Cyber
Discussion Paper #2

Literature Review - Cyber Dependency at a Domestic and International Levels

Mohar Thakur
July 2016
Abstract

This literature review offers some insight into how scholars have studied cyber dependencies. The main studies present, in considerable depth, the growing importance of cyber assets in the daily functioning of society. By detailing the differing types of infrastructure dependencies, the scholars affirm the fundamental risks of such dependency in the case of critical infrastructure, and the challenges these vulnerabilities present for resilience management. However, in contrast to the gravity of the vulnerability, the research reviewed reveals a lack of comprehensive information and analysis of cyber dependency that might clearly define the implications of it for critical infrastructure resilience. While some scholars provide comprehensive modelling tool applications, they are mainly theoretical or limited to closed environments. There is an absence of practical scenarios and multi-infrastructure analyses. It would appear that scholars will need live and extensive cooperation from the operators of infrastructure and essential services, both nationally and globally, to reach the next level of comprehensive modelling and simulations that can provide insights into cyber dependencies.
Table of Contents

Abstract .................................................................................................................................. 4
Introduction ............................................................................................................................ 5
Dependencies and Interdependencies .................................................................................... 7
Global Cooperation ................................................................................................................ 9
Open Source Modelling Tools ............................................................................................. 13
Conclusion ........................................................................................................................... 18
Introduction

In 2001, the state of California in the United States of America (USA) was affected by a number of blackouts that occurred between June 2000 and May 2001, impacting between 100,000 and 1.5 million homes in the region.\(^1\) A shortage of electricity supply in the market caused by market deregulation and manipulations led to the eventual collapse of the state’s largest energy company, Enron.\(^2\) Even more widespread, was the blackout in 2011. While shorter and less political in its nature, the technical error affected seven million people for just over three days.\(^3\) As the San Diego skyline darkened, the city grew to a near standstill as public transport such as trains and trams were shut down. While confirmed as not an act of terrorism\(^4\), the power outage took days to restore to normal output levels, emphasising our dependency on an activity that is both operated and regulated through cyber infrastructure.

This paper reviews current literature in the field of cyber dependency. By generalising the case of dependency on critical infrastructure, researchers argue for further investment in the robust security of infrastructure. Yet, many are unable to take it one step further and explore how we can manage interdependency links through simulation modelling to achieve efficient investment to ensure delivery of critical urban services of water, energy, transport and communication, often controlled by information technology. Scholars describe an overarching need for global collaboration in the research and development of critical infrastructure modeling and simulation tools, the early stages of which are reviewed here, in the event of a cyber attack.

Hasan and Foliente (2015) use the 2011 California energy crisis to understand the dependencies in interconnected critical infrastructures and essential services.\(^5\) While they note the obvious impact on household electricity consumption, they concentrate on the cascading effects that

such an electricity outage can have on other critical infrastructure systems. As dependencies between infrastructure sectors rise as a result of interconnectivity, there is a diminishing ability to robustly protect these critical foundations. While the examples of the California blackout crises were not due to a specific failure on the part of the cyber infrastructure, the daily operations and technical systems of energy sector are heavily dependent on and monitored by cyber infrastructure. There are also numerous circumstances at international and domestic levels where the effects of failure in the cyber infrastructure system can have cascading effects on critical infrastructure. The cumulative economic effect can be devastating.

Public policy analysts, business planners and commentators are aware of the problem. They know that the ability to analyse and implement a working model on infrastructure dependencies and to understand the cascading effects of cyber infrastructure failures would allow for the gathering of accurate information in regards to resource allocation. Efficient investment into the critical infrastructure could translate into a more hardy system of protection and resilience. The basic awareness has however not translated in most cases to mapping the potential cascading effects, how and if they might affect society at large, and how public and private enterprises can mitigate the effects of such disasters and manage the appropriate restoration of normal services in a reasonable timeframe. As one observer summed it up, public and private entities can no longer afford to have varying types of risk management policies focusing merely inside an enterprise but rather need to develop a holistic risk management policy for the entire organisation and supply chain.

Over time, “our society crossed the line from merely benefiting from new electronic tools to being totally dependent on them.” What we can learn from the instability of human co-dependence, we have yet to learn for cyber dependency. Cooperation, honesty and trust can boost our resilience, and by managing how we can analyse these relationships, we can better understand how to protect them. While the emergence of cyberspace has revolutionised engagement between global communities, scholarly research is struggling to keep up with the changes. This review of the literature seeks to evaluate the extent of research on the dependency

---

6 ibid. p.2147.
in cyber space between critical infrastructure systems and essential services, at both a domestic and international level.

Dependencies and Interdependencies

Petit et al define a dependency as a “linkage or connection between two infrastructures, by which the state of one infrastructure influences or is reliant upon the state of the other.” Rinaldi et al go further and suggest that each interaction that is the result of an infrastructure influence can be categorised into four classes of dependency:

- **Physical** – an infrastructure has a physical dependency if the quality of its operations is reliant upon the material output of another infrastructure i.e. the tangible product of one infrastructure is required by another for its operations or as an input.
- **Cyber** – if operations are dependent on information and data transmissions through electronic links, there is a cyber dependency.
- **Geographic** – if an event in the local environment generates variations in the ability or state of operations of an infrastructure, assets are geographically dependent.
- **Logical** – often attributed to human decisions or actions, rather than as the result of a physical, cyber or geographic dependencies.

Rinaldi et al suggest that we now have an environment in which infrastructure is much more interdependent, rather than simply dependent and that this leads to little or no cushion in the case of failure, due to few, if any, alternative sources of available service. Petit et al define this interdependency as a “bidirectional relationship between two infrastructures in which the state of each infrastructure influences or is reliant upon the state of the other.” Rinaldi et al point out that with the rise of automation in a number of infrastructure sectors, the cyber interdependency across infrastructures has increased dramatically, concurrently with the rise in their complexity. Second, as mergers further eliminate surplus redundancies and overheads in infrastructure operations, a shift towards deregulated markets has also shed formerly mandated reserve capabilities that served as shock absorbers against system failures, leading

---


to a rise in vulnerabilities. “Tighter, more complex, and more extensive interdependencies lead to increased risks [and therefore] greater requirements for security.”12

Pederson et al13 describe five main sources of interdependency levels within communities;

- **Physical** - A requirement, often an engineering reliance between components of infrastructure.
- **Informational** - An informational or control requirement between components where one source of infrastructure provides pivotal information to the operation of another.
- **Geospatial** - A relationship that exists entirely because of the proximity of components.
- **Policy/procedural** - An interdependency that exists due to policy or procedure that relates a state or event change in one infrastructure sector component to a subsequent effect on another component.
- **Societal** - The interdependencies or influences that an infrastructure component event may have on societal factors such as public opinion, public confidence, fear, and cultural issues.

To ensure that global infrastructure networks are hardy and secure, we cannot avoid the requirement of mapping global cyber interdependencies. The Argonne National Lab report, by Petit et al14 describes the four phases in a dependency/interdependency assessment as;

- **Phase 1 – Initial Estimate:** research and data collection, open source information, offers general understanding of functions of critical infrastructure
- **Phase 2 – Present:** development of data collection tools and models
- **Phase 3 – Advanced:** consideration of all dimensions of critical infrastructure dependencies and interdependencies, new data collection mechanisms required, integration of existing independent assessment tools and approaches
- **Phase 4 – Ultimate Goal:** comprehensive understanding of all dependency and interdependency dimensions, allows for decision makers to anticipate and characterize, in real time, how dependency dimensions influence resilience and protection of critical infrastructure systems of a region

14 Analysis of Critical Infrastructure Dependencies and Interdependencies. Petit, F et al. Risk and Infrastructure Science Centre, Global Security Sciences Division, Argonne National Laboratory. June 2015 p. 33
To reach Phase 4, given the amount of data and information analysis required, across various critical infrastructure sectors, both domestic and internationally, Petit et al make it clear that international cooperation is needed.

Global Cooperation

Given the output of scholarly and government discussion papers, importance given to combatting cyber threats and investing in cyber infrastructure resilience measures, there is a real lack of cooperation on both a regional and global scale. Bradshaw believes that this “lack of communication [could] not only result in redundant analysis, but also [delay] defensive and corrective measures which could [limit damage]”15 While a number of resources identify evidence demonstrating the dependent nature of society on cyber infrastructure, many do not address the lack of methods nor do they provide methods to analyse these dependencies. Furthermore, many of the models that are mentioned in the open-source literature, are seemingly theoretical. While this may be useful in very early stages of data and information analysis, as Petit et al mention in their interdependency assessment, to reach phases three or four, policy and research on cyber infrastructure and interdependencies now require much more sophisticated simulations, requiring real world data to analyse real world issues. Given the breadth and depth of cyber infrastructure dependency in society, this requires data from a number of information sectors.

“A data-driven capability that operationalises the analysis of dependencies and interdependencies would not only provide an unprecedented level of situational awareness, it would also enable decision makers to anticipate disruptions. To achieve this ultimate goal, [as described above in Phase 4 of the interdependency development assessment], the development of a comprehensive and interactive assessment of critical infrastructure dependencies and interdependencies, requires the combination of multiple areas of expertise in an adaptive and flexible assessment framework.”16

In this statement concluding a report focusing on the analysis of critical infrastructure dependencies and interdependencies by the Argonne National Laboratory, it is clear that while


such a “data-driven capability”\textsuperscript{17} would be ideal, the reality is difficult. This is due to “the combination of multiple areas of expertise”\textsuperscript{18}, as there is a real lack of cooperative communication and information sharing between infrastructure sectors. Bradshaw’s\textsuperscript{19} Chatham House paper thoroughly discusses combating cyber threats through international cooperation. She discusses cooperation on a global scale that could assist in the prevention or response to cyber incidents through incident analysis, response, information sharing and dissemination and skills training. Bradshaw also addresses the complex legal questions and lack of trust between governments and private sector firms that discourages sharing of the aforementioned information and skills.

Karl Rauscher\textsuperscript{20} further develops the argument for international cooperation from an engineering perspective. He argues, that at a global level, the overall interconnectivity of the continents is entirely reliant on a single point of failure - undersea cables - and hence violates one of the most fundamental design principles. This high level of dependence, rapidly increasing, highlights an enormous expected future dependence, which must result in a diligence to ensure its reliability and performance.\textsuperscript{21} Again, given the international nature of our cyber dependency, an international cooperative method must be found.

As it is increasingly integrated into the fabric of our daily lives, the reliance on cyber infrastructure grows, and there are greater incentives and opportunities for actors to exploit these systems. When everything is a part of the Internet, there are innumerable entry points into a weak network. Bradshaw believes that sovereign states recognise this new domain and many are already exerting control, demonstrating their lessening desire to share knowledge and cooperate to prevent cyber attacks.\textsuperscript{22} Kunreuther and Heal find\textsuperscript{23} that in some scenarios,

\textsuperscript{17} ibid p. 33
\textsuperscript{18} ibid p. 33
\textsuperscript{21} Rauscher, Karl Frederick. Proceedings of the Reliability of Global Undersea Cable Communications Infrastructure Study and Global Summit. ROGUCCI: The Report. IEEE. Issue 1, 2010 p. 102
\textsuperscript{22} Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity. Global Commission on Internet Governance. Bradshaw, Samantha Chatham House, The Royal Institute of International Affairs. Paper Series No. 23, December 2015 p. 6
without the incentives of government policy in regards to insurance, liability or regulation of the cyber infrastructure sector, the private sector may have to take the lead in adopting or promoting global cyber security standards. Both papers recognise that sharing timely and actionable information about threats and strategies is required to improve situational awareness and expand threat horizon and defensive agility understandings, which can therefore result in better decision making.

It remains that one way to gain information about cyber attacks, is to be attacked and perform a full analysis on the attack and recovery of systems. The disseminating of such information to other firms may prove to be useful in the longer term for an industry sector or country to protect or mitigate further attacks, but Bradshaw does concede that such an admission of breach or ask for help can be seen as a “reputational damage” liability. Yet, Hasan argues that by understanding the extent of an attack, the interdependency between infrastructure sectors and the cascading effects, a more robust infrastructure grid can be developed. Similarly, the Department of Homeland Security established a Cyber Incident Data and Analysis Working Group (CIDAWG) in February 2015, comprised of members from various critical infrastructure sectors and other cybersecurity professionals. The aim, to explore how anonymous cyber incident data sharing and a trusted cyber incident data repository would work to improve cybersecurity for U.S. public sector agencies and private sector companies.

Kunreuther and Heal concur with Bradshaw on many points raised in relation to cooperation, however their focus is on a local industry level, where they discuss interdependent group security through group think and pushing for the incentive to invest in security - which is diminished if not all parties take action and participate. They identify that vulnerabilities in

---


cyber infrastructure and in cyber interdependencies not only depend on the way a single firm manages risk but also on the way the entire supply chain does too. It is possible to encourage investment in rigorous cyber protection as it leads to positive externalities that can mitigate the possibility of contamination from other firms. Thus Kunreuther and Heal argue for an intervention from the public sector to coordinate mechanisms that will induce such activities. However, the prisoner’s dilemma represents the main problem with encouraging the adoption of such protective measures, as it is only advantageous if all agents invest, but there is no economic incentive to do so on their own.

Ito reminds us that “cyberspace as a shared global resource” that promotes an open and collaborative environment, may now simply be an image of the past. Bradshaw continues, stating that “internal coordination and exogenous contextual problems influence institutional dynamics” Diversity in Internet governance has made cooperation difficult leading to different interests, values and views of legitimate procedures on how governance should be conducted. While a varied perspective can be beneficial, given the fluid nature of what the Internet means and represents, it also leads to an increased chance of deadlocks on negotiations for norms and regulations.

Open Source Modelling Tools

As aforementioned, in the literature presented, we have seen limited international cooperation, consent, trust, and information sharing between public and private sectors in the realm of cyber security and cyber dependency analysis. This can be attributed to negative impacts that both governments and private firms are fearful of, such as the sharing of information. However, if realised, international cooperation could have higher rewards than the current environment of mistrust and lack of information sharing. Furthermore, the current open access literature has very limited modelling information and data dissection. Modeling for individual infrastructures in well development, however, no infrastructure exists isolated and on its own. Multinational investment into the research and development of multi-infrastructure modelling tools and simulation, a field greatly underdeveloped, would allow for a more efficient methodology in

28 ibid p. 3
29 ibid p. 8
analysing such scenarios given the experience and knowledge that would be brought together to create such models.

The research and development of infrastructure modelling tools published by research organisations are mostly focused on the domestic level, or local infrastructure level. This research and data dissection is largely coming from the USA, highlighting the specific investments made into the national research laboratories that are overseen by the Department of Energy. A few key sources are mentioned below, highlighting specific readings that have provided beneficial insights into where current research focuses stand.

**Interactive Dependency Curves**
Petit et al\(^{32}\) describe an interactive dependency curve as a curve that addresses the dependency of an organisation on any given resource. The curve characterises the effects of an organisation’s operatives given the loss of this resource. Current versions solely address the amount of degradation over time that would be generated by the loss of a physical resource but could be manipulated to include cyber and logical resources. The curve highlights information and data on events and procedures in place in the case of a loss of resource, times and durations of impacts and recovery and amount of degradation. A ‘dashboard’ view allows for the view of multiple dependency curves to compare with given resources.

**I2Sim and MATE**
By combining the output from the infrastructure interdependencies simulator (I2Sim) and multi-area Thevenin equivalent (MATE) model based on a matrix partitioning technique, Rahman et al\(^{33}\) identify an efficient alternative to agent-based simulations. The paper identifies agents as autonomous individuals interacting to reach higher-level objectives given physical space, capabilities and experiences. Agent-based simulations are most often used, similar to complex systems that are unpredictable to a single agent, but have their limitations, most significantly, scalability. MATE, often used for large-scale real time power system simulation, matched with I2Sim, represents interdependencies through mathematical functions. The cell-channel model infrastructure interdependencies simulator, I2Sim, “allows


multiple infrastructure operators to coordinate their interdependencies while maintaining their respective organisation level security procedures and confidentiality requirements."34

**DOMINO Modeling Tool**

Published in The Center for Infrastructure Protection and Homeland Security monthly *The CIP Report* is a detailed analysis by Morabito and Cloutier35 on the DOMINO mapping tool. This tool, originally developed by the Centre Risque & Performance at the Ecole Polytechnique de Montréal, is a decision and planning assistance method that anticipate domino effects in managing critical infrastructure interdependencies at a regional level. As an operationally and economically feasible approach of analysis, modeling and mapping physical and geographical interdependencies between critical infrastructures, DOMINO was developed by seven critical system operators in Montreal. The bottom-up approach has reaped rewards, increasing local government understanding of interdependent links between regional infrastructures and what their societal reliance is.36

While still in early prototype stages, the DOMINO program consists of a database that is linked to various geographic information systems, functioning on consequence based risk management approaches. An example of the DOMINO simulation analysis tool is provided in the report outlining a simulated attack on critical infrastructure in the New York City tri-state area.37 By identifying the critical services that have been affected, and to what extent, the analysis also demonstrates the interdependencies between infrastructure sectors.

The analysis provided by DOMINO reports the equipment and infrastructure affected and planned protective measures. Morabito and Cloutier state that it allows managers to better understand any given situation and potential changes to the domino affects, thus resulting in more relevant and coherent decision-making. The “cartographic module that displays the propagation of failures over time and space”38 could be integrated into a regional disaster


36 ibid p. 5

37 ibid. p.6

management plan, to increase general resilience or specific prevention/preparation or intervention/recovery from cyber attacks. While assisting in ensuring organisations and infrastructure sectors are less vulnerable to failure, and therefore greater security, Morabito and Cloutier note that the DOMINO mapping tool process implementation demands real long term cooperation as it is based on a mechanism of sharing and handling sensitive data in a context of mutual trust and respect of confidentiality.

**US National Laboratory Research Papers**

The US Department of Energy (DoE) National Laboratories is a network of 17 national laboratories that are overseen by the DoE. The laboratories are responsible for advancing science and technology research and development. While their primary focus is related to national security initiatives, other missions include research and development in energy and environmental programs, as well as the security of critical national infrastructures. Here, we will discuss the research developed by three national laboratory papers – Sandia, Idaho and Argonne National Laboratories. All papers mention the central concern of cyber dependency and attempt to provide some answers.

In 2009, the Argonne National Laboratory, along with support from the Department of Homeland Security, began assessing high-risk critical infrastructure with targeted questionnaires that produced a valued system through the Protective Measures Index, Resilience Measurement Index and Vulnerability Index. These results will help support decision-making, based on multi-attribute utility theory and decision analysis principles. While zero stands for low protection and 100, high protection, a higher number does not necessarily mean that a specific event will not affect the facility or have severe consequences. Conversely, a low number does not mean that a disruptive event will automatically lead to a failure of the critical infrastructure and to serious consequences. The numbers are instead used to compare the level of protection, resilience and vulnerability of critical infrastructure and also guide the prioritisation of limited resources for improving protection and lowering vulnerability. Each

---


index is directly aligned with the need to address capabilities required of critical infrastructure and can be used as a standalone for addressing the protection of a specific facility, in combination with the other indices mentioned to characterise an overall risk and for guiding decisions.

Kelic et al\textsuperscript{41} discuss that the need for real time operations has impeded the use of security technologies that will assist in infrastructure resilience, due to fears that they will hinder operations. Many current operational control systems, which have been in use for decades, have limited computational capabilities with respect to cyber resilience. These design limitations are a factor in preventing security technologies from being implemented, with open access control systems designed for efficient daily programming and management of systems rather than cyber security. However, Kelic et al accept that customized systems are equally difficult to implement, as effective software patches are harder to develop and apply.

“Sandia currently has modeling tools [- some are briefly summarised below -] that analyze cyber effects and how those cyber effects lead to physical impacts. Sandia also has modeling and simulation capabilities to understand the economic consequences of the loss of a critical physical asset. A method is needed that will allow the bridging of these two capabilities and provide analysts with the ability to understand the national-level risk from cyber attacks.”\textsuperscript{42}

\textit{Supervisory Control And Data Acquisition (SCADA):}  
A type of control system that can be used for larger geographic areas, the primary benefit of SCADA is that data from various system functions can be collated from a regional area, which can be substantially more effective in decision-making. Furthermore, this can result in increasingly efficient and coordinated critical infrastructure management. However, the numerous host computers, local processors and communication pathways, which are both short and long range, provide a number of access points to cyber attacks. Yet Eisenhauer et al, supporters of the SCADA system, reflect that “without sufficient means to fully quantify and demonstrate the potential impacts of cyber attacks on energy sector control systems, asset owners are hard pressed to justify SCADA control system security as a top funding priority.

The result is a reactionary policy to cyber security that places our bulk electric and critical oil and gas assets at greater risk to emergent cyber threats.\(^{43}\)

**Virtual Control Systems Environment (VCSE):**
A test bed environment, VCSE, has capabilities to combine real, emulated and virtual entities that are involved in the power and energy generation and distribution industry. There is a possibility for this to be extended to other industries, but there seems to be no mention of whether there can be multi-infrastructure sector integration through this model. The use of this program and help researchers, developers and managers to learn about system dependencies and identify threat attack pathways that could be used to exploit open vulnerabilities.\(^{44}\)

**IEEE Reliability Test:**
To compare and benchmark electrical power reliability, the IEEE model can be used, essentially ensuring that energy management systems can handle low or high power system loads dependent on the time of day and year. It is therefore designed to have a standardised application, “with no intention of developing a system that is representative of a specific of typical power system.”\(^{45}\)

**Fast Analysis and Simulation Team (FAST) Analysis Infrastructure Tool (FAIT):**
As the name suggests, the FAST team is able to provide rapid responses to questions about threats to national security infrastructure. These evaluations are conducted in response to specific threats, again, implying the requirement for prompt analyses. Kelic et al give the example of a sizeable cyber attack on a major city or large regional area, that results in the disabling of power and other energy resources. Here, the FAST team would be asked to report to the Department of Homeland Security in response to consequences of the attack and what this could mean for other infrastructures and the wider economy.\(^{46}\) Interrelated, is FAIT, which can be used to determine specific infrastructure interdependencies, assisting in overall critical infrastructure analyses.


\(^{45}\) ibid pp. 28

\(^{46}\) ibid pp. 28
The focus of the Sandia National Laboratory is in the energy sector and electrical power reliability analyses, touching on the complexity of critical infrastructure interdependencies. The modeling systems outline that while a single point of failure does not imply that the whole system will fail, as more parts of a system fail, the more likely it is for far-reaching impacts to be felt. The modeling templates outlined also provide real-life cyber attack consequence assessment processes. If extended in use for other infrastructure sectors to allow for a wider array of data to be gathered to further analyze cyber dependency and critical infrastructure interdependencies.

The Idaho National Lab, along with co-sponsor U.S. Technical Support Working Group, has conducted a survey of 30 simulations to identify and outline the current area of research in the field of modelling and analysis of interdependencies between critical infrastructures. The survey, which aims “to develop a single source reference of critical infrastructure interdependency modelling tools”\(^{47}\) allows users to assess the varying levels of capabilities and also provide guidance for directing research and development to where it is required to address the needs of end users.

From the summarising table provided in the Idaho National Laboratory paper, we can make some inferences on which infrastructure sectors are targeted for modelling data and therefore, those most at risk, those easiest to gather data on, or those that are the easiest to reinforce. The table also highlights the varying maturity levels of modelling applications, however, fails to include actual examples of the use of these tools, but simply provides a snapshot description of their attributes. Some observations include, but are not limited to;

• All identified simulations have been developed with primary funding from the USA, with exception of CIPMA (Australia) and CISIA (University Roma Tre)
• There is a focus on developing simulations for the electrical power grid, with limited focus on the transport system – highways and railways.
• There is little to no focus on the simulated disruptions related to water infrastructure, ranging from drinking water to sewerage and storm water.
• The focus on the electrical power grid can be attributed to the investment into the US Department of Energy National Laboratories, whereas other federal departments may not be investing in such research and development.
• Roughly 40% of the simulations surveyed are at a mature internal usage level, with an additional 40% at the research and developmental stages.
• Five simulations surveyed are at a mature commercial level; TRANSIMS, Nexus Fusion Framework, Fort Future, DEW and CARVER
• Three simulations surveyed are suitable for use with all 15 infrastructure sectors that are listed; Athena, CIP/DSS and Fort Future.

Conclusion

A broad look at the literature available in this study finds that research and development of the dependency/interdependency assessment described by Petit et al is currently in Phase 2. The absence of practical scenarios and comprehensive multi-infrastructure analyses stymies the possibility of movement into Phase 3; live and extensive cooperation between operators of infrastructure and essential services, both nationally and globally. The DOMINO modeling tool developed in Montreal best exemplifies the possibility of this cooperation, albeit at a small scale. While still in the prototype stage, the tool demonstrates that collaboration is possible and can produce considered data and forecasting methods for integrated critical infrastructure management. The inclusion of “external dependency management” as one of ten pillars of the Department of Homeland Security “cyber security and resilience health check,” confirms the shift in focus to management of critical infrastructure dependency.

While all relevant research papers in this literature review pertaining to cyber critical infrastructure interdependencies have been published since the year 2000, the vast number providing tangible strategies and results have only been published in the last four to five years. Few have been published by scholarly journals, with most sponsored through government means ranging from the NATO Cooperative Cyber Defence Centre of Excellence, the DoE National Laboratory program and George Mason University publications. Contrastingly, a number of research papers do mention the limited input that can be supported by government
sponsorship of cyber interdependency, and the need for further private research and development in this field.

The understanding of the extent of interdependency between critical infrastructure systems is crucial in the development of a more robust infrastructure grid to which cyber dependency, and the foundation of society, is deeply enmeshed. The literature demonstrates this as one of the most difficult and burgeoning policy challenges of the 21st century as the dependence on cyber has profound effects on the foundation of society. A global community that can find an optimal balance between freedom and security in cyberspace, in addition to ensuring safe management of our dependency, will reap rewards that are far greater than the costs.