emergency services reported using ICT for emergency functions as well.

Social media was cited as a particularly large area of growth in ICT use in transportation especially in the period from 2010 to 2013 often supplanting the growth of other ICT systems especially among freeway agencies (U.S. DOT 2014: 17). Social media has been cited by Symantec (2017: 61, 66, 73) as a potential route for certain types of cyber attacks.

In summary many early ICT deployment examples in the area of road infrastructure seem to concentrate on user interfaces.

The *automotive sector* as distinct from road infrastructure gradually introduced ICT connections for the operation of road vehicles in addition to trends in the introduction of ICT in road infrastructure discussed above. Automation has been introduced in many areas in automobiles incorporating ICT, and the nature and extent of deployment has changed over time with the introduction of new technologies and strategies. Control functions include safety features such as air bags and braking systems, measurement such as tire pressure gages, operational systems like navigation and steering systems, timing of windshield wiper speed to rainfall intensity, and diagnostics (Dawson 2017). Many of these computerized functions and the potential for intrusions were summarized by Zimmerman (2012). Many of these computerized systems, however, are decentralized in the sense that they perform single functions and are unconnected to one another. Some systems however such as diagnostics and external communications are connected with other systems and are potential sources of intrusion. Records are increasingly being reported in terms of the capabilities of such vehicles and their ICT deployment (Hook and Waters November 10, 2017). The automotive sector may be increasingly dependent on ICT with the introduction of newer technologies such as autonomous, driverless or self-driving vehicles (Litman 2017: 3) apparently using, however, more centralized ICT than the computer systems introduced in more conventional vehicles described above. The controls tend to be more centralized for example through computer area networks (“CANS”) in spite of the installation of gateways which is considered by some to contribute to vulnerability to cyber attacks (Perlroth June 7 2017).

Energy

The energy sector has had a long history of the deployment of ICT. The trends have increased as well as being transformed, as products have evolved and the need for security has been introduced.

The U.S. DOE (2017: 1-13) has traced the evolution of ICT deployment over the 20th century into the 21st century noting the introduction of supervisory control and data acquisition (SCADA)

systems in the early part of the 20th century aimed at providing 24/7 coverage and at the same time workforce reduction. Inter-utility interconnections expanded the use of ICT to connect utilities to one another and also monitor the flow of electricity, and provided management with increased capabilities with the introduction of analog computer systems in the middle of the 20th century (U.S. DOE 2017: 1-13). The U.S. DOE (2017: 1-9) underscores the increasing dependency of the electric power grid upon ICT and this dependency they indicate occurs across the entire electricity system. The economies of scale this technological integration supported were considered a contributing factor to the increasing interconnectivity of the two sectors (U.S. DOE 2017: 1-13). Moreover, interconnections across sectors within the energy system, for example, electric power and gas systems are enabled by ICT.

V. Impacts: Cases Illustrating Interconnected CI Only (not including ICT Linkages)

The objective of understanding how CI is disabled contributes to an understanding of what components and operational procedures are at risk in one infrastructure system when interacting with components in other systems. This informs infrastructure management.

Numerous cases exist from which such component level interconnections and interactions can be derived. Examples where interactions primarily occurred between electric power and transportation (and other infrastructures) are presented below not including ICT connections or deliberate cyber attacks, which are covered in other sections that follow.

Miles, Jagielo, and Gallagher (2015) studied interactions between electric power outages and other infrastructure failures in connection with Hurricane Isaac. An earlier study addressed the 2011 San Diego outage (Miles, Gallagher, and Huxford 2014). Both studies evaluated restoration time as well as the location of the outages.

During Hurricane Sandy, massive disruptions to rail transit and other transportation and infrastructure services resulted from electric power outages as well as from the physical impact of surge waters (NYS 2100 Commission 2013). These in turn potentially impaired the ability of workers to get to jobs that either directly or indirectly supported the services and supplies for electric power repair, thus translating into an interconnection that is an interdependency.

A Metro-North railway outage occurred September 25 2013 due to a failed 138,000-volt feeder cable, and effects occurred over the MTA Metro-North New Haven line estimated to carry at the time 40,000 passengers per day at rush hour as well as suspending Amtrak trains between New York and Boston over shared track (Flegenheimer 2013). It had been anticipated that the duration of train service outages would last several days though some accounts indicated they would be back the next day. According to MTA (October 5 2013) the full disruption lasted from September 25 to October 7 2013 or 12 days along with train delays from partial service. Contributing to the length of the restoration time was the decision to complete a new substation to provide power rather than repairing the feeder cable. The MTA (October 5 2013) indicated that within the 12 day outage period after which full service was restored partial service was provided through diesel locomotives to haul trains that were originally electric

powered, the use of temporary substations to provide power, and buses and park and ride facilities to access other rail systems.

Transformer explosions resulting in power outages have impaired transit systems for example historically in New York City on July 29, 2001 and power outages have caused closures of San Francisco Bay Area and Chicago transit lines (summarized in Zimmerman 2005: 27-28).

On December 19, 2009 Eurostar trains were halted in the Channel Tunnel (Chunnel) due to a power failure caused by water condensation from a temperature differential between the warmer air in the tunnel and the exterior cold weather temperature where the trains originated; the power outage in turn stopped the trains, interior lighting and ventilation systems; and communication lapses and unavailability also were reported that compounded the problems (Clark 2010; Charlet December 19 2009). Electric power was disabled due to the effects of condensation causing arcing and other problems, and though these problems were in the process of being fixed, not all cars had been retrofitted at the time of the outage (Garnett and Gressier 2010: 23-24).

VI. Impacts: Cases Illustrating ICT and CI interactions

Some cases are introduced here to illustrate the ICT interconnections with CI using disruptions as a context to understand the relationships. The importance of ICT and CI connections is underscored by the fact that when one is a disabling force on the other it costs money, affects social services, and impedes the initial use of the service and in some cases can adversely affect the users' lives, safety and health in the process. The examples below illustrate transportation, electric power and ICT interconnections often simultaneously.

In 2017 a string of at least a half dozen mass transit stoppages in NYC occurred attributed to power outages (NYS Office of the Governor 2017). In order to manage the electric power, Con Edison installed smart meters in NYC subway stations, thus connecting ICT to both rail transit and electric power infrastructure (Con Edison 2017).

On September 29, 2011 a Long Island Railroad computer was struck by lightning and disabled the railroad's train system for quite some time (MTA October 24 2011). According to the MTA web site, the operating system is highly centralized (most trains go through a single station complex), and the system is noted for its very high volume of traffic (81 million annually) which is one of the largest in the country. Passengers have few rail transit alternatives in the area. The computer that was struck was a single computer exposed to external weather conditions. Multiple failures at the same time increased consequences dramatically: the lightning strike disabled the computer operating the trains giving false readings, the electrical system west of Jamaica was affected, a programming error affected service, the third rail shut independently from police action to protect passengers, and in all there were 17 trains stranded trains and 9 standing trains (MTA October 24 2011). The MTA used ICT in connecting and communicating with customers to inform them of the conditions and changes, including close to a half dozen different forms of social media: "84 customer email alerts, 80 Tweets, 26 message board

postings, 18 web page updates and 19 Facebook postings" with an additional 50 text messages to the workers (MTA October 24, 2011: 2).

VII. Extent of Cyber Attacks in General and Those Specifically Targeting CI

Some patterns and trends in cyber attacks provide a general context for the extent to which attacks are targeting CI. Relatively little systematic data seems to focus on cyber attacks on CI.

The extent of and trends in cyber attacks in general is tracked in a number of ways (Symantec 2017; McAfee 2014; others): as number of attacks also referred to as targeted attack incidents, attack vectors, attack purposes, extent of destruction, and monetary losses. Insurance losses are estimated by insurance providers such as Swiss Re (2017). Trends in a couple of these – insurance costs and events - are noted below.

The Extent of Losses from ICT and Cyber Interactions

Estimates of losses associated with cyber attacks reported by the insurance industry are in the many billions of dollars and probably more when second and third order effects are taken into account (Romanosky 2016; Gandel 2015; Swiss Re 2017). Swiss Re (2017: 3, footnote 7 citing McAfee 2014) captured the cost of cyber-related attacks as follows: "The McAfee study assumed the cost of cyber crime as a constant share of national income, adjusted for levels of development. It used available national estimates to extrapolate a range of estimates for cyber crime costs from USD 375 billion to USD 575 billion. This includes both direct and indirect costs, loss of intellectual property, theft of financial assets and sensitive business information, opportunity costs, additional costs for securing networks, and the cost of recovering from cyber attacks, including reputational damage."

Swiss Re notes that: "A recent Swiss Re/IBM survey found that 40% of companies were affected by a cyber incident in the past three years, and that 60% of all companies expect the risk to increase in the coming years. This was true across all regions and industries and not just in those areas or sectors where cyber attacks have recently been most prominent (eg, retail and healthcare)" (Swiss Re and IBM, October 2016).

In the context of insurance, the Swiss Re survey found that lack of insurance coverage appeared in several critical infrastructure lifeline sectors. Telecom, transportation and utilities indicated that insurance coverage was most missing for uninsured non-malicious failures that caused non-malicious business continuity and physical facility disruptions (Swiss Re and IBM 2016: 15). The prognosis for the insurability of CI attacks is not considered good, according to Swiss Re and IBM (2016: 38): "Ultimately, however, some cyber risks, especially those related to extreme catastrophic loss events such as a disruption to critical infrastructure or networks, may be uninsurable. The ambiguity over the likelihood of a loss event and/or its magnitude together with the potential for significant accumulated losses mean that there are natural limits on the risk absorbing capacity of private insurers and investors."

Events

Some databases are beginning to identify cyber attacks on CI. The extent of cyber attacks are reported at aggregate levels for critical infrastructure sectors, with difficulty disaggregating to specific CI sectors.

Symantec tracked what are referred to as "zero-day vulnerabilities" using the metric "vulnerabilities not discovered by the software's vendor" and noted the following trend which they attribute to increased security:
"2014 4958
2015 4066
2016 3986" (Symantec April 2017: 16)
This represented a decline in vulnerability (as distinct from attacks) between 2014 and 2016 of about 20%.

Others argue that attacks, distinct from vulnerabilities, are apparently becoming more frequent and changing in form not only for cyber but attacks in general on infrastructures. In the latter part of the 20th century and early 21st century Kjaerland (2006) summarized dramatic increases in cyber attacks overall citing Hansman and Hunt(2005) for increases in the number and severity of the attacks and Clarke and Zeichner (2004) who identified 21,000 viruses with costs in the many billions. Symantec (2017) traced trends in cyber attacks across numerous sectors and generally noted the increase though the trends can vary depending on the mode of attack.

Some noteworthy cases of CI intrusions from ICT are provided generally or in an aggregated form by Symantec and ICS-CERT and can be derived from specific incidents from the Repository of Industrial Security Incidents or RISI database. Patterns and trends from the first two databases are summarized followed by an indepth analysis of the RISI database and supplemented by others. The RISI database not only identifies deliberate cyber attacks but also disruptions created by unintentional and intentional computer disruptions not related to cyber attacks. The latter set is valuable for understanding cyber attacks since it points to vulnerabilities and modes of entry for cyber intrusions.

Symantec

Symantec monitors the "Transportation & Public Utilities" combined sector as the only lifeline sector included in its annual reports. However, in the 2016 report, presenting 2015 data, details of the energy sector are given (Symantec 2016: 33, 42). In the Fall of 2017 Symantec noted one attacker particularly targeting energy systems (Symantec Official Blog September 6 2017).

In 2012, Symantec (2013: 15) reported transportation, communications, electric, and gas sectors as the sectors with the lowest number of attacks of the ten sectors they reported accounting for 1% of the attacks. Although the lifeline sector generally ranks lower relative to

other sectors some of the Symantec patterns and trends are noteworthy. For the combined Transportation & Public Utilities lifeline sector, Symantec tracks email spam, phishing, spear phishing, malware, identities exposed, and overall breaches, and found the following:

- Email malware rates were reported as 1 in 176 emails in 2016 (Symantec 2017: 25) which Symantec noted was an increase over the 2015 rate of 1 in 338 (Symantec 2016: 35). Interpreting the relationship to other sectors however requires information about how many emails each of the sectors has, which the reports do not provide.
- The phishing rate for the transportation and public utilities sectors was 1 in 6176 in 2016 Symantec 2017: 26) which is a dramatic decline from the 2015 rate of 1 in 2948 (Symantec 2016: 33).
- Spam was reported as 51.8% of emails in 2015 (Symantec 2016: 32) compared with about the same – 52.9% - in 2016 (Symantec 2017: 28).
- The number and percentage of data breaches in the transportation and public utilities sector increased substantially from 6 incidents (2.0% of incidents in 8 sectors reported) in 2015 (Symantec 2016: 51) to 75 incidents (7.3% of incidents in 10 sectors reported) in 2015 (Symantec 2017: 48).

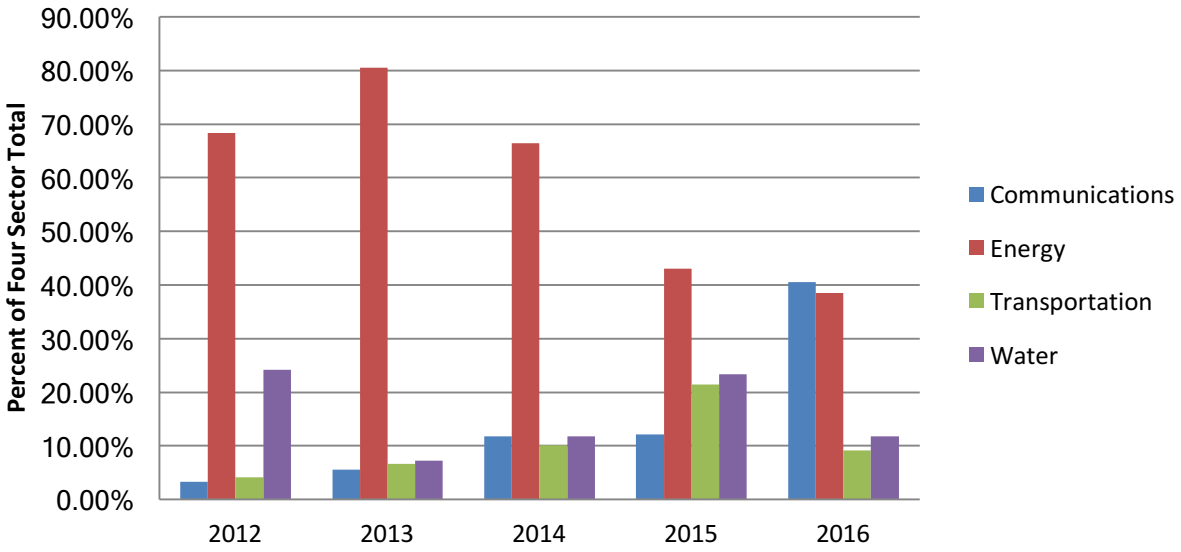
ICS-CERT (2012, 2013, 2014, 2015, 2016)

ICS-CERT monitors cyber intrusions across a wide variety of types of attack and targets. Between 2012 and 2016 ICS-CERT included the lifeline sectors – electric power, transportation, water and communications. These are separated out for analysis here.

Figure 3 shows the percentage share of the total lifeline cyber incidents that each sector accounts for over the five years of record. These findings show that:

Electric power continued to exceed the other sectors in the number of attacks up until the last year, 2016. The share that electric power accounted for across the four sectors had been declining as attacks on communications infrastructure increased over the five year period.

Figure 3. Trends in Relative Shares of Cyber Incidents in Four Lifeline Sectors, 2012-2016



Source: Computed from the ICS-CERT databases from 2012-2016

The Repository of Industrial Security Incidents or RISI database

An incident database collected by the Repository of Industrial Security Incidents over a thirty year period consists of 242 incidents over many different sectors, countries and time periods.

The specific characteristics of the entire database are:

- Dates of events: 1982-2014
- Number of countries: 33 (including an "unknown" and "Europe" categories as well as listing individual countries within Europe separately)
- Number of sectors: 15 (including "other" and "unknown" sectors)

The incidents are described in text form including a general description, impact and action taken though all three of these categories are not consistently used.

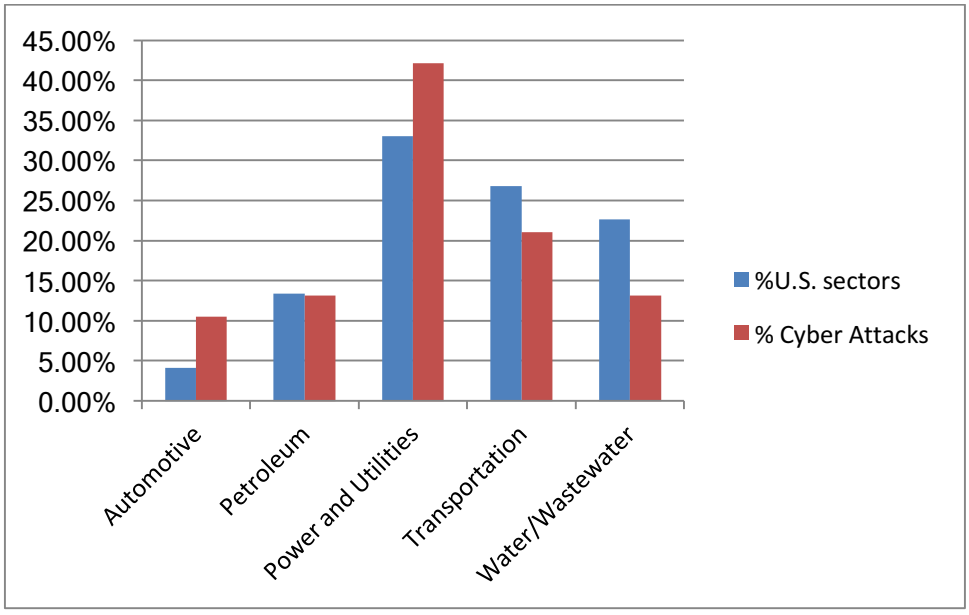
The analysis presented in this paper focuses on five lifeline infrastructures as coded in RISI where the facilities occurred in the U.S.

The U.S. accounts for about half of the events listed in the entire RISI database. Incidents categorized as lifeline sectors – power and utilities, transportation and water/wastewater – account for two thirds of all of the sectors for which incidents are reported in the RISI database internationally. Those sectors for the U.S. incident dataset show that in terms of number of incidents, transportation ranks first, followed closely by power and utilities, then petroleum.

Some analysis of the RISI events has been done in other research. For example, Miller and Rowe (2012) analyzed a subset of incidents involving SCADA systems arguing that a number of circumstances have led to their vulnerability to attack, such as ease of access and the widespread usage.

It is instructive to compare the extent of incidents with respect to those that involved cyber attacks vs. those that didn't. The incidents in the RISI database (RISI 2014; Exida.com LLC 2017) restricted to those that were in the five lifeline categories and only in the U.S. were coded based on the database descriptions for those that had been subject to cyber attacks and those that were not.

Figure 4. Comparison of CI Incidents Not Involving Cyber Attacks and Those Involving Cyber Attacks, RISI database, 1982-2014



Source: Computed from the RISI database 1982-2014. "%U.S. sectors" denotes the percentage of the total of lifeline infrastructures in each lifeline category not subject to cyber attacks. "% cyber attacks" denotes those infrastructures that were subject to attacks.

What is apparent is that the information confirms what other literature has identified about CI alone and CI connected with ICT in the context of an attack. Power and utilities dominate both categories and account for a larger share of the infrastructures subject to attacks than those in that category that were not attacked. Transportation ranks second: cyber attacks are a smaller percentage of the total relative to non-cyber attacks.

VIII. Infrastructure Interconnections and Recovery

Recovery time of critical infrastructures is considered a key factor in the ability of society to withstand the adverse impacts of an infrastructure disruption. Recovery time is a common

indicator of resilience yet it is typically analyzed for single infrastructures and the social and economic systems they support (Zimmerman 2016). Electric power recovery times are a common focus given the dependency of other sectors on it. The Executive Office of the President (2013) normalized duration for electric power outages only across many hurricanes and other storms and estimated that regardless of the destruction most electric power systems recovered in about a quarter of the total duration time of the outage.

The social and economic impacts of outages of even a single infrastructure are believed to propagate over time. The U.S. DOE survey of businesses found that over two thirds of the businesses surveyed felt that negative impacts to their business were felt with the outage duration being an hour or less (U.S. DOE 2017: 1-12).

Non-cyber interconnected infrastructure cases illustrate recovery time for interconnected ICT and CI. Case histories of the recovery of interconnected infrastructures provide important lessons for the contribution of interdependence to recovery. Some of the cases were described in more detail in Section V above and the recovery data are drawn out here and summarized in Table 2 for just a few of them.

Table 2. Recovery times for Electric Power and Rail Transit Connectivity Cases

Event name	Date and Place	Recovery Metric	Values
2003 NE US blackout[1]	8/14/2003 NE U.S., Canada	Multiplier of electric power recovery, e.g. NYC transit signals NYC traffic signals	 1.3 2.6
Eurostar [2]	12/19/2009 Europe	Restoration of train service	3 days
LIRR lightning strike [3]	9/29/2011 Long Island	Resumption of train service (hrs) Normal AM service (hrs)	7.5 hrs 14 hrs
Hurricane Sandy [4]	10/29/2012 NE U.S.	Recovery of rail service	3-12 days
MTA Metro-north high voltage cable [5]	9/25/2013 NY region	Total recovery of rail service	12 days

References:

[1] Zimmerman and Restrepo 2006: 223. Other infrastructures were also affected. Recovery of the Detroit water supply system was 2 times as long and Cleveland water supply 3 times as long as the time for power restoration.

[2] Garnett and Gressler 2010: 59

[3] MTA October 24, 2011: 2

[4] Kaufman et al. 2014; Zimmerman 2014b

[5] MTA October 5, 2013

What is clear from these few examples is the considerable variation in recovery time. Recovery time estimates depend upon a lot of factors. One factor is the way in which restoration or system recovery is defined, i.e., as partial (a percentage of full service) or full restoration. Second, the precise estimation of restoration time depends upon what service substitutions are made and what improvements are made to make the final fix more resilient. Third, recovery is influenced by deliberate actions on the part of CI managers. These actions include deliberate shutdowns given unstable conditions or expected impending upsets. This is done to protect equipment and apparently people from explosions and fires.

IX. Conclusions

ICT connections to already interconnected CI present benefits but also adverse impacts if not planned in an integrated way. This is the challenge in the 21st century given the pervasiveness and very rapid pace of change that emerged in the previous century.

Some directions for future investigation are noteworthy. Interestingly, trends in connections between ICT and CI seem to be understood to a greater extent than trends in interconnections among CI in general and such trends will help to inform how ICT will interact with other infrastructures in the context of those interdependencies. A second area for future investigation is given the recovery times for CI not connected with ICT, the question remains is to how ICT can improve recovery times rather than exacerbate recovery.

The agencies and professional associations associated with CI have developed extensive ways to improve interconnections that avoid the level of destruction that can occur in the context of a threat e.g., APTA (2010) for public transit and the U.S. DOE (2017) for the electrical sectors. Decentralization and contingencies provide some solutions. Also, worker training is a critical necessity given how rapidly change is occurring and will continue to occur. As the CI and ICT connections expand, such knowledge resources will be needed to avoid the negative impacts of increasing interconnections.

Bibliography

American Public Transportation Association (APTA). July 30, 2010. Securing Control and Communications Systems in Transit Environments. http://www.aptastandards.com/Portals/0/1PubComment/APTA_RP_CCS_1_RT_001_10.pdf

Ashton, K. June 2009. That 'Internet of Things' Thing In the real world, things matter more than ideas, The RFID Journal, p. 1. http://www.rfidjournal.com/articles/view?4986

Charlet, D. December 19 2009. Four Eurostar trains stuck in Channel tunnel https://www.theguardian.com/uk/2009/dec/19/four-eurostar-trains-break-down

Chui, M., M. Loffler, and R. Roberts. March 2010. The Internet of Things, McKinsey Quarterly. http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things.

Clark, N. February 12 2010. Eurostar Criticized for Winter Breakdowns. http://www.nytimes.com/2010/02/13/world/europe/13eurostar.html

Clarke R. and L. Zeichner. 2004. Beyond the moat: new strategies for cybersecurity, Bank systems & technology. http://www.banktech.com/showArticle.jhtml?articleID¼17501355; 2004 [2005].

Con Edison. July 27, 2017.Statement From Con Edison Media Relations Re: MTA Project Plan. https://www.coned.com/en/about-con-edison/media/news/20170727/statement-from-con-edison-mta-project-plan

CTIA. 2017. Annual Year-End 2016 Top-Line Survey Results, Washington, D.C.: CTIA. https://www.ctia.org/docs/default-source/default-document-library/annual-year-end-2016-top-line-survey-results-final.pdf?sfvrsn=2 https://www.ctia.org/industry-data/ctia-annual-wireless-industry-survey

Daintith, J., ed. 2009. "IT", A Dictionary of Physics, Oxford University Press.

Dawson, C. Sept. 17, 2017. The Dangers of the Hackable Car, Wall Street Journal. https://www.wsj.com/articles/the-dangers-of-the-hackable-car-1505700481

Executive Office of the President. August 2013. Economic Benefits of Increasing Electric Grid Resilience to Weather Outages, Washington, D.C. http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf

Exida.com LLC. 2017. Repository of Industrial Security Incidents.

Federal Trade Commission (FTC). 2015. Internet of Things: Privacy and Security in a Connected World, Washington, DC: FTC. https://www.ftc.gov/system/files/documents/reports/federal-

trade-commission-staff-report-november2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Flegenheimer, M. September 25, 2013. Power Failure Disrupts Metro North's New Haven Line; May Last Days, New York Times. http://www.nytimes.com/2013/09/26/nyregion/metro-norths-new-haven-line-suspended-after-power-loss.html

FOLDOC. 9/19/08. Computing Dictionary, foldoc.org

Gandel, S. January 23, 2015. Lloyd's CEO: Cyber attacks cost companies $400 billion every year, Fortune. http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

Garnett, C. and M. Claude Gressier. February 12 2010. Eurostar Independent Review. http://www.continuityforum.org/sites/default/files/images/EurostarIndependentReview.pdf

Gartner, Inc. February 7, 2017. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Press Release. Stamford, CT: Garner, Inc. https://www .gartner.com/newsroom/id/3598917

Hansman, S. and R. Hunt. 2005. A taxonomy of network and computer attacks, Computers & Security, 24(1): 31-43.

Hilbert, M. and P. Lopez. 2011. The World's Technological Capacity to Store, Communicate and Compute Information, Science, 332 (60): 60-65.

Hook, L. and R. Waters. November 10, 2017. Google's Waymo passes milestone in driverless car race, Financial Times. https://www.ft.com/content/dc281ed2-c425-11e7-b2bb-322b2cb39656

Kaufman, S., C. Qing, N. Levenson, and M. Hanson. 2012. Transportation during and after hurricane Sandy. https://wagner.nyu.edu/files /faculty/publications/sandytransportation.pdf

Kjaerland, M. 2006. A taxonomy and comparison of computer security incidents from the commercial and government sectors. Computers & Security. 25, 7: 522–538.

Litman, T. September 8, 2017. Autonomous Vehicle Implementation Predictions Implications for Transport Planning Victoria Transport Policy Institute. https://www.vtpi.org/avip.pdf

McAfee and Center for Strategic and International Studies. June 2014. Losses: Estimating the Global Cost of Cybercrime.

Metropolitan Transportation Authority (MTA). October 2011. Preliminary review September 29, 2011 lightning strike at Jamaica, New York, NY, USA: MTA. http://web.mta.info/supplemental/lirr/images/09-29-2011_LightningStormPR.pdf

MTA. October 5 2013. Full New Haven Line Service To Resume Monday Morning. http://www.mta.info/press-release/metro-north/full-new-haven-line-service-resume-monday-morning

Miles, S., H. Gallagher, and C. Huxford. 2014. Restoration and Impacts from the September 8, 2011, San Diego Power Outage. J. Infrastruct. Syst., 10.1061/(ASCE)IS.1943-555X.0000176, 05014002.

Miles, S., N. Jagielo, and H. Gallagher. 2015. Hurricane Isaac Power Outage Impacts and Restoration. J. Infrastruct. Syst., 10.1061/(ASCE)IS.1943-555X.0000267, 05015005.

Miller, M. and D. C. Rowe. 2012. A Survey of SCADA and Critical Infrastructure Incidents Proceedings of the 1st Annual conference on Research in information technology, RIIT '12: 51-56.

Murray, J. December 18, 2011. Cloud network architecture and ICT - Modern Network Architecture.

National Academies of Sciences, Engineering, and Medicine. 2016. Attribution of Extreme Weather Events in the Context of Climate Change. Washington, DC: The National Academies Press. doi: 10.17226/21852.

National Infrastructure Advisory Council (NIAC). June 2016. Water Sector Resilience Final Report and Recommendations, Washington, D.C.: NIAC. https://www.dhs.gov/sites/default/files/publications/niac-water-resilience-final-report-508.pdf

National Oceanic and Atmospheric Administration (NOAA) National Centers for Environmental Information (NCEI). 2017. U.S. Billion-Dollar Weather and Climate Disasters. https://www.ncdc.noaa.gov/billions/

New York State 2100 Commission. 2013. NYS 2100 Commission Report. Recommendations to Improve the Strength and Resilience of the Empire State's Infrastructure. Albany, NY: The Commission.

New York State Office of the Governor. August 9, 2017. Governor Cuomo Announces State Orders Con Edison to Take Immediate Action to Guarantee Power Reliability Across the Subway System. Albany, NY: State of NY. https://www.governor.ny.gov/news/governor-cuomo-announces-state-orders-con-edison-take-immediate-action-guarantee-power

Ouyang, M. 2014. Review on modeling and simulation of interdependent critical infrastructure systems. Reliab. Syst. Saf., 121: 43 –6.

Perlroth, N. June 7, 2017. Electronic Setups of Driverless Cars Vulnerable to Hackers, New York Times. https://www.nytimes.com/2017/06/07/technology/electronic-setups-of-driverless-cars-vulnerable-to-hackers.html

Petit, F., D. Verner, D. Brannegan, W. Buehring, D. Dickinson, K. Guziel, R. Haffenden, J. Phillips, and J. Peerenboom. June 2015. Analysis of Critical Infrastructure Dependencies and Interdependencies, Argonne National Laboratory. http://www.ipd.anl.gov/anlpubs/2015/06/111906.pdf

Quinn, R. January 20, 2008. Cybercrooks Hacking Power Grid, Newser. http://www.newser.com/story/16862/cybercrooks-hacking-power-grid.html

Rinaldi, S., J. Peerenboom, T. and Kelly. 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine. 21(6): 11-25. doi: 10.1109/37.969131.

RISI. 2014. RISI - The Repository of Industrial Security Incidents. http://securityincidents.org/. Last update: January 28, 2015.

Romanosky, S. August 2016. Examining the costs and causes of cyber incidents, Journal of Cybersecurity.

Saidi, S., L. Kattan, P. Jayasinghe, P. Hettiaratchi, J. Taron. 2018 Integrated infrastructure systems A review, Sustainable Cities and Society, 36: 1 – 11.

Simonoff, J.S., C.E. Restrepo, and R. Zimmerman. 2007. Risk Management and Risk Analysis-Based Decision Tools for Attacks on Electric Power, Risk Analysis, 27 (3): 547-570.

Swiss Re/IBM. October 2016. In search of resilience in an interconnected world.

Swiss Re Institute. 2017. Sigma No 1/2017. Swiss re, Zurich Switzerland. http://media.swissre.com/documents/sigma1_2017_en.pdf

Symantec. 2013. Internet Security Threat Report (ISTR) 2013. Mountain View, CA: Symantec.

Symantec. April 2016. Internet Security Threat Report (ISTR) 2016, Volume 21. Mountain View, CA: Symantec. https://infolocktech.com/wp-content/uploads/2016/04/Internet-Security-Threat-Report-ISTR-2016.pdf

Symantec. April 2017. Internet Security Threat Report (ISTR) 2017 Volume 22. Mountain View, CA: Symantec. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Symantec Official Blog. September 6 2017. Dragony: Western energy sector targeted by sophisticated attack group.

U.S. Department of Energy (DOE), Quadrennial Energy Review Task Force. 2017. Quadrennial Energy Review: Transforming the Nation's Electricity System: The Second Installment of the QER. https://energy.gov/policy/initiatives/quadrennial-energy-review-qer/quadrennial-energy-review-second-installment https://energy

U.S. Department of Homeland Security (DHS). November 2011. Blueprint for a Secure Cyber Future, Washington, DC: U.S. DHS.

U.S. DHS. July 11, 2017. Critical Infrastructure Sectors, Washington, DC: U.S. DHS. https://www.dhs.gov/critical-infrastructure-sectors

U.S. DHS 2012. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) ICS-CERT Monitor, October/November/December 2012. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf

U.S. DHS ICS CERT. 2013. ICS-CERT Year in Review 2013. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_In_Review_FY2013_Final.pdf

U.S. DHS ICS CERT.2014. ICS-CERT Year in Review 2014. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2014_Final.pdf

U.S. DHS ICS CERT. 2015. NCCIC/ICS-CERT Year in Review National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team FY 2015. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

U.S. DHS ICS CERT. 2016. NCCIC/ICS-CERT Year in Review National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team 2016. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf p. 5, 8

U.S. DHS ICS-CERT. 2017. National Cybersecurity and Communications Integration Center 2016 Pie Charts. https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_IR_Pie_Chart_FY2016_S508C.pdf

U.S. DHS ICS-CERT. 2017. Monitor March-April 2017. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Mar-Apr2017_S508C.pdf

U.S.DOT. 2010. 2010 Deployment Tracking Survey Results. http://its2010.ornl.gov/

U.S. DOT. August 2011. Deployment of ITS: A Summary of the 2010 National Survey Results. FHWA-JPO-11-132. http://its2010.ornl.gov/documents/nationalreport.pdf

U.S. DOT. August 2014. Deployment of Intelligent Transportation Systems: A Summary Of the 2013 National Survey Results FHWA-JPO-14-146. https://ntl.bts.gov/lib/54000/54200/54268/2013-National-ITS-Summary-Rpt_FINAL-7.pdf

U.S. DOT. 2013. 2013 Deployment Tracking Survey Results. http://www.itsdeployment.its.dot.gov/

U.S. DOT. 2008. Status of the Nation's Bridges, Highways, and Transit Conditions & Performance, Washington, DC: U.S. DOT. From the ITS Deployment Statistics Database, Research and Innovative Technology Administration.

Varga, L., and J. Harris. 2015. Adaptation and resilience of interdependent infrastructure systems: A complex systems perspective. Int. Symp. for Next Generation Infrastructure Conf. Proc., T. Dolan and B. Collins, eds., International Institute of Applied Systems Analysis, Vienna, Austria, pp. 133-137.

Verner, D., F. Petit, and K. Kim. October 2017 Incorporating Prioritization in Critical Infrastructure Security and Resilience Programs. Homeland Security Affairs 13, Article 7. https://www.hsaj.org/articles/14091

Walsh, J., et al. 2014. Ch. 2: Our Changing Climate. Climate Change Impacts in the United States: The Third National Climate Assessment, J. M. Melillo, Terese (T.C.) Richmond, and G. W. Yohe, Eds., U.S. Global Change Research Program, pp. 9-67. doi:10.7930/J0KW5CXT

Weiss. J. March 19, 2009. Cyber Security and Critical Infrastructure Protection. Testimony by Joe Weiss. http://cimic.rutgers.edu/WS-CFP/Joe-Weiss.pdf

The White House. February 12, 2013. Presidential Policy Directive -- Critical Infrastructure Security and Resilience Presidential Policy Directive/PPD-21. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Wikipedia. December 1, 2017. Information technology. https://en.wikipedia.org/wiki/Information_technology

Wikipedia. December 26, 2017. Information and communications technology. https://en.wikipedia.org/wiki/Information_and_communications_technology

Zimmerman, R. 2005. Mass Transit Infrastructure and Urban Health, J. of Urban Health, 82(1): 21-32.

Zimmerman, R. 2012. Transport, the Environment and Security. Making the Connection, Cheltenham, UK and Northampton, MA: Edward Elgar Publishing, Ltd.

Zimmerman, R. 2014a. Network attributes of critical infrastructure, vulnerability, and consequence assessment," Chapter 372 in Safety, Reliability, Risk and Life-Cycle Performance of Structures and Infrastructures, edited by G. Deodatis, B. R. Ellingwood, and D. M. Frangopol, London, UK: Taylor & Francis Group, CRC Press, pp. 2777-2782.

Zimmerman, R. 2014b. Planning Restoration of Vital Infrastructure Services Following Hurricane Sandy: Lessons Learned for Energy and Transportation, Journal of Extreme Events, 1(2), DOI: 10.1142/S2345737614500043
http://www.worldscientific.com/DOI/pdf/10.1142/S2345737614500043

Zimmerman, R. 2016. Chapter 32, Resilient Urban Infrastructure for Adapting to Extreme Environmental Disruptions, In: The Routledge Handbook of Urbanization and Global Environmental Change, edited by K.C. Seto, W. D. Solecki and C. A. Griffith, New York, NY: Routledge, pp. 488-512.

Zimmerman, R. and M. G. Dinning. November 2017. Benefits and Needs for an Integrated Approach to Cyber-Physical Security for Transportation, In Transportation Systems Resilience: Preparation, Recovery, and Adaptation, Transportation Research Circular E-C226, Transportation Systems Resilience Section, Standing Committee on the Logistics of Disaster Response and Business Continuity, Standing Committee on Emergency Evacuations, Standing Committee on Critical Transportation Infrastructure Protection, Transportation Research Board, Washington, DC: National Academies Transportation Research Board, pp. 15-21.
http://onlinepubs.trb.org/onlinepubs/circulars/ec226.pdf

Zimmerman, R. and C. E. Restrepo. 2006. The Next Step: Quantifying Infrastructure Interdependencies to Improve Security, International Journal of Critical Infrastructures, 2 (2/3): 215-230.

Zimmerman, R., Q. Zhu, F. de Leon, and Z. Guo. December 2017. Conceptual Modeling Framework to Integrate Resilient and Interdependent Infrastructure in Extreme Weather, Journal of Infrastructure Systems, 23(4): (online) 04017034-1 to 13.
http://ascelibrary.org/doi/pdf/10.1061/(ASCE)IS.1943-555X.0000394

Zimmerman, R., Q. Zhu, and C. Dimitri. 2017. A Network Framework for Dynamic Models of Urban Food, Energy and Water Systems (FEWS), Journal of Environmental Progress & Sustainable Energy. http://onlinelibrary.wiley.com/ Published online 22 AUG 2017, DOI: 10.1002/ep.12699.

Zimmerman, R., Q. Zhu and C. Dimitri. 2016. Promoting Resilience for Food, Energy and Water Interdependencies, Journal of Environmental Studies and Sciences, 6(1): 50-61. Published online: February 12, 2016. DOI: 10.1007/s13412-016-0362-0

Acknowledgements

The author acknowledges the Hewlett Foundation Grant to the NYU Center for Cybersecurity. Zimmerman's research on other grants that supported portions of this work included:

- "Urban Resilience to Extreme Weather Related Events Sustainability Research Network (UREx SRN)" funded by The National Science Foundation (NSF) (#1444755) to Arizona State University.
- Critical Resilient Interdependent Infrastructure Systems and Processes (CRISP) Type 1—"Reductionist and integrative approaches to improve the resiliency of multi-scale interdependent critical infrastructure," funded by the NSF (1541164)
- "Dynamic Resiliency Modeling and Planning for Interdependent Critical Infrastructures," funded by the Critical Infrastructure Resilience Institute, U. of Illinois, Urbana-Champaign, part of the Homeland Security Center of Excellence funded by the U.S. Department of Homeland Security

Disclaimer: Any opinions, findings, and conclusions or recommendations expressed in this work are those of the author and do not necessarily reflect the views of the sponsors.