2011

Cyberinfrastructure Inside Out: Definition and Influences Shaping Its Emergence, Development, and Implementation in the Early 21st Century

Kerk F. Kee
Lucy Cradduck
Bridget Blodgett
Rami Olwan

Running head: CYBERINFRASTRUCTURE INSIDE OUT

Cyberinfrastructure Inside Out:
Definition and Influences Shaping Its Emergence, Development, and Implementation in the Early 21st Century

Kerk F. Kee

Department of Communication Studies, The University of Texas at Austin, USA

Lucy Cradduck

Faculty of Law, Queensland University of Technology, Brisbane, Australia and

Business Faculty, University of the Sunshine Coast, Australia

Bridget Blodgett

College of Information Sciences and Technology of the Pennsylvania State University, USA

Rami Olwan

Faculty of Law, Queensland University of Technology, Brisbane, Australia

Cyberinfrastructure Inside Out:

Definition and Influences Shaping Its Emergence, Development, and Implementation

in the Early 21st Century

Cyberinfrastructure (Atkins, et al., 2003; Seidel, Muñoz, Meacham, & Whitson, 2009; Stewart, 2007), also commonly known as e-infrastructure in the UK (Meyer & Dutton, 2009 ; Meyer, Schroeder, & Dutton, 2008) and e-research infrastructure in Australia and Europe (Eccles, et al., 2009; Jankowski, 2009; Schroeder, 2007a), officially emerged and was recognized at the turn of the millennium. Since then, it has attracted serious attention and much investment from the scientific and scholarly communities as an emerging method and platform of research; and from political and policy organizations as a new entity with tremendous economic, societal, and global implications. Due to its potential, multiple stakeholder groups are grappling with the concept of cyberinfrastructure and engaging in the building of this "next-generation Internet" (Foster, Kesselman, & Tuecke, 2001, p. 217). As we look forward to the second decade of the 21st century, the time is ripe to explore three interrelate research questions:

- What is cyberinfrastructure?
- What are they key political influences shaping its domestic emergence and development?
- What are the key challenges impacting its international implementation?

By drawing widely from literature in the social sciences, law and policy studies, as well as computer and information sciences, this chapter attempts to provide some preliminary answers to these important questions.

Our purpose for this chapter is threefold. First, in order for multidisciplinary scholars and policymakers to study cyberinfrastructure, it is critical to have a coherent definition. Therefore, we synthesize definitions from a range of disciplines and propose an integrated and generative definition of cyberinfrastructure based on four dimensions: characteristics, layers, processes, and outcomes. As cyberinfrastructure continues to expand in the future, we anticipate the four dimensions will generate new examples while remaining useful as an integrated framework.

Second, in order for appropriate policies to be developed around cyberinfrastructure, we sketch a political model of cyberinfrastructure development based on three key influences: market, policy, and law. By drawing from the case of the Internet, this model describes the recursive relationships among these three domestic influences and how they can impact the case of cyberinfrastructure. We also discuss the concepts of digital divides and network neutrality as cautionary tales from the Internet that scholars and policymakers need to keep in mind while they work to advance cyberinfrastructure domestically.

Third, as cyberinfrastructure builds on the Internet, its implementation at the international scale deserves careful examination. Cyberinfrastructure projects at national borders often encounter challenges that limit their effective implementation. We draw a typology based on key influences in three categories - international challenges, national challenges and common project challenges, and argue that the lack of international standard policy structure is a fundamental challenge to effective implementation. We discuss how these influences shape

cyberinfrastructure implementation at the international scale while balancing between policy harmonization and conformation among large and small countries.

Collectively, we believe the integrated definition, political model of domestic influences, and typology of international influences contribute to an understanding of the emergence, development, and implementation of cyberinfrastructure in the early 21st century. Although the chapter is primarily based on developments in, and the jurisdictions of the United States and Australia, some reference is made to positions and/or laws of the European Union and the United Kingdom to ensure a more comprehensive discussion. We conclude the chapter with a brief discussion of implications and a modest proposal for future research. Let us turn our attention to the first research question: What is cyberinfrastructure?

Defining Cyberinfrastructure

Although scholars have reviewed the definitions of related concepts, such as *e-science* (Jankowski, 2007; Schroeder, 2007b) and *collaboratory* (G. Olson, Zimmerman, & Bos, 2008), the definition of *cyberinfrastructure* is still unclear. Scholars in computer and information science, science and technology studies, and the fields of communication, sociology, and management have written about cyberinfrastructure based on a diverse range of disciplinary perspectives and agenda foci. Instead of picking the most cited definition, we believe a synthesis of existing definitions serves to bring several important insights together. We propose an integrated and generative definition of cyberinfrastructure based on its characteristics, layers, processes and outcomes.

Characteristics

Cyberinfrastructure can be characterized as data-intensive, computationally powerful, distributed, hierarchical, interoperable, and with second-order growth (i.e. generation of data about data and metadata). The first characteristic of data-intensive refers to cyberinfrastructure's capacity of hold a large amount of data in various forms, including numbers, text, multimedia, acoustic and nonverbal data (Poole, 2009). The goal of combining data sets among groups of researchers was a key driver of initial cyberinfrastructure development. Traditionally, science was limited by regional data, human resources, and the technological capacity of small groups of independent researchers at various locations. With cyberinfrastructure, researchers can combine multiple datasets into one that exceeds what a traditional small group of researchers can collect and analyze. Consequently, researchers can do science at a scale otherwise not possible.

Cyberinfrastructure is computationally powerful and has the capacity to analyze intensive data (Friendlander, 2008) via parallel and distributed computing processes. Traditionally, researchers executed computer analyses of scientific data in local laboratories, and research studies were limited by the processing speed and power of individual (or a small network of) commercial personal computers (PCs) or local supercomputers, if available at affiliated institutions. A supercomputer is a large network of powerful modular servers and commercial PCs run on parallel and distributed computing algorithms. Via this technique, a data-intensive job can be divided into small chunks and fed into individual servers and/or PCs (within a supercomputer architecture) concurrently and recursively, and then the results aggregated at the end of the computational process, thus increasing processing speed and capacity.

Cyberinfrastructure is a network of supercomputers across the country, such as TeraGrid, which connects 11 supercomputers across the US. Due to the combined computational power, cyberinfrastructure provides the fastest computational resources available, enabling science at a speed otherwise not possible.

As alluded to in the characteristic of computational power, cyberinfrastructure is a distributed platform. Via cyberinfrastructure, a group of researchers can submit a data- and computationally intensive job from a remote location, and have the job processed at multiple supercomputers, with the combined results returned back to the initiating location. The group of researchers is only required to have access to cyberinfrastructure through their local institution. The distributed characteristic of cyberinfrastructure takes research beyond local constraints to virtual computational resources at impressive speed.

Due to its complexity, it is logical to describe cyberinfrastructure as hierarchical. Cyberinfrastructure involves a range of large and small components, from a cable modem that can be picked up by a child to a supercomputer the size of a building basement. However, it is important to note that since cyberinfrastructure is a network it cannot function properly without its smallest component (Friendlander, 2008). Therefore, the smallest component also holds the entire infrastructure together, although it may be hierarchical in a physical sense.

In order for cyberinfrastructure to operate and function as a coherent whole, the scientific data, computational resources, technological systems, and human organizations must be interoperable. Interoperability (ACLS, 2009) refers to a property of cyberinfrastructure wherein a range of diverse data, resources, systems, and organizations inter-operate and work seamlessly together. Without interoperability, the former four characteristics reviewed have no value. Data sets, computer resources, computational jobs, and technological components will remain local, separate, and small-scale.

Given the aforementioned characteristics, cyberinfrastructure grows in its data overtime, leading to second-order growth. The aggregated scientific data and the human activities recorded on cyberinfrastructure are first-order data that can be analyzed by researchers. Careful coding, qualitative observations, statistical analyses, and network visualizations by these researchers yield second-order data (Poole, 2009) or metadata added to the existing cyberinfrastructure data repositories. This unique characteristic facilitates longitudinal research in a wide range of disciplines at a scale and fashion never possible before. Cyberinfrastructure grows in its potential for new discoveries by means of complex cross-referencing (Poole, 2009) to explore large-scale global challenges. In sum, cyberinfrastructure possesses the characteristics of data-intensivity, computational power, distribution, hierarchy, interoperability, and with second-order growth. Its complex make-up requires a careful explication of its different layers.

Layers

The second dimension of cyberinfrastructure is its four layers of hardware, software, agents, and interactions. The hardware layer can be further divided into the specialized/niche hardware and the general/commercial layers. Based on the discussion thus far, it is apparent that a key piece of the cyberinfrastructure puzzle is a network of supercomputers. Supercomputers

are mainly used for niche research analyses as described earlier, and specialized commercial applications, such as airplane design and automotive crash tests too big in scale and expensive for frequent trials and errors.

The specialized/niche layer of cyberinfrastructure also includes advanced instruments (Stewart, 2007), digitally-enabled sensors, observatories and experimental facilities (NSF, 2007), and large-scale data storage systems/repositories (Atkins, et al., 2003). These are examples of a range of physical hardware for specialized purposes and niche usage. Many of them, such as observatories, were uniquely built with specific utilizations in mind. In other words, these is hardware researchers cannot simply buy 'off-the-shelf'.

Beyond its specialized/niche hardware, cyberinfrastructure is also made up of a general/commercial layer of distributed personal computers (Atkins, et al., 2003), desktops (Friendlander, 2008), and portals (Poole, 2009). In addition to commercial PCs, cyberinfrastructure also includes phone devices (landline, mobile, and smart phones), fax machines, printers, modems, and other off-the-shelf electronic devices researchers concurrently use for non-research purposes. These hardware components, both specialized/niche and general/commercial, are tied together through a range of software applications.

The software layer mirrors the hardware layer in terms of its specialized and general applications. In order to process large-scale data and specialized analyses on supercomputers, researchers need appropriate analytic tools (Poole, 2009) and high-performance computing (HPC) applications. HPC applications are used by highly trained researchers. Loosely generalized, HPC applications enable parallel and distributed processing of large-scale data on supercomputers to generate scientific results. However, these results need to be shared with collaborating researchers and interested colleagues. This is where the next category of software applications comes in.

A range of information and communication technologies (ICTs) supported by telecommunication systems, the Internet, and World Wide Web make up another critical layer of cyberinfrastructure. Specific examples include email applications, net meetings, personal and organizational web pages, digital libraries, and search engines such as Google (Hai, 2004), and web 2.0 technologies such as blogs (Poole, 2009). These ICTs can be used by researchers for interpersonal, group, and organizational communication between their scientific and non-scientific work concurrently.

We suggest that human agents individual or collective, are key to an active cyberinfrastructure. Without users, an infrastructure by itself is not cyberinfrastructure (Ribes & Finholt, 2009) nor active but static. Although, the notions of people (Stewart, 2007), groups and organizations (C. P. Lee, Dourish, & Mark, 2006), and personnel and institutions (Atkins, et al., 2003) have consistently been mentioned in cyberinfrastructure literature. Human agents usually are assumed to be independent actors in the context of cyberinfrastructure. That is they represent 'nodes' in a network, as understood in traditional social network literature rather than vital components.

In contrast to human agents, nonhuman agents are also important in cyberinfrastructure. Nonhuman agents refer to documents, concepts, key words, data sets, etc (Contractor, 2009). They are somewhat discrete entities and resources (Friendlander, 2008) in the context of cyberinfrastructure. However, they are labeled as 'agents' because they appear to do things, or have impacts on other 'nodes' in the network. The notion of nonhuman agents departs from traditional social network literature and draws in actor network theory (Latour, 2005). However, human and non-human agents as nodes have no impact on each other or the overall cyberinfrastructure if they do not interact.

Human and non-human agents interact and are tied together through multidimensional networks. The notion of networks is not simply high performance grid networks (Stewart, 2007) and the Internet in the physical sense, but relationships and ties as commonly defined in traditional social network literature. Furthermore, the notion of networks is 'multidimensional', because nodes in cyberinfrastructure are both people and 'nonhuman agents' (Contractor, 2009). Networks therefore represent complex physical connections and relational ties among human and nonhuman agents in cyberinfrastructure.

A specific type of multidimensional network is middleware (NSF, 2007), which are computer software that tie multiple software applications together and allow them to interact in a parallel, distributed, and interoperable environment. We highlight middleware because it plays a significant role in creating key processes in cyberinfrastructure, which will be discussed next. Cyberinfrastructure consists of hardware, software, agents, and interactions. When the four layers are in actions, they create cyberinfrastructure processes.

Processes

There are two key processes of cyberinfrastructure: virtual environment and virtual organization. The first key cyberinfrastructure process is the technologically generated virtual environment (VE) (ACLS, 2009; Poole, 2009; Schroeder & Axelsson, 2006), which represents the continuously generated virtual space in which researchers interact with data. In the present development, virtual environment consists of visualizations (Stewart, 2007), simulations (Leonardi, 2009), and models (Monteiro & Keating, 2009). Based on HPC applications on large-scale data, researchers are able to use visualization techniques, interactive simulations, and computer modelling to analyze and predict complex scientific phenomena with significant societal and global implications. One example is real-time simulation on combined data from nearby locations that effect the development and expansion of a hurricane threatening a local community.

The second key cyberinfrastructure process is the socially generated virtual organization (VO). A VO brings a group of distributed researchers together for a common purpose and allows them to interact with each other. A VO is dispersed but coordinated, diverse yet coherent, and flexible and secured (Bird, Jones, & Kee, 2009). For instance, a VO for the Large Hadron Collider project brings about 2,000 researchers together across multiple countries. Embedded with the notion of a VO is interdisciplinary collaboration (Monteiro & Keating, 2009) and community-building (Poole, 2009). So far, cyberinfrastructure can be defined by its unique

characteristics, multiple layers, and key processes; however, it is most importantly defined by its intended outcomes.

Outcomes

Cyberinfrastructure emerged to promote three specific outcomes. The first outcome of cyberinfrastructure is that it increases productivity (Stewart, 2007). Productivity can be understood as the ability to do more in less time. Due to its intensive data and computational power, cyberinfrastructure can process larger data at faster speed than traditional personal computers and local networked machines. If nothing else, cyberinfrastructure increases the productivity of researchers.

The second outcome of cyberinfrastructure is innovation (Atkins, et al., 2003). Innovation refers to the ability to produce novel outcomes. Due to its intensive data and computational power, cyberinfrastructure enables research at a scale and speed never before possible, facilitating the exploration of complex phenomena at the edge of scientific frontiers. As a result, cyberinfrastructure enables innovations in research.

The third outcome of cyberinfrastructure is that of revolution (Atkins, et al., 2003; Stewart, 2007). Revolution can be defined as ability to cause a paradigm shift. With increased productivity and a stream of innovations, cyberinfrastructure stimulates a revolution in science, causing researchers to think of science differently, explore big questions, and work in new ways. Cyberinfrastructure also generates a new set of scientific practices (Monteiro & Keating, 2009). Once transitioned, researchers cannot return to their previous paradigm of doing science, thus effecting a mental and practical revolution.

Integrated and Generative Definition of Cyberinfrastructure

Taken together, cyberinfrastructure is data intensive, computationally powerful, large-scale, distributed, hierarchical, interoperable, and with second-order growth over time. It consists of specialized and general hardware, high-performance computing applications and information and communication technologies, human and nonhuman agents, all interacting and connecting through multidimensional networks. This platform facilitates technologically generated virtual environments and socially generated virtual organizations that orient people, data, and technology towards common goals. Cyberinfrastructure leads to increased productivity, breakthrough innovations, and paradigmatic revolutions.

At the heart of cyberinfrastructure outcomes of productivity, innovation, and revolution is the notion of ‘empowerment.’ Empowerment can be interpreted as the ability to mobilize people to produce, innovate, and revolutionize. In the influential Blue Ribbons Report, which led the US National Science Foundation to eventually establish the Office of Cyberinfrastructure in 2005, Atkins and colleagues (2003) articulate that cyberinfrastructure “should provide an effective and efficient platform for the empowerment of specific communities of researchers to innovate and eventually revolutionize what they do, how they do it, and who participates.” This vision is ambitious and bold, and reminds us of the initial emergence of the Internet as an information and communication network for scientists to share information and collaborate.

Following its public introduction, the Internet has become a political and economic phenomenon where multiple stakeholders wrestle to define what people do, how they do it, and who participates. Beyond proposing an integrated and generative definition of cyberinfrastructure, we intend to discuss the domestic and international influences that shape cyberinfrastructure emergence in the early 21st century. The second research question we explore is: what are they key political influences shaping its domestic emergence and development?

Proposing a Model of Domestic Influences

The emergence, development, and implementation of cyberinfrastructure is primarily a national effort. In this section, we propose a political model of domestic influences on cyberinfrastructure based on three interrelated forces: market, policy, and law, including differing impact of 'soft' laws (i.e. accepted policies or industry behaviors) and 'hard' laws (i.e. as found in legislation). We pay particular attention to the issues of digital divides (Hammond, 2002; Ypsilanti & Paltridge, 2004) and network neutrality (Wu, 2003) in the context of the Internet, and access to it and its services, because they have significant implications for the future market, policy, and law surrounding cyberinfrastructure. Whilst cyberinfrastructure effectively has no comparator, lessons may be learnt from the development of the Internet that will benefit the future development of cyberinfrastructure.

In the context of the Internet, digital technologies have radically changed how people interact, work, learn, engage politically, and spend their free time. As Benkler considers, "The change brought about by the networked information environment is deep" (2006, p.1) Whilst the development of computers from being a research tool to their wide adoption for private use occurred over several decades (Bresnan & Greenstein, 1999), it is anticipated that cyberinfrastructure adoption for commercial and private use will occur more quickly.

Two Critical Issues of the Current Internet

Digital Divides The term 'digital divide' has been used by authors to refer to a variety of gaps. As Gunkel (2003) considers these gaps include those representing the inequality in educational opportunities; the differences of opinions regarding engineering solutions; and the level of access to new technologies and a person's ability to use them. The digital divides of relevance to this chapter are those jn respect of the gaps between people who have effective access to and are able to utilize the Internet and those who do not. These gaps are often defined through the categorization of users by their socioeconomic status and generation and education levels. Although digital divides exists between countries at the global level, we primarily focus on its domestic manifestation.

The Internet now enables a wealth of information to be available to all at the touch of a button. One divide that exists is that not all people in all countries are able, for reasons of government policy or their own lack of means; or in some cases lack of desire, (Crump & McIlroy, 2003) to access this information. Given the ubiquity of the Internet and information technologies, there is the risk that these people will be disadvantage in the future without the

access to digital information for the education, work and social activities and engagement (Crump & McIlroy, 2003).

The ability to access information by itself is but one divide. The other of relevance to this chapter exists between those who are digitally literate and those who are not for merely being able to access information is not the same as being literate, which to an extent involves the ability to communicate with others (Cole & Lorch, 2003) beyond the abilities to read and write (Buckingham, 2007). This is an important distinction to draw for digital literacy.

To be digitally literate, similarly to being literate generally, is more than simply being able to access information on the Internet. Utilizing Prensky's (2001) terminology, for the sake of ease of description only whilst appreciating that it is a starting point and merely representative of broader and more complex issues, we suggest that 'digital immigrants' must quickly become digitally literate if they are to do more than merely exist in the 21st Century. They need to acquire the communication norms and social rules of the cyberspace in order to co-exist with the 'digital natives' (Prensky, 2001) for whom digital information and computer-mediated communication are an integral part of everyday life. In other words, digital immigrants must learn how to study digitally; to read and contribute to blogs effectively; to send tweets appropriately; to visit virtual worlds competently; and to create and read texts and emails meaningfully.

Prior claims that education will exponentially and significantly improve with the introduction of the Internet (Jankowski, 2007) have not in fact been realized. They will not be until everyone is able to access it from anywhere with digital literacy (Tapia, Blodgett, & Jang, 2009). Beyond education, the digital divide also restricts access to vital governmental services, leading to what some have referred to as the "participation divide" (Goldfinch, Gauld, & Herbison, 2009 p. 335). Therefore, the need to boost participation, as identified by La Rose (2007), rises to the top of policy agenda in a 21st century society. How is the lesson of the digital divide applicable to the case of cyberinfrastructure?

The key implication of the current digital divide for cyberinfrastructure is how to avoid creating another form of (digital and participation) divide while at the same time ensuring the current one is overcome without sacrificing the needs of all users in the current system (Tapia, et al., 2009). In the case of cyberinfrastructure, literacy involves acquiring the skills and knowledge to remotely access supercomputers and high-performance computing applications with advanced computer programming techniques, along with the skills to manipulate large-scale data. Given the specialized layer of cyberinfrastructure defined earlier, most digital immigrants and digital natives of the Internet are considered 'immigrants' to cyberinfrastructure. As the specialized layer of cyberinfrastructure continues to develop rapidly, a second-degree digital divide is likely to emerge. That is, the ability and/or means to use cyberinfrastructure, or rather the lack thereof, will impact not just ordinary users but also sophisticated ones without the necessary means or skills. A second-degree digital divide will have a detrimental impact on the vision of cyberinfrastructure as an effective and efficient platform for the empowerment of what people do, how they do it, and who participates, beginning in and with the scientific community. Given this anticipation, appropriate access and educational policies need to be developed to prepare and speed immigration of all users to cyberinfrastructure in the 21st century.

Within the US, an example of such policy building has emerged in the form of the Broadband Technologies Opportunities Program drafted as part of the economic stimulus bill initiated by President Obama (Tapia, et al., 2009). However, as Tapia et al. establish, there are many competing groups for limited cyberinfrastructure funds, which may require the creation of a two-fold government policy. As well as distributing funds to research and scientific groups for cyberinfrastructure projects, consideration must also be given to increasing the ability of all individuals to be connected to high speed broadband internet. An important aspect of overcoming the digital divide and ensuring widespread and ongoing access to a network is to ensure that government policy appropriately addresses the issue of network neutrality (Endres, 2009).

Network Neutrality The issue of network neutrality gained serious public attention in the US in 2002, about the same time as cyberinfrastructure started to gain momentum in the scientific and research community. However, network neutrality has been debated for several years in the US, the UK, Germany, Italy, and Japan with little to no connection with the parallel cyberinfrastructure development. As the issue has progressed, many policymakers and lawyers are interested in finding appropriate solutions for network neutrality in the context of the Internet.

Although its complexity makes definition difficult, (Cave & Crocioni, 2007), network neutrality could be defined as preventing Internet providers from blocking, speeding, or slowing web content based on its source, ownership, or destination (Internet, 2009). Currently, network operators around the world engage in various discriminatory behaviors to control what is been sent over the Internet networks, with new technologies that discriminate between different applications; that is Internet carriers will examine the packets (data) sent, see what application/s it comes from and tier your access based on that analysis. For example, one way this discrimination may occur is that a 'black box' may be installed in the network as a packet sniffing technology in order to recognize and decode certain packets of interest within network traffic (Dierickx, 2006) for the purposes of selective de-/prioritization.. A lack of network neutrality means service providers (who are also access providers) can act to prevent users' access to their competitors' services, or can work to make that access less effective.

At the heart of the debate is the 'openness' of the Internet for those seeking lawful access to contents and services. Network neutrality simply requires network operators not to distinguish between data packets, whether in the form of a text, video, chat or any other format, and to push them through their pipelines at the same speed (Editorial, 2009). Network operators such as telecommunication and cable companies argue that they should be able to provide preferential treatment to online companies willing to pay for their data packages to be transferred faster than others. The profit from such arrangements will allow telecommunication and cable companies to further develop advanced fiber-optic networks and increase broadband access to more users. Moreover, they argue that discrimination is needed to protect their users against spam and other security threats, and to insure the quality of VOIP services (Cerf, 2006). These arguments constitute the principle of network diversity.

However, there are three arguments for network neutrality and against network diversity in the form of discriminatory control by network operators. First, network neutrality prevents

anticompetitive practices by cable and telecommunications companies, which enjoy a domination of the market (Berner-Lee, 2006). Second, network neutrality will help promote Internet innovation, no matter how big or small, by allowing everyone to be a creator, speaker, and broadcaster (Balkin, 2006). Third, enforcing neutrality ensures the free flow of information and will prevent the evolution of a two–tiered system in which service providers could inhibit or prioritise the transmission of data based on what is good for their own business, not what is in the users' best interests (Editorial, 2009). The network should treat all content, sites, and platforms equally (Wu, 2003). The lack of network neutrality presents a serious and real threat to the Internet and its future "as an open network" (Berner-Lee, 2006).

The open architecture of the Internet allows users to publish their work without payment of fees, and without seeking permission from anyone. This is changing with network diversity that differentiates between packets and changes the underlying architectural design of the Internet. As well as the Internet rests on foundations of openness, most technology is not developed in isolation as a new technology but builds on prior technologies. The suggestion therefore is that a completely independent technology is not possible (Nakamura, 2000) as without the openness of the Internet for sharing, learning, and experimenting, many of the services we currently take for granted would soon cease to exist (Johnson, 2009).

Instead of debating the principles of network neutrality or network diversity, Zittrain (2006) argues for looking at these principles as a 'means' in and of themselves rather than an 'end.' He challenges common understandings of the architectural design of the Internet and focuses on fundamental issues associated with upholding principles of openness. Lessig and McChesney identify some of these key issues:

> Most of the great innovators in the history of the Internet started out in their garages with great ideas and little capital. This is no accident. Network neutrality protections minimized control by the network owners, maximized competition and invited outsiders in to innovate. Net neutrality guaranteed a free and competitive market for Internet content. The benefits are extraordinary and undeniable… (Lessig & McChesney, 2006)

This argument for a free and competitive market that fosters innovation can be extended to cyberinfrastructure. As defined earlier, cyberinfrastructure ideally envisions an effective and efficient platform for the empowerment of what people do, how they do it, and who participates. Currently, cyberinfrastructure operation, such as the case of TeraGrid in the US, is supported by multiple academic supercomputer centers and national research laboratories. In the case of EGEE in Europe, it is supported by many supercomputer centers across multiple countries. Many of these supercomputer centers are supported by governmental funding and cyberinfrastructure is not yet commercialized. However, commercial and corporate involvements in cyberinfrastructure development and implementation are increasing. Drawing from the parallel comparison between the Internet and cyberinfrastructure, appropriate funding and commercial policies need to be developed to ensure an open cyberinfrastructure platform with minimum or no domination or monopoly by specific supercomputer centers, access operators, or countries.

The choices we make today in connection with how we should run the Internet network are critical for its future and that of cyberinfrastructure. Appropriate access, educational, funding,

and commercial policies need to be developed to reduce and possibly avoid the issues of digital divide and network neutrality being replicated within cyberinfrastructure. In order to help guide this preventative effort, we propose a political model of how market, policy, and law may regulate the emergence and development of cyberinfrastructure.

A Political Model of Domestic Market, Policy, and Law

Our examination of market, policy and law and how they can impact the case of cyberinfrastructure begins with a consideration of three fundamental issues that must be kept in mind. First, in most societies, disputes and conflicts of interests are resolved in terms of norms and standards. In making any decision, reliance is placed by the parties involved on the rules and principles provided by statutes and precedents (Boulle, 1996). As stated, although cyberinfrastructure has no comparator, lessons from the development of the Internet deserve consideration. The issues of the Internet digital divide and network neutrality, and how they are dealt with by the market, policy and law, will directly influence how cyberinfrastructure will be regulated by the market, policy, and law. However, how courts interpret and apply the law (which tends to be focused on their specific jurisdiction only) will also influence cyberinfrastructure policy development, as judicial interpretations, and thus precedents, will vary from jurisdiction to jurisdiction.

Second, the preferred method for policy and legislation development is to be proactive in dealing with an issue before it develops, such as the projected implications of the digital divide and network neutrality on cyberinfrastructure. However, governments more often than not take a reactive approach to the development of policy and legislation, doing so in a manner that Beardsley and Farrell (2005, p. 2) refer to as "trial and error [by] confusing economic goals with political and social ones." A reactive approach can, regretfully, allow an issue to continue well after it was first identified. Also, without a 'global legislator' (Benvenisti, 2008), it is left to the separate jurisdictions to determine what appropriate cyberinfrastructure policy is and to develop and implement it through domestic law. This is a concern, as there is a real risk that there will be inconsistent policy adoption and implementation which may adversely impact upon cyberinfrastructure's future developments and collaborations. How various governments perceive their position in developing and creating laws, and determine which entities are to be regulated by those laws, is a real concern as there is a potential for conflict (Burk, 2007). In particular, the potential issues of the digital divide and network neutrality for cyberinfrastructure should be clearly identified and proactively addressed by early policy development to enable them to be resolved before they become issues in fact.

Third, changes in society are continual (Gibbs, 2000) and these changes affect both the Courts (Cranston, 1986) and the law in that policy, and thereafter the law, generally develops in response to those changes (Gibbs, 2000). One issue that requires specific consideration for any cyberinfrastructure project is in relation to ownership and rights to any resource created. One solution may be to determine that the resources created would be made available to all by means of open licensing (Fitzgerald and Pappalardo, 2008). However, this is unlikely to be a workable option in practice, due to the interests of funding bodies (David and Spence, 2008). Other legal issues arise with respect to the legal relationships between the parties; the need for the

apportionment of liability for any risks arising from the project, and how this is dealt with by the various domestic laws; as well as the need to ensure compliance with anti-trust laws (David and Spence, 2003, 2008).

A concern is to ensure the ability of policy and laws to easily change and develop as society does (White, 2008). For cyberinfrastructure, this requires ensuring that any law and policy is both internationally consistent and also technology neutral, so as to encompass all future developments and thus maximize the prospects of the law's enforcement. This would be difficult to achieve practically, but even if it was another challenge arises. As the society within each jurisdiction is unique, any changes wrought by one society, which then require implementation into policy and law, are likely to vary from jurisdiction to jurisdiction. This could lead to a situation where whilst an activity is currently treated consistently by all jurisdictions, in the future, as has occurred with some intellectual property laws (Middleton, 2008), the same activity could be permitted in one jurisdiction but prohibited in another.

As Unsworth (2008) identifies, cyberinfrastructure "… is the infrastructure for a knowledge economy…" (p. 40) but it is also both "…a scientific challenge [and] … a social and human challenge…" (p. 42) Therefore, in order to create appropriate and durable policy and law for cyberinfrastructure, it is necessary to ensure that policy is not created in isolation. That is, it must *not* be created by one jurisdiction only, in isolation from true input from all other jurisdictions; *nor* created by one interest group only in isolation from true input from all stake holders. Proper cyberinfrastructure policy and law development will require a multi-disciplinary, multi-jurisdictional, open and accountable process. Policy development is also influenced by, and in turn influences, the operation of the market and the law. We propose a model detailing this relationship as follows.

Market drives policy. The demand for appropriate infrastructure and policy generally is driven by demand for services, although there are exceptions to this observation (such as in the case of Google or Facebook, where the service itself creates its own market; and in the case when specialist advice is required after taxation policy and laws have been changed, therefore the policy itself creates the need for the service). When there is a market demand for services, restrictions on consumer choice and thus on network neutrality can arise both by means of technological prevention and/or by means of contractual obligation. Policymakers and regulators are therefore required to balance the benefits technology brings against possible methods by which it may be used inappropriately - to decide how and if choices should be restricted in order to address what others refer to as "…'High Tech' competition technology" (Depypere, 1995)

Moreover, the market is crucial in imposing a simultaneous constraint upon how an individual might behave in cyberspace through the price they exact (Lessig, 2009). An example of this market mechanism is the price of software constraining the ability of 'netizens' to use it on the Internet and communicate with others. Lessig (1999) has identified fours modalities of regulating behaviors in cyberspace: through law, norms, market, and code (Buckingham, 2007) (architecture), or any combination of them.

On the other hand, public policy is based on consistent principles and supported by enduring values in the society (CEDA, 2006), but is often influenced by market demands at the

same time. In order to incorporate these principles and values, policy development should involve all relevant parties and follow a clear policy framework, which is implemented in the market rigorously and systematically by means of the adoption of clear and accountable processes (M. Edwards, 2001, p. 3). Edwards suggests a useful framework adapted from the Bridgman and Davis model. This policy development framework utilizes the following six stages: issues identification (problem definition and articulation), policy analysis (data/information collection, objectives/questions clarification, and options/proposals development), consultation, decision, implementation, and evaluation.

Under the influence of the market, the process of policy and legislative implementation can be costly and time consuming (CEDA, 2006) as it may be necessary to revisit earlier policy development stages in Edward's (2001) framework before it is possible to move forward. In addition to the direct influence of the market, the "…electoral cycle can play a large part in determining what items get on the agenda and whether they are pursued past a certain point" (M. Edwards, 2001, p. 10). A clear example of this, and the impact of a change of government has on policy, was seen in Australia after the 2007 federal election, when significant aspects of the previous coalition government's broadband policy and projects (for example the OPEL contract) were "discontinued" (Department of Broadband, 2008). Overall, the economic market, along with cyclical political influence, drives policy.

Policy drives law. The ultimate object of policy is the creation of a norm by which societal behavior is regulated – that is, the creation of law. As Holland (2006) explains, the objects of "…[l]aw are the creation and protection of legal rights," which he defines to be the "…capacity residing in one man of controlling with the assent and assistance of the State, the actions of others." (p. 66). Law making is a process that involves a variety of actors, including "…government ministers, and public servants, as well as experts such as academics and others in the community" (M. Edwards, 2001, p. 1). Law is essentially the ultimate implementation of developed policy into practice.

Furthermore, written law (i.e. that created by the legislature or parliament as opposed to judge-made law) is not developed in isolation. It requires the impetus of government or society and usually arises from the need to address something that is 'missing' (i.e. not addressed by current law) or an issue has arisen since existing laws were written, and not addressed by those laws (Heydon's Case, 1584, p.637). The law does not exist in a vacuum, and as such, any proper analysis requires that a law and its underlying policies be examined where, and why, it operates (Murray, 2007). A good starting point is to ask - What is the purpose of this law? The policy process therefore commences with an accurate identification of the objective/s to be addressed (M. Edwards, 2001, p. 2). In this regard, policy drives law.

Law drives the market. In return, the law affects the market as a modality of regulating cyberspace, by using taxes to increase or reduce market constraints on certain behaviors and activities. The market could play an important role in regulating cyberinfrastructure when and where laws are not comprehensively put in place to regulate it. Initially this may not appear to be such a problem, as most cyberinfrastructure is funded by government, however, learning from the experience of the development of the Internet, after cyberinfrastructure becomes a public domain (even though this may be many years off) attempts at regulation are likely to be highly

ineffectual. Furthermore, governments are also concerned with the enforceability of the laws they implement (Burmeister, 1999; Coughlan, Currie, Kindred, & Scassa, 2006), as without an effective means of enforcement, any law implemented is arguably not worth the paper it is printed on, is of no use to regulators, and of no comfort to consumers.

However, the influence of the law on the cyberinfrastructure market is, for the time being, different from the impact of the law on the Internet market. That is because cyberinfrastructure is a bespoke (mostly for e-science) and artisan (sometimes for digital humanities) product due to its newness, whereas the Internet is a commodity product. The Internet became widely diffused because personal computers and home computing suddenly became much cheaper and therefore more available to both businesses and consumers and networking capability was achieved (Crandall & Jackson, 2001). Moreover, there are many service operators and suppliers for Internet access at very cost effective prices. This ease of availability impacts on network neutrality, as consumers expect and demand a level of access unrelated to the ISP used. If consumers want to change the commodity used, they are able to easily change service operators and suppliers.

Conversely, cyberinfrastructure is so new and specialized it is not yet possible to 'buy it off the shelf.' Cyberinfrastructure is a bespoke/artisan product that is yet to be commoditized and commercialized, and have its services mass-produced and as such has not yet reached the networking capability of the Internet. How we approach policy development and legal regulation for cyberinfrastructure needs to be undertaken differently and, it is suggested, with more forethought and wider consultation. Nonetheless, when everyone is able to easily access cyberinfrastructure enabled processes such as virtual environments and virtual organizations through a portal, as defined as a part of cyberinfrastructure's general layer, we are likely to witness the commoditization of cyberinfrastructure portals and cyberinfrastructure services in a similar fashion to that of the Internet.

For many jurisdictions, the digital divides and network neutrality are critical issues that shed light on the rapid development and future implementation of cyberinfrastructure as we move into the second decade of the 21st century. Appropriate and proactive policies, as they are influenced by market and the law, need to be developed with forethought and wide consultation to reduce or prevent similar impacts and ensure openness and empowerment. In the meantime, we must also consider that any over-regulation could restrict creativity.

We have described a political model of cyberinfrastructure implementation based on market, policy, and law. It is important to note that where the conduct to be regulated or the product to be protected will have an impact on the international stage, it also requires international collective policy making. Moreover, from an international perspective herein lies a problem, as although the behavior constituting a breach of law may not fundamentally change from jurisdiction to jurisdiction, each jurisdiction likely identifies or describes the same act in a slightly different manner, and consequently legislates in a slightly different fashion to address it. These international aspects highlight the need to expand the discussion to the international arena. As such, what are the key challenges impacting cyberinfrastructure's international implementation?

Describing a Typology of International Influences

Cyberinfrastructure is not an isolated national effort. Given its rapid emergence and steady development, the vision of an all-encompassing digital system evolving into an 'E-topia' (Mitchell, 2000) and "global innovation system" (Schroeder, 2007b, p. 3) may soon be witnessed internationally, as evidenced by the fact that the grid network infrastructure in Europe spans more than 30 countries (Bird, et al., 2009).

Further, there is much investment internationally in cyberinfrastructure. The U.S. National Science Foundation established the Office of Cyberinfrastructure in 2005 (Seidel, et al., 2009) and the U.S. government allocates about $175 million annually to develop and maintain its national cyberinfrastructure (P. Edwards, Jackson, Bowker, & Williams, 2009). The U.K's Office of Science and Technology implemented a large funding initiative in 2000, and spent about £275 million between 2001 and 2006 in a similar effort (P. Edwards, et al., 2009). The Australian e-infrastructure investment plan, represented by the Platforms for Collaboration capability area, had a notional $75M allocated to it by the end of 2006, out of the total NCRIS budget of $542M (Reid, 2007). The vision driving these investments is cyberinfrastructure's potential to improve cutting-edge research and enable global collaborations (Fry & Schroeder, 2009).

However, whilst cyberinfrastructure development clearly has government support, as identified previously, there is not currently an international policy, regulator, or legislature. Cyberinfrastructure policy and legal development is therefore left to the individual jurisdictions to manage by themselves, or preferably by means of international treaties and/or cooperation. The power of individual governments to create policy and laws, and the processes that they must follow, will impact upon what is ultimately (able to be) developed.

For example, the Australian government has the power to make laws for peace, order and good government within their jurisdiction (Constitution, Sec. 51), and its power to legislate, as Gleeson CJ observes, '…includes a power to makes laws with respect to places, persons, matter or things …external to – Australia' (XYV v Cth, 2005, p. 499). Proposed legislation and subordinate regulations are required to be approved by both the House of Representatives and Australian Senate before they become a law. The power in the U.S., however, is found in both the legislative Congress and the executive branch headed by the President, which provide many of the same facilities as the Australian government. However, these initiatives are often undefined until approved by both the congress and president. Before this occurs they remain open in their scope, allowing for many of the details regarding the implementation of the law to be worked out by the state and local governments, or through government-run organizational branches such as the National Science Foundation or National Telecommunications and Information Administration (Tapia, et al., 2009). This could lead to uncertainty and inconsistent policy development.

Aside from the issue of the lack of one consistent policy and law, the issue of how an international cyberinfrastructure project is to be properly regulated is of concern where actions and actors are located in multiple jurisdictions (Burk, 2007), and any alleged breach of law may occur in one or many of those jurisdictions. For example, an Australian Court may restrain

conduct occurring outside the territorial boundaries of their jurisdiction; however, whether it does so is a matter of discretion for the Court (Helicopter Utilities, 1963; Dunlop Rubber, 1921; Tosier, 1885). In exercising this discretion, Australian courts must determine whether they are a 'clearly appropriate' forum (Voth, 1990) in which to determine the matter. Further, even if the Court determines it is the appropriate forum within which to determine the matter, it may be that it will not grant an order that the Court knows is unenforceable (Macquarie v Berg, 1999). Conversely, in the U.S., the Court must consider '…whether Congress intended extraterritorial application of the statute proscribing the alleged conduct' (Messigan, 2006). Due to the nature of operation of the American federal government, any extraterritorial actions require not only approval from the presidential seat but also from the congressional legislature. Even then, such actions and decisions are subject to review by the federal court, to determine if the actions taken are both within the realm of established common law as well as supportable under the Constitution, to ensure that any actions meet not only the founding ideals of the nation but also promote and support cooperative habitation with other states.

Although it may be difficulty to achieve (as identified earlier), harmonization of policy and laws regarding cyberinfrastructure may be one means to address any international issues that arise from inconsistent policy development or legal application. The EU, for example, embraces harmonization of laws through Article 5 of the EC Treaty where, by means of the principle of subsidiarity, the EC is able to adopt measures at a community level where the objective of a regulation cannot be sufficiently achieved by member States, and where, by reason of the transnational nature of the offence, regulation can be better achieved at the community level. However, as can be seen from the European experience, working toward harmonization of policy and laws can take some time, and is not always successful in practice.[i]

However, the EU appears to have achieved a level of harmonization with regards to cyberinfrastructure. In June 2009, the European Commission, pursuant to Article 171 of the EC Treaty which gives the Community power to *"...set up joint undertakings or any other structure necessary for the efficient execution of Community research, technological development and demonstration programmes"*, adopted a specific regulation to enable the establishment of European research infrastructure consortia (referred to as an ERIC) (Commission, 2009). The establishment of this legal framework gives us confidence that, with regards to cyberinfrastructure at least; many of the international challenges identified earlier can and will be overcome in the not too distant future.

However Murray's (2007) observation regarding the impact of any one State's laws on harmonization generally remains pertinent, in that '…a distinctive set of legal principles in any one nation can undermine the effectiveness of law as a regulatory tool in an international environment…'. In order for there to be true harmonization of policies internationally and not just within the EU, all countries must have the same approach to their regulation of the actors and their multijurisdictional activities.

The desire for consistent policy and application must also be considered in the light of a recent observation by Benvenisti (2008) that some governments are increasingly "…consciously try[ing] to disengage from traditional law", in that they prefer informal means of commitment as opposed to establishing formal international organizations and treaties. Finally, others negatively

(but perhaps realistically) view internationalization as an '…Americanization of the law…' (Michaels & Jansen, 2007). We are not taking a position on this matter but raise it simply as an observation from the literature. Essentially, we present a tension between harmonization and conformity at the international policy arena without advocating for a preference. It is simply an inherent tension that needs to be managed appropriately.

Additionally, despite much enthusiasm, cyberinfrastructure projects face international challenges, which are compounded in implementation by national specific issues, and common project challenges which are compounded in practice by project specific issues. We present a typology of challenges based on these three general categories with eight specific examples.

International Challenges. The first international challenge involves working with technological diversity and choices that must be determined before cyberinfrastructure projects go forward. International cyberinfrastructure projects can be adversely impacted by differences in the speed and data carrying capacity of national communication backbones, which vary greatly from one nation to another - even in countries that share a border (J. Olson, Ellisman, James, Grethe, & Puetz, 2008; Petrazzini & Kibati, 1999). Software used also often varies greatly between one country and another, as well as the hardware that is available to run current or developed cyberinfrastructure (Ackerman, Hofer, & Hanisch, 2008; Taskforce, 2005). International projects can be further complicated by the requirements set by national governments regarding the types of software that must be used in their research labs and governmental agencies. For example, Venezuela has a orientation towards open source software (Maldonado & Tapia, 2007).

The second challenge for international projects arises from the difficulties surrounding data storage for data produced or collected during an international scientific project (Arzberger, et al., 2004). Currently, data in such projects is often stored on the site that has the faster connection or largest data storage (Hofer, McKee, Birnholtz, & Avery, 2008). This arrangement creates a bias in favor of more developed nations when collaborations span very diverse countries, as it allows more developed nations to dictate how the data is stored, the times and methods through which it may be accessed, and generally privileges those countries in terms of travel and accessibility benefits.

The third challenge to international implementation is the lack of a standard implementation policy. There are many cyberinfrastructure projects spanning national borders that need to work with the continuing struggle of setting policies about how the project is coordinated, how credit and work are distributed, how risk is managed, how results are owned/shared, and how international and national regulations are handled. Often, each project is responsible for answering these questions for themselves. Currently there are no set international policies regarding collaboration on a multinational project that engages with cyberinfrastructure (Lynch, 2008). However, while these policies do not currently exist, there are international initiatives, many arising from collaborations like the Large Hadron Collider (LHC), regarding the creation of such a policy. Two things that many of the participants in these primordial international policies seek to address are the issues of the digital divides that were raised earlier in this chapter (Lynch, 2008).

National Challenges. The fourth overall and first national specific challenge is imposed by national security concerns and the resulting increased costs to address the various concerns. For example, cyberinfrastructure project data often requires particular devices and software that are not accessible in areas outside of a single nation. Transportation of agents from one location to another can incur additional costs to an international project. In many cases, negotiations between the different agencies and governments involved in the project must be opened to discuss issues of visas and national security issues (Arzberger, et al., 2004). In some cases, workarounds to this problem have been found through the further implementation or careful expansion of the current cyberinfrastructure, to allow for greater remote access to equipment and data (Ackerman, et al., 2008; Myer, 2008; J. Olson, et al., 2008). However, this workaround arrangement is not yet standard in international cyberinfrastructure projects.

The fifth challenge involves the funding arrangement adopted. International projects are often collaborations which draw their funding from various political entities such as the United Nations, countries like the United States or France, and multinational governments such as the European Union (Borgman, Wallis, Mayernik, & Pepe, 2007). Each of these entities wish to gain something from the results of the research, as well as position themselves well in the international community as centers of science and research (Borgman, et al., 2007; Hofer, et al., 2008). This can put further pressures on international cyberinfrastructure projects as they attempt to include the entities' funding requirements in the goals and basis of the research project (Taskforce, 2005). This could result in any number of changes and can cause some project decisions (such as what software to use, how and where to store data, where research centers are located, and how time at the centers is divided), to become political decisions of national and international significance.

Although these five challenges involving technological choices, data storage, national security, and funding arrangement are particularly salient in national cyberinfrastructure projects where projects are influenced by the participants' desires, similar issues may also arise at the international level, as these projects are influenced by the participants' home jurisdictions' desires. In other words, such dynamics manifest themselves in most national and international cyberinfrastructure projects, although they appear magnified at the international level. The effects of these challenges are further compounded by the three common project challenges in our third category.

Common Project Challenges. The sixth challenge overall and first common project challenge is related to scientific communication practices, such as the setting of standards for communication, interaction, and documentation in international cyberinfrastructure projects. Scientific research groups often improvise standards for routine communication. However, these standards must be negotiated between the different members and power structures that exist in distant teams (C. Lee & Tibbo, 2007). A common problem cited by such project members is the passing of data and papers from one team/member to another. Currently, teams have a wide variety of technologies to choose from, such as concurrent versions system (CVS), email, files, and file servers, to name just a few. Who is allowed to access and work on data, or publish from particular subsets of data must also be discussed to avoid complications (C. Lee & Tibbo, 2007). This can often be another downfall of data within projects being centrally located at one team's site, establishing them as gatekeepers who can determine what projects or information should be

handed out or published, and which members of the team should be allowed to do so (Fry & Schroeder, 2009).

The seventh challenge involves internal knowledge management. The nature of many international cyberinfrastructure projects also elevates the need for compatible documentation policies and technologies – that is, interoperability of systems and processes. Since these projects can often span many years, much longer than a single graduate student, research assistant, or even investigator may stay at a organization, documentation makes it possible for the knowledge, process and policies established during the course of the project to be transferred from one researcher to another as the working staff of the project changes. However, international differences can often make the keeping of such documentation difficult (Taskforce, 2005). Preferences for the type of document technology used (text files, data repositories, videos, lab notes, etc.), as well cultural idiosyncrasies (beyond the scope of this chapter to consider), can often render this valuable information difficult to access or understand (due to variances in dates, times, measurements, what information is recorded, etc.) (Lynch, 2008).

The eighth challenge arises in respect to the background of the researchers involved. Many CI projects are composed of researchers from different areas and disciplines of research (Lynch, 2008). This can further complicate existing tensions within international teams, as groups within the project vie to establish their interests as dominant among the research goals. A classic example given by Myer (2008) is the competition between computer scientists wishing to study the development of the CI programs used in the Pacific Northwest National Laboratory and the physicists who were using the CI to study energy. The tension that arises in such groups often exists because each group in invested in the project for a specific set of goals. In Myer's example, the computer scientists were most invested in pushing the boundaries of advanced remote presence and collaboration technology and software, while the physicists wished for an established and reliable set of tools which they could then use to focus on their own goals of studying energy consumption and usage.

These are merely some of the most common challenges faced by international cyberinfrastructure projects. Each project faces a number of unique difficulties that arise out of the combination of countries, institutions, researchers, and goals that make up that particular project. While many of these issues must be faced on a one-by-one basis, the establishment of international standards and policies for collaboration on large-scale scientific research and the creation of cyberinfrastructure would ease the process of establishing a project for many future efforts.

Conclusion & Implications

As set out in the beginning of this chapter, the time is ripe to explore three interrelated research questions: What is cyberinfrastructure; what are they key policy influences shaping its domestic emergence and development; and what are the key challenges impacting its international implementation? We provided some preliminary answers to these important questions.

What is cyberinfrastructure? Cyberinfrastructure is data intensive, computationally powerful, large-scale, distributed, hierarchical, interoperable, and with second-order growth over time. It consists of specialized and general hardware, high-performance computing applications and information and communication technologies, and human and nonhuman agents, all of which interact and are connected through multidimensional networks. This platform facilitates technologically generated virtual environments and socially generated virtual organizations that orient people, data, and technology towards common goals. Cyberinfrastructure leads to increased productivity, breakthrough innovations, and paradigmatic revolutions.

What are they key political influences shaping cyberinfrastructure's domestic emergence and development? The political process through which domestic policies are made is complex. We propose a cyclical model to describe how the market drives policy, policy drives law, and law drives the market in return. This model helps us understand the key domestic influences shaping cyberinfrastructure emergence and development, especially with regard to the issues of the digital divides and network neutrality.

In the case of cyberinfrastructure, the digital divide presents the tension between the wish to advance technology on the edge without creating another layer of access and participation division. Network neutrality reveals a further tension between the need to build more advanced and secure infrastructure without limiting creativity and innovations. Both issues have critical implications for cyberinfrastructure's vision of empowering what people do, how they do it, and who participates. Based on observations and lessons learned from the case of the Internet, we suggest early and proactive policies in the area of access, education, funding, and commercialization, to reduce and possibly avoid the effects of the digital divide and network neutrality in the case of cyberinfrastructure.

What are the key barriers impacting its international implementation? We describe a typology of international challenges based on three categories: international specific challenges, nationally based challenges and common project challenges. Key challenges include technological diversity and choices; international data storage decisions; lack of standard implementation policy; national security concerns; and funding arrangements. These challenges are amplified by three common project challenges: inconsistent scientific communication practices, incompatible internal knowledge management strategies, and diverging disciplinary interests. These challenges collectively point to the fundamental challenge of a lack of international standard policy to guide cyberinfrastructure projects at the global scale. In practice, there is no 'global legislator' in the world. International cyberinfrastructure projects will have to balance the tensions of harmonization and conformation with the domestic law of big and small countries.

Future Research

As we look into the future of cyberinfrastructure, there are nine key focal points we believe would advance our understanding of this important development. First, research could document cyberinfrastructure emergence, such as what social, economical, political, and technological forces collectively led to the emergence of cyberinfrastructure in the early 21st century. Second, research could explore the design of cyberinfrastructure, especially the co-

production between scientists as users and computational technologies as developers, as they co-design different pieces of cyberinfrastructure together. Third and similar to design-focused research, we could also pursue the process of development, especially with regards to the organization of cyberinfrastructure projects and related socio-technical dimensions of development, as they involve stakeholders such as funding agencies, supercomputer centers, policy institutions, and commercial vendors, in addition to users and developers.

Fourth, the process of adoption at both the individual and organizational levels deserves critical attention, as an infrastructure without individual and organizational users would be a major problem. Fifth, and in the beginning stage of adoption, research could track how cyberinfrastructure is used to support implementation at the micro level, such as distributed collaborations among teams of scientists and users. As the number of users grows and distributed collaborations begin to overlap, research could address the sixth focal point of virtual organizing/organizations at the macro level of deployment.

Seventh, future research could also track the impacts of cyberinfrastructure adoption and implementation on individuals, groups, organizations, communities, societies, and the world. In the next few years, as the concept of cyberinfrastructure continues to emerge, the eighth focal point suggests exploration of the roles of supercomputer centers as service providers, infrastructure operators, and access regulators in open science, similar to the roles of ISPs in the case of the Internet and the information world. Ninth, and finally, when access to cyberinfrastructure becomes possible through commercial portals and cyberinfrastructure's funding mechanisms go beyond primarily governmental investments, future research could investigate the commercialization of cyberinfrastructure services as a public commodity beyond being a bespoke/artisan product.

Predicting the future of cyberinfrastructure and related research is problematic, as is most IT predictions, particularly in view of the specific and common challenges we have identified. Cyberinfrastructure is a complex and constantly developing phenomenon. Future researchers need to take into consideration the historical, political and cultural context in which it has and is developing. What is clear however is that the future will be more certain if nations and disciplines work together to achieve it, as this multi-national, multi-disciplinary, and multi-time zone team have worked together to write this chapter.

References

Ackerman, M., Hofer, E. C., & Hanisch, R. (2008). The National Virtual Observatory. In G. Olson, A. Zimmerman & N. Bos (Eds.), *Scientific Collaboration on the Internet* (pp. 135 - 142). Cambridge, Massachusetts: The MIT Press.

ACLS. (2009). What is cyberinfrastructure? Retrieved October 25, 2009, from http://www.acls.org/programs/Default.aspx?id=644

Arzberger, P., Schroeder, P., Beaulieu, A., Bowker, G., Casey, K., Laaksonen, L., et al. (2004). An International Framework to Promote Access to Data. *Science, 303*(5665), 1777-1778.

Atkins, D. E., Droegemeier, K. K., Feldman, S. I., Garcia-Molina, H., Klein, M. L., & Messina, P. (2003). Revolutionizing science and engineering through cyberinfrastructure: Report of the National Science Foundation blue-ribbon advisory panel on cyberinfrastructure. Washington, DC: National Science Foundation. Retrieved December 19, 2006 from http://www.communitytechnology.org/nsf_ci_report/.

Balkin, J. M. (2006, April 27). The democratic case for network neutrality Retrieved October 15, 2009, from http://balkin.blogspot.com/2006/04/democratic-case-for-network-neutrality.html

Beardsley, S., & Farrell, D. (2005). Regulation that's good for competition. *The McKinsey Quartley, 2*.

Benvenisti, E. (2008). The Conception of International Law as a Legal System *Tel Aviv University Law Faculty Papers*. Tel Aviv University Law School.

Berner-Lee, T. (2006, June 21, 2006). Net Neutrality: this is Serious, from http://dig.csail.mit.edu/breadcrumbs/node/144

Bird, I., Jones, B., & Kee, K. (2009). The organization and management of grid infrastructures. *Computer, 42*(1), 36-46.

Borgman, C., Wallis, J., Mayernik, M., & Pepe, A. (2007). *International and Interdisciplinary Collaboration in Cyberinfrastructure: A case study with embedded networked sensor technology* Paper presented at the AAAS Annual Meeting. Presentation retrieved from

Boulle, L. (1996). *Mediation: Principles, Process, Practice*. Butterworths: Tottel Publishing.

Bresnan, T. F., & Greenstein, S. (1999). Technological Competition and the Structure of the Computer Industry. *The Journal of Industrial Economics, 47*.

Buckingham, D. (2007). Digital Media Literacies: rethinking media education in the age of the Internet. *Research in Comparative and International Education, 2*(1), 45.

Burk, D. L. (2007). Intellectual Property and Cyberinfrastructure. *First Monday, 12*(6).

Burmeister, K. (1999). Jurisdiction, Choice of Law, Copyright, and the Internet: Protection Against Framing in an International Setting. *Media & Entertainment LJ., 9*, 625.

Cave, M., & Crocioni, P. (2007). Does Europe need network neturality rules? *International Journal of Communication, 1*, 669-679.

CEDA, C. f. P. D. (2006). Reclaiming our Commonwealth: Policies for a Fair and Sustainable Future. *Common Sense Paper, 1*.

Cerf, V. (2006). Prepared Statement of Vinton G. Cerf to U.S. Senate Committee on Commerce, Science, and Transportation Hearing on "Network Neutrality.

Cole, R. J., & Lorch, R. (Eds.). (2003). *Buildings, Culture & Environment: Informing Local & Global Practices*. Oxford: Blackwell Publishing Ltd.

Community Legal Framework for a European Research Infrastructure Consortium (ERIC) (2009).

Contractor, N. (2009). The emergence of multidimensional networks. *Journal of Computer-Mediated Communication, 14*(3), 743-747.

Coughlan, S., Currie, R., Kindred, H., & Scassa, T. (2006). Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization Law Commission of Canada.

Crandall, R., & Jackson, C. (2001). The $500 Billion Opportunity: The Potential Economic Benefit of Widespread Diffusion of Broadband Internet Access. Washington, D.C., : Criterion Economics.

Cranston, R. (1986). What Do Courts Do? *Civil Justice Q, 5*(124).

Crump, B., & McIlroy, A. (2003). The digital divide: Why the "don't-want-tos" won't compute: Lessons from a New Zealand ICT Project'. *First Monday, 8*(12).

Department of Broadband, C. a. D. E. D. (2008). Annual Report 2007-2008: Australian Government.

Depypere, S. (1995). Speech - Why do we a need a competition policy? : Europa.

Dierickx, S. (2006). Web Analytics: what about Packet Sniffing? Retrieved May 31, 2006, from http://webanalytics.ox2.eu/2006/05/31/web-analytics-what-about-packet-sniffing/

Eccles, K., Schroeder, R., Meyer, E. T., Kertcher, Z., Barjak, F., Huesing, T., et al. (2009, 24-26 June). *The future of e-research infrastructures.* Paper presented at the the 5th International Conference on e-Social Science (Proceedings), Cologne, Germany.

Editorial, A. T. (2009). Neutrality Vital to Health of Internet *St. Petersburg Time* Retrieved September 23, 2009, from http://www.tampabay.com/opinion/editorials/article1038353.ece

Edwards, M. (2001). *Social Policy, Public Policy: From problem to practice*. Crows Nest, NSW: Allen & Unwin.

Edwards, P., Jackson, S., Bowker, G., & Williams, R. (2009). Introduction: An agenda for infrastructure studies. *Journal of the Association for Information Systems, 10*(5), 364-374.

Endres, J. (2009). Net neutrality – How relevant is it to Australia? *Telecommunications Journal of Australia,, 59*(2), 22.21 - 22.10.

Foster, I., Kesselman, C., & Tuecke, S. (2001). The anatomy of the grid: Enabling scalable virtual organizations. *International Journal of High Performance Computing Applications, 15*(3), 200-222. doi: 10.1177/109434200101500302

Friendlander, A. (2008). The triple helix: Cyberinfrastructure, scholarly communication, and trust. *Journal of Electronic Publishing, 11*(1), Retrieved on June 13, 2008 from http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.3330011.3336109.

Fry, J., & Schroeder, R. (2009). Towards a sociology of e-research: Shaping practice and advancing knowledge. In N. W. Jankowski (Ed.), *e-Research: Transformation in scholarly practice* (pp. 35-53). New York: Routledge.

Gibbs, S. H. (2000). Oration Delivered at the Opening of the Supreme Court Library's Rare Books Room at the Supreme Court of Queensland.

Goldfinch, S., Gauld, R., & Herbison, P. (2009). The Participation Divide? Political Participation, Trust in Government, and E-government in Australia and New Zealand. *Australasian Journal of Public Administration, 68*(3), 333-350.

Gunkel, D. (2003). Second thoughts' toward a critique of the digital divide'. *New Media & Society, 5*(4), 499-522.

Hai, Z. (2004). China's e-science knowledge grid environment. *Intelligent Systems, IEEE, 19*(1), 13-17.

Hammond, A. S. (2002). The Digital Divide in the New Millennium. *20 Cardozo Arts & Entertainment L.J*, 135-156.

Hofer, E. C., McKee, S., Birnholtz, J. P., & Avery, P. (2008). High Energy Physics: The Large Hadron Collider Collaborations. In G. M. Olson, A. Zimmerman & N. Bos (Eds.), *Scientific Collaboration on the Internet* (pp. 143 - 151). Cambridge, MA: MIT Press.

Holland, T. E. (2006). *The Element of Jurisprudence*. Clark, New Jersey: The Lawbook Exchange Ltd.

Internet, S. t. (2009). FAQ Retrieved November 8 2009, from http://www.savetheinterent.com

Jankowski, N. W. (2007). Exploring e-science: An introduction. *Journal of Computer-Mediated Communication, 12*(2), article 10. http://jcmc.indiana.edu/vol12/issue12/janakowski.html.

Jankowski, N. W. (2009). *E-Research: Transformation in Scholarly Practice*. New York, NY: Routledge.

Johnson, K. (2009). The importance of net neutrality to the digital economy. *Telecommunications Journal of Australia,, 59*(2), 19.11 - 19.11.

La Rose, R., & al, e. (2007). Closing the rural broadband gap: Promoting adoption of the Internet in rural America. *Telecommunications Policy, 31*, 359-373.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford: Oxford University Press.

Lee, C., & Tibbo, H. (2007). Digital Curation and Trusted Repositories: Steps Toward Success. *Journal of Digital Information, 8*(2).

Lee, C. P., Dourish, P., & Mark, G. (2006). The human infrastructure of cyberinfrastructure. In P. Hinds & D. Martin (Eds.), *CSCW '06: Proceedings of the Conference on Computer Supported Cooperative Work, Banff, Alberta, Canada* (pp. 483-492). New York: ACM Press.

Leonardi, P. (2009). Why do people reject new technologies and stymie organizational change of which they are in favor? Exploring misalignments between social interactions and materiality. *Human Communication Research, 35*, 407-441.

Lessig, L. (1999). The law of the horse: What cyber law might teach. *Harvard Law Review*.

Lessig, L. (2009). Code version 02 Retrieved December 14, 2009, from http://codev2.cc/download+remix/

Lessig, L., & McChesney, R. (2006, June 8th). No Tolls on the Internet, *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108_pf.html

Lynch, C. (2008). The Institutional Challenges of Cyberinfrastructure and E-Research. *EDUCAUSE Review, 43*(6).

Maldonado, E., & Tapia, A. (2007, September 28-30). *Government-Mandated Open Source Development: The Case Study of Venezuela.* Paper presented at the Telecommunication Policy Research Conference, Washington, DC, US.

Meyer, E. T., & Dutton, W. H. (2009). Top-down e-infrastructure meets bottom-up research innovation: The social shaping of e-research *Prometheus, 27*(3), 239-250.

Meyer, E. T., Schroeder, R., & Dutton, W. H. (2008, 28 February-1 March). *The role of e-infrastructures in the transformation of research practices and outcomes.* Paper presented at the iConference UCLA, Los Angeles, CA.

Michaels, R., & Jansen, N. (2007). Private Law Beyond the State? Europeanization, Globalization, Privatization *Duke L School Working Paper Series,* . Duke L School Faculty Scholarship Series.

Mitchell, W. J. (2000). *E-topia*. Cambridge, MA: The MIT Press.

Monteiro, M., & Keating, E. (2009). Managing misunderstandings: The role of language in interdisciplinary scientific collaboration. *Science Communication, 31*(1), 6-28.

Murray, A. D. (2007). *The Regulation of Cyberspace: Control in the Online Environment*. Oxon: Routledge-Cavendish.

Myer, J. (2008). A National User Facility That Fits on Your Desk: The Evolution of Collaboratories at the Pacific Northwest National Labratory. In G. Olson, A. Zimmerman & N. Bos (Eds.), *Scientific Collaboration on the Internet* (pp. 121-134). Cambridge, Massachusetts: The MIT Press.

Nakamura, L. (2000). Economics and the New Economy: The Invisible Hand Meets Creative Destruction. *Business Review, July/August*.

NSF, C. C. (2007). *Cyberinfrastructure vision for 21st century discovery*. Arlington, VA: Retrieved from http://www.nsf.gov/pubs/2007/nsf0728/nsf0728.pdf.

Olson, G., Zimmerman, A., & Bos, N. (Eds.). (2008). *Scientific Collaboration on the Internet*. Cambridge: MIT Press.

Olson, J., Ellisman, M., James, M., Grethe, J., & Puetz, M. (2008). The biomedical informatics research network. In G. M. Olson, A. Zimmerman & N. Bos (Eds.), *Scientific collaboration on the Internet* (pp. 221 - 232). Cambridge, MA: MIT Press.

Petrazzini, B., & Kibati, M. (1999). The Internet in developing countries. *Communications of the ACM, 42*(6), 31-36.

Poole, M. S. (2009). Collaboration, integration, and transformation: Directions for research on communication and information technologies. *Journal of Computer-Mediated Communication, 14*(3), 758-763.

Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. *On the Horizon, 9*(5), 1 - 6.

Reid, T. A. (2007, May 2). *The new holy grail: An Australian e-infrastructure.* Paper presented at the EDUCAUSE Australasia, Melbourne, Australia. http://www.caudit.edu.au/educauseaustralasia07/authors_papers/Reid-238.pdf.

Ribes, D., & Finholt, T. A. (2009). The long now of technology infrastructure: Articulating tensions in development. *Journal of the Association for Information Systems, 10*(5), 375-398.

Schroeder, R. (2007a). e-Research infrastructures and open science: Towards a new system of knowledge production? . *Prometheus, 25*(1), 1-17.

Schroeder, R. (2007b). *Rethinking science, technology, and social change*. Stanford, CA: Stanford University Press.

Schroeder, R., & Axelsson, A. (Eds.). (2006). *Avatars at work and play: Collaboration and interaction in shared virtual environments*. Dordrecht: Springer.

Seidel, E., Muñoz, J., Meacham, S., & Whitson, C. A. (2009). A vision for cyberinfrastructure. *Computer, 42*(1), 40.

Stewart, C. (2007). Indiana University cyberinfrastructure newsletter Retrieved November 1, 2008, from http://racinfo.indiana.edu/newsletter/archives/2007-03.shtml

Tapia, A., Blodgett, B., & Jang, J. (2009). *The Merging of Telecommuncations Policy and Science Policy Through Broadband Stimulus Funding*. Paper presented at the TPRC

Research Conference on Communication, Information and Internet Policy, Arlington, VA.
Taskforce, C. R. (2005). Final Report of the Indiana University Cyberinfrastructure Research Taskforce: Indiana University.
White, L. J. (2008). *The Role of Competition Policy in the Promotion of Economic Growth*. New York University School of Law and Economics Working Papers. New York University School of Law.
Wu, T. (2003). Network Neutrality FAQ Retrieved November 8 2009, from http://www.timwu.org/network_neutrality.html
Ypsilanti, T., & Paltridge, S. (2004). OECD Broadband Market Developments. In R. Cooper & G. Madden (Eds.), *Frontiers of Broadband, Electronic and Mobile Commerce*. Heidelbery: Physcia-Verlag.
Zittrain, J. (2006). The Generative Internet. *Harvard Law Journal, 119*.

Cases and Legislation Cited

Commonwealth of Australia Constitution Act 1900

Dunlop Rubber Company v Dunlop [1921] 1 AC 367

Helicopter Utilities v Australian National Airlines Comm. (1963) 80 WN (NSW) 48

Heydon's Case (1584) 3 Co Rep 7a at 7b; 76 ER 637.

Macquarie Bank v. Berg [1999] NSWSC 526

Tosier and Wife v Hawkins (1885) 15 QBD 680.

Voth v Manilda Flour Mills Pty Ltd (1990) 171 CLR 538, 565

XYZ v Commonwealth (2005) 227 ALR 495

With thanks and acknowledgments to –
Ralph Schroeder – for taking time over his Christmas break to provide comments on a prior version – all errors remain those of the authors
Tessa Jade Houghton – our section Editor for her invaluable, honest and supportive critique
Andrea Tapia – for her review and suggestions for improvements

[i] For the progress of the European Parliament towards the creation of one area of 'freedom, security and justice' see – European Parliament 'Scoreboard: Union-wide fight against crime', Committee on Citizens; freedoms and Rights,

Justice and Home Affairs, Freedom, security and justice: AN AGENDA FOR EUROPE, <http://www.europarl.europa.eu/comparl/libe/elsj/scoreboard/crime/default_en.htm>.