Digital Policy, Regulation and Governance

Cybersecurity governance: a prehistory and its implications
Bradley Fidler,

Cybersecurity governance: a prehistory and its implications

Bradley Fidler

Abstract

Purpose – *The purpose of this paper is to understand the emerging challenges of cybersecurity governance by analyzing the internet's early history.*

Design/methodology/approach – *Tracing the design and management of early internet and network security technologies in the USA in the 1970s and 1980s.*

Findings – *The US Department of Defense separated the research and management regimes for networks and network security, with the latter restricted to military networks. As such, the absence of cybersecurity technologies on the early internet was not an oversight, but a necessary compromise. This ordering of networks and security had enduring technological, political and even cultural consequences, which are breaking down today.*

Social implications – *Political, technological and metaphoric distinctions between networks and security should be challenged; cybersecurity will transform internet governance.*

Originality/value – *New historical sources and analysis provide a novel perspective on contemporary challenges of cybersecurity governance.*

Keywords *Governance, History, Cybersecurity, Arpanet, Defense Data Network, Transmission Control Protocol (TCP)/Internet Protocol (IP)*

Paper type *Research paper*

Bradley Fidler is Assistant Professor of Science and Technology Studies, Stevens Institute of Technology, Hoboken, New Jersey, USA.

Introduction

This paper provides an analysis of early internet history, so as to better understand the challenges faced in contemporary cybersecurity governance and its relationship to internet governance. Its focus is on the design and management of the Arpanet, as well as the early phase of the internet's development, when the internet was centered on its Arpanet backbone (c. 1979-1985). It argues that, during the 1970s, the US Department of Defense separated major elements of the design and management of networks from the design and management of network security. This separation of network from network security was a consequence of the Department of Defense's need to build and secure military networks: not only did the networks require the security necessary to carry classified traffic, but many of the technologies they used to provide this security were also classified. It impacted the design and management of the internet in part because, through the mid-1980s, the infrastructure and management of the civilian internet was a component of a larger military internet, the Defense Data Network.

The split of networks from network security was extremely influential on the development of the civilian internet. There are two major consequences of this split. The first impact can be traced to the research and development strategy used by the Information Processing Techniques Office (IPTO) of the Advanced Research Projects Agency (ARPA; now DARPA). IPTO was the computing office within DARPA, the US defense agency tasked with creating revolutionary technological advances for the military. This strategy involved testing prospective computing technologies for the

Received 22 May 2017
Revised 1 July 2017
Accepted 2 July 2017

The author would like to thank Milton Mueller and two anonymous reviewers for their extremely insightful observations and criticisms – this paper is far stronger as a result of their contributions. The author would also like to thank Arpanet and early internet practitioners, many of whose interviews the author draws on here, for their time and insights. Any remaining errors are the author's responsibility.

DOI 10.1108/DPRG-05-2017-0026

Department of Defense in the unclassified, civilian world. If the technologies proved successful, they could be transferred to the military or intelligence community for (usually classified) use. In the case of computer networking, this meant unclassified networking testbeds such as Arpanet, the general-purpose computer network funded by DARPA that went online as an experiment in 1969. Through its funding of the Arpanet, DARPA created a civilian networking community in the USA that designed, built and managed unsecure networks. To put these networking technologies to use for the military, DARPA funded research and development projects to add security technologies in a modular fashion, modifying the existing networks for military use. Thus, the modular structure of the security technologies that developed in this arrangement mirrored the modular structure of the classified and unclassified research worlds. The absence of network security on the early internet was not an oversight (Timberg, 2015), but a byproduct of its institutional and political context. By the mid-1980s, the protocols that structured the internet architecture were unsecure by design. The internet technology, management governance organizations of the early to mid-1980s had little experience developing security technologies and even less in governing their use. Computers attached to the internet could contain their own security software, but the networking protocols themselves did not provide the security technologies that we increasingly take for granted today. For example, while a mainframe or personal computer might be protected against unauthorized entry, the design of the internet did not provide for encrypted traffic, secure routing or a secure namespace.

The second consequence lies in the historical origins, and present moment, of internet governance. By the mid-1980s, the lack of network security, noted above, was accompanied by emerging (civilian) internet governance practices that evolved around managing networking – and not security – technologies. This history is significant because the technologies and management structures of the Arpanet and early civilian internet ultimately became *the* global internet, as the internet absorbed competing systems and as others fell to the wayside.

This paper addresses only a limited portion of the breadth of technologies and organizations that fall under the label of cybersecurity. Today, cybersecurity is a broad topic that extends beyond what might come to be managed by internet governance organizations like the Internet Corporation for Assigned Names and Numbers (ICANN). The early history of security addressed in this paper is that of network security, which refers to security technologies deployed as part of network architecture. (Today, technologies like BGPsec and DNSsec fall under this category; the firewall on a personal computer would not.) This paper is an effort to understand the technologies of network security and the path dependency that they created for the portions of cybersecurity that deal with technologies integral to networks. This focus is necessarily limited, as there were less security technologies in existence decades ago, and not all of the security technologies in existence were deployed on networks or in network-facing machines.

A similar caveat is necessary for the distinction between the history of computer networking and the historical trajectory of the internet. The history of computer networks is far broader than the history of the internet, and includes many more networks and technologies than identified here. Some of these networks and technologies – such as those identified below – were influential in the design of the internet. However, the present-day technologies and governance model of the global internet emerged, in large part, in a subsection of the history of computer networking. To only address the history of the internet is not to say that the larger, global history of networking is any less important. Rather, this paper's focus on the history of the internet is more limited, meant only to better understand specific characteristics of the technologies and governance models with which we live today. Finally, the analysis that follows is agnostic regarding the quality, utility or any other evaluative criteria that may be applied to the organizations and technologies of networks and network security. In computer science communities, discussion of the history or politics of a technology can be laudatory or critical; this work is neither.

This paper proceeds as follows. In the section that follows, I will provide a brief overview of literature on networks, cybersecurity and internet governance. Next, I will analyze the history of the Arpanet's research and management ecosystem, discussing the initial separation between networks and network security, as outlined above. Following this, I will explain the emergence of the civilian internet as a component of the military internet, the Defense Data Network, and its consequences for security technologies and internet management. Finally, I will conclude with questions and observations regarding the future of cybersecurity governance.

Histories of networks, cybersecurity and internet governance

The three areas of inquiry sketched in this section – internet governance, the histories of cybersecurity and the histories of networks themselves – remain largely separate areas of inquiry. As a result of this separation, it is difficult to understand how the three areas interact, both in history and in the challenges of the present day. What follows is a brief sketch of illustrative works and themes in these three areas.

The first generation of histories of the internet, written in the late 1990s and early 2000s, were histories of core internet technologies and the organizations that supported their development (Abbate, 1999; Hafner and Lyon, 1999; Norberg *et al.*, 1999; Salus, 1995). They were stories about the ecosystem of largely US researchers, and especially those whose work was funded by DARPA. These works typically began with IPTO's funding of computer networking research in the 1960s and document the development of the Arpanet and the early history of the internet. This first generation of scholarship drew attention to computer networking for the fields of history, science and technology studies, and scholars of technology more broadly. Work by Abbate (1999) in particular drew on methods from science and technology studies to provide groundbreaking analysis of technologies that, until then, were largely the domain of biographies and popular accounts. Technologies such as packet switching, electronic mail and the transmission control protocol/internet protocol (TCP/IP) that is central to the operation of the modern internet were analyzed as the outcome of social, political and cultural forces. To say that this generation of histories did not focus on governance is in no way a criticism: their emphasis, while broad, was earlier in time and focused on technology and the organizations dedicated to its development. Eventually, however, accounts of internet technologies need to incorporate analysis of management and governance, if only because each of these technologies presupposes a management or governance structure.

A second generation of scholars revisited the histories of networking from the 2000s onward. Their purpose was less to revise the first generation's focus on the Arpanet and internet lineage, but rather, to expand the historiography with new methods and areas of inquiry. This new scholarship included work on computer networking in Latin America (Medina, 2011), the French national network Minitel (Fletcher, 2002) and a cultural history of spam email (Brunton, 2013). Importantly, for this paper, Russell (2014) provided a history of the contest between DARPA's internet protocols and those under development by engineers coordinated through the International Organization for Standardization (ISO). He outlined the very different political and organizational approaches to standards development represented by the DARPA and ISO communities, providing fresh insight into the DARPA story. However, his purpose was not to investigate internet governance of the mid-1980s and beyond. Most recently, Peters (2016) documented the thwarted efforts to create a national computer network in the Soviet Union. Computer networks were a global phenomenon in the 1970s and in no way limited to the USA and UK. These important new works make clear the distinction noted above, between the history of computer networking in general, and the narrower history of the development of the internet.

Scholarship on the early history of network security and cybersecurity is more recent than that on computer networks. An early and canonical work provided a historical survey of cryptography (Kahn, 1967), and Mackenzie's *Mechanizing Proof* (Mackenzie, 2001) was the first work to identify a history of modular security technologies on the internet. Two recent special issues of the *IEEE Annals of the History of Computing* provided a range of new histories (Yost, 2015, 2016), from the early US government policy in computer security (Lipner, 2015; Warner, 2015), to security discourse at government contractors (Misa, 2016), to the late twentieth century efforts to deploy public key infrastructure in South Korea (Park, 2015). Other works in these special issues included histories of computer security metrics (Slayton, 2015), as well as what DeNardis (2015) calls the "design tension between surveillance and security". In this works, DeNardis (2015, p. 74) argued that security was a concern by 1986, pointing to interest in access control and authentication. Indeed, access control and authentication was an issue on the Arpanet in the early 1970s (and finally implemented in the early 1980s). Nonetheless, security was discussed in early IETF meetings, in specific ways, as I explore below. Recent work by DuPont and Fidler (2016) documents the early history of cybersecurity technologies as network security. Our argument, some of which is reproduced here, links modern cybersecurity architecture to design decisions of the early 1970s on the Arpanet.

The third body of scholarship addressed here analyzes the interaction between internet governance, state sovereignty and internet technology (Mueller, 2002, 2010). Studies of internet routing security (Kuerbis and Mueller, 2017) link discussions of security from more traditional forms of crime (e.g. identity theft, spam) to security issues that intersect management of critical infrastructure itself and argue that technological fixes can move around but not solve fundamental problems of collective action. Other literature (Mueller *et al.*, 2013) notes that, against a backdrop of urges to impose state sovereignty over the internet directly, governments have, in fact, worked within existing private governance structures to influence standards and practices. Rather than face a fundamental incompatibility of states and networks, initial findings suggest that we are witnessing an evolution of governance strategies. Other central work in this field, which speaks directly to the themes of this paper, includes Laura DeNardis' scholarship, on the technological and infrastructural basis of internet governance. It points to, among other things, the way in which internet technologies become integral to governance and can even be instruments of political power (DeNardis, 2009, 2012). Mueller and DeNardis are the focus here, as both use historical analysis in their scholarship: for example, Mueller provides a history of the Domain Name System and its management, and both explore the early history of the Internet Engineering Task Force. In the sections that follow, I aim to build on their work by expanding this historical analysis to include the origins of network security architecture and its relationship to network management and internet governance.

The Arpanet research and management ecosystem

It is worthwhile to begin with the origins of DARPA-funded computer networking research and its basis in defense priorities. J C R Licklider, the oft-cited 1962 founder of DARPA's IPTO, was interested in building research programs that would benefit the defense and civilian worlds simultaneously. Licklider clarified the dual uses to which he saw his research contributing:

> The fact is, as I see it, that the military greatly needs solutions to many or most of the problems that will arise if we tried to make good use of the [information processing] facilities that are coming into existence [. . .]. I am hoping that there will be, in our individual efforts, enough evident advantage in cooperative programming and operation to lead us to solve the problems, and thus, to bring into being the technology that the military needs. When problems arise clearly

> in the military context and seem not to appear in the research context, then ARPA can take steps to handle them on an *ad hoc* basis (Kita, 2003; Licklider, 1963).

In other words, civilian investigation of information processing technologies would predict uses and problems that would eventually be faced by the military. Less important for ARPA were straightforward technological problems that the military would discover on their own.

During Licklider's two-year term, he funded exploratory research into computer communication which the next IPTO Director, Ivan Sutherland, continued through 1964-1966. In 1966, the subsequent Director Robert Taylor funded initial research into what would become known as the ARPA Computer Network (Arpanet) in 1966. Taylor understood that solving civilian and military problems simultaneously would make for stronger research outcomes for the military, and then-ARPA Director Charles Herzfeld understood ARPA research in this Licklider tradition (Herzfeld, 1990; Taylor, 1989). Defense priorities were not incidental within DARPA, a US defense agency, in the projects it funded. The initial funding for ARPA's IPTO was provided by the Kennedy White House, a "Command and Control Research" portfolio meant to improve communications for the military (Norberg, 1996).

Nonetheless, strong defense priorities cannot be assumed to have been uniform throughout the DARPA computer network research ecosystem. The principal investigators, funded by DARPA to house Arpanet nodes and to conduct research on or with the network, were likely far more interested in their own research, if they were based at academic institutions, than military applications. It is even more likely that the graduate students – often remembered in lore as "hippies" – who worked for the principal investigators were no cold warriors, either (Hafner and Lyon, 1999). This civilian configuration was culturally significant, but does not, however, change the way that the Defense Department, through DARPA, fashioned the design and management of the Arpanet. In this section, I will address the management of the Arpanet, followed by its security architecture.

The analysis that follows distinguishes between network and internet management, on the one hand, and governance, on the other. I describe the practices and institutions used to administer the Arpanet and early internet as management, based on institutional and other historical differences from internet governance today. Internet governance, I argue, emerges with organizations like the Internet Engineering Task Force from 1986 onward and differs in important ways from earlier management. Nonetheless, in this analysis, the history of Arpanet and internet management was deeply influential on internet governance. Relatedly, I have not discussed the role of the National Science Foundation or its NSFNET internet backbone. While its contributions are certainly important – not only in the funding of the early internet, but in its major expansion of its infrastructure and user base – they would not alter my arguments. For the sake of brevity, I have not addressed its role.

One way that the management of the Arpanet can be understood is in terms of the organizational requirements of network architecture. In short, all networks, even decentralized networks, require significant coordination. The reason is that each node must cooperate with other nodes in exchanging data, control and routing information. Routing algorithms, for example, must be implemented in a uniform fashion and must be implemented properly for the network to function. Similar requirements exist for maintaining a global address space, or a hierarchical namespace. For the Arpanet, the answer to this requirement lay in the authority of DARPA to set Arpanet policy. Histories of the Network Working Group (NWG), an *ad hoc* association of graduate students charged with developing the host software for the Arpanet, often remark on its self-organizing and informal character (Metz, 2012). What is less commented on is how, once the NWG would agree on a protocol (and, crucially, have it approved by DARPA), it would eventually be adopted across the entire Arpanet. (Here I am referring to the "host-host protocol", implemented as the Network Control Program, which was software that handled communication across the Arpanet for connected computers.)

By 1972, the Arpanet experiment not only saw engineers demonstrate its utility in resource sharing, but also its general utility in person-to-person communication. In the early 1970s, other networks, sometimes inspired by the success of the Arpanet, were underway and usually without the military backing of the Arpanet. Military control is certainly not required to manage network architecture. In the case of the Arpanet, however, there was no need to develop non-military management or governance structures. In 1975, management of the Arpanet (for example, of the Network Control Center, general contracting and user registration) was transferred to the Defense Communications Agency (DCA; now DISA), the US defense agency responsible for communication systems that spanned large portions of the Department of Defense (e.g. "common-user" networks). In place of DARPA's effective technocratic management, it convened a small "Arpanet Sponsors Group", in which the DCA would solicit feedback and advice, and communicate policy to major institutional network users such as NASA, the Department of Energy and the National Security Agency. In 1980, the DCA's Arpanet Sponsors Group had only 11 members, representing a network of more than 80 institutional nodes (Fidler and Russell, 2018). A year later, the management of assigned numbers (later called the Internet Assigned Numbers Authority, or IANA) emerged as a semi-formal operation under the direction of Jon Postel at the University of Southern California's Information Sciences Institute, a function that also relied on DARPA's power to enforce policy. Again, this was less governance that it was management.

The second consequence of the defense ecosystem was a long-term path dependency in network security. By the mid-1970s, plans were underway to build Arpanet-like networks for agencies such as the National Security Agency, and to use the Arpanet to link classified users to other military networks (DuPont and Fidler, 2016; Elsam, 1980). As DARPA had already developed the network architecture, making secure variants of the Arpanet meant adding cryptographic resources to the ends, or edges, of the network. The network architecture would remain completely open, and cryptographic resources would be added between the attached devices and the network switches. This established the contrast that remains in place in end-to-end security today, namely, encrypted packet payloads and cleartext packet metadata. This design process was initiated in 1973, and the first cryptographic devices – the Private Line Interface (PLI) – were operational on the Arpanet by 1976. In some cases, PLIs created overlay networks on the Arpanet itself so as to facilitate classified communications. In others, they were used to provide a secure channel through the Arpanet to external classified networks, thereby extending the reach of these networks through the Arpanet (Fidler and Currie, 2016). This Arpanet/PLI model represented a technological and institutional compartmentalization of networking and network security. The networking (or computer communication) community in the USA was largely comprised of university researchers doing unclassified work, while the classified development of the security architecture for the Defense Department's new networks was undertaken by defense contractors and certified by the NSA (DuPont and Fidler, 2016). In addition to the compartmentalization of security technologies on the Arpanet, entire classified versions of the network were constructed elsewhere in the Defense Department. Not only was the NSA replacing its Community Online Intelligence Service (COINS) with a new network based on the Arpanet (COINS II), but it was also used as a prototype replacement for other major network infrastructures, such as the Worldwide Military Command and Control System (WWMCCS) (Pearson, 2000).

The Arpanet represented two important directions in computer networking. First, the management of the network was accomplished in a minimal, technocratic style, relying on a military hierarchy that would set policy, in consultation with a technical cadre of civilian computer scientists. Second, secure networks and security architecture were both separated from the civilian users of the network. The importance of these directions to the internet will be discussed in the following section. The Arpanet, to be sure, was not the only form of computer networking; it was not even the only network in the USA. Indeed, the early and mid-1970s were formative times for computer networks. In 1970, the earliest forms of both the Arpanet and the UK National Physical Laboratory's Mark I network were operational. It had already been eight years since Arthur Schlesinger Jr warned President Kennedy that "we are finished" if the USSR's computer networking plans would come to fruition (Gerovitch, 2008). In 1972, Chile embarked on its CYBERSYN program to network its own socialist economy (Medina, 2011), and in the same year, France embarked on its own experimental packet-switched network, CYCLADES (Russell and Schafer, 2014). In the USA, the early 1970s saw private computer networks TYMNET and TELENET seek to bring to market services similar to those offered by the Arpanet (Mathison *et al.*, 2012), and Compuserve, created in 1969 to serve the insurance industry, went national with its BBS-style service MicroNET (Campbell-Kelly and Garcia-Swartz, 2013). In 1977 (and planned since 1971), the EU brought online its own internetwork, the European Informatics Network (Barber, 1975), which connected CYCLADES with several other European networks. This is not an exhaustive list, and it is meant to illustrate how the Arpanet's influence on the internet was not a consequence of its uniqueness as a computer network. Rather, its significance lies in the fact that its technologies – including its security architecture – were adopted for the internet, as was a derivative of its system of management.

The civilian internet and the defense data network

In 1972, the International Conference on Computer Communication, held in Washington DC, saw the first meeting of the International Packet Network Working Group (INWG), modeled after the Network Working Group (McKenzie, 2011). The INWG was comprised almost entirely of civilian researchers, and their interest was the straightforward next step in computer networking: given the multitude of heterogeneous computer networks coming into existence, how to inter-network them? Vinton Cerf served as INWG's first chair, and in part based his work on the first TCP specification from the initial meetings. Based on a reading of its first specification and an earlier partial specification (Cerf, 1973; Cerf and Kahn, 1974), this protocol was designed for civilian internetworking – or, perhaps, it was a case of designing technologies that would transform both military and civilian worlds. While Cerf and Kahn's TCP did not address the broader political and regulatory environment in which it might be put to use, other work from members of the INWG members, especially proposals put forward by Pouzin (1973), envisioned large, institutionally independent national networks with standards harmonized between them.

Beginning in the same year, DARPA program manager Robert Kahn funded the development of internetworking protocols as a component of his programs for packet radio and satellite packet communications. It was designed to enable a military internet comprised of a long-haul, Arpanet-like continental network, which would interconnect with a variety of radio and satellite networks (Abbate, 1999). (Until now, such military networks would typically not interoperate, or interoperate very poorly). For the first several years of this work, it ran in parallel to internetworking research by INWG members, with Cerf continuing to serve as chair and contribute his work on the TCP. By 1976, however, DARPA research had moved ahead of INWG work: the TCP had several built implementations, while actual testing with the INWG was still in the planning stages (Cerf, 2016). Although INWG researchers did reach a compromise protocol all parties could agree to, its adoption would mean that DARPA would take steps backward in protocol development. Thus, while Cerf would continue to contribute to the group's discussions, in 1976, he resigned his chair and began as a DARPA program manager in charge of its new internet program (Kahn was now Director of the IPTO) (Russell, 2014).

The backdrop to these decisions was the Department of Defense’s 1976 decision to build a new computer network to link multiple services (e.g. Army, Air Force), agencies and other portions of the Defense Department. The new network, the Automatic Digital Network II (AUTODIN II), was a replacement of the first, aging AUTODIN that had been in place since the early 1960s. Based on an earlier generation of computer technologies, it lacked many features of the Arpanet, such as interactive communication and was not considered “survivable” (e.g. able to continue to operate after natural or human-made disasters) (Corrigan, 2015; Lyons, 1980). For two or more years, the Department of Defense, through the Defense Communications Agency, was developing the requirements and basic design for the network; some of this work was chaired by Robert Kahn and involved Vint Cerf. In 1974-1975, the Department of Defense funded a reference implementation of Cerf and Kahn’s TCP, modified specifically for AUTODIN II (Kahn, 1975). In other words, the new AUTODIN II network provided a large, concrete use for the TCP, and it also provided Cerf and Kahn with deadlines for its development.

The AUTODIN II specification offered a different security architecture than the trajectory developed by DARPA for the Arpanet and classified Arpanet-like networks. On AUTODIN II, network security was incorporated not only at the connected computer systems, but in the network architecture itself. The TCP specification developed for the Arpanet was modified to fit this design: in addition to a sophisticated access control system, the network nodes were involved in user authentication, checking against a database that each party to a connection possessed the security clearance to be connected from their location and to communicate with the other party (Postel *et al.*, 1976).

Based on the documentation generated by the DARPA internet program, AUTODIN II was also a major reason that the Department of Defense supported DARPA’s development of internet protocols. At the very least, as mentioned, AUTODIN II was the source of deadlines imposed on Cerf and Kahn by the Department of Defense. Memoranda of 1978 and 1980 from the Department of Defense, distributed by Cerf to internet program participants, place the AUTODIN II plans in context: AUTODIN II would serve as a common-user computer network that would also link together existing defense and intelligence networks. It would do so with the TCP and IP (Cerf, 1980; Dinneen, 1978, 1980). These memoranda were also clear that updated AUTODIN II security requirements would be built into the internet program’s protocol specifications (e.g. into TCP and IP). Prior to the AUTODIN II’s first tests, in 1978, one of the five TCP implementations under development was designed to mimic the AUTODIN II while it was being tested on the Arpanet (Ruizendaal, 2017)[1]. Cerf, as chair, would invoke Defense Department schedules to inspire his team. Minutes for a November 1978 meeting read, in part, as follows:

> Vint: We need to show an operational capability. [. . .] Preliminary specifications are to be ready in December 1978, and final in April 1979. Thus, all this is extremely visible in DOD and its contractors.
>
> Col. Russell [Colonel David Russell]: Confirmed the visibility of this effort, and the realization in DOD that protocols and internetting are now very important. The DOD is now about to make a commitment in the computer-communication area. There is a window (in time) in which input is considered and decisions are taken (Postel, 1978a, p. 1).

There was little place for an expanding civilian internet in the AUTODIN II plans, and thus less of a future for the DARPA internetworking protocols. Minutes from an internet program meeting of the same year provide an outline: “Cerf: Phase out of ARPANET by replacing the crosscountry sections by Autodin II, leaving (for a while) regional ARPANETs in the Boston, Washington, Los Angeles, and San Francisco areas. These regions connected to AUTODIN II (and thus each other) via gateways” (Postel, 1978b: 14). In other words, the Arpanet would exist in small pieces, connected to the larger military internet centered around the AUTODIN II. In this plan, the Arpanet would not become (as it did) the backbone of a new civilian internet, but exist to link research sites to a military internet. In fact, whether the AUTODIN II was a truly an internet by contemporary standards is up for debate (some of its connections with member networks appear more as mapping/translating gateways, and its initial specification was explicitly for a network and not an internetwork). The security architecture of this system, as mentioned, diverged from that of the Arpanet, for in the AUTODIN II's design, its fundamental networking protocols were meant to be secure.

By 1979, DARPA built on its internetworking tests of 1976 and 1977, and they eventually became permanent connections. A highly experimental internet emerged, centered around the Arpanet as its backbone. It utilized the internet protocols we understand in retrospect as standard, but at the time may have appeared stripped-down in contrast to their more complex AUTODIN II iterations. The identities of the participating networks in this early internet, comprised heavily of research contractors, may provide an insight into the type of civilian internet that was moving forward, if AUTODIN II was to be successful. By August of 1979, of the 30 reported networks provided identification numbers (giving them the ability to participate in the DARPA internet), three were run by DARPA-funded US universities, seven by allied foreign civilian organizations with a close DARPA relationship, two by private US firms; one by the UK military; the remaining 17 were run either by IPTO or by the US Defense Communications Agency (Strazisar and Perlman, 1978).

Cerf, however, was *also* driving the development of an unsecure civilian internetwork architecture for what he called a "global catenet", based on DARPA internet technologies and not linked to AUTODIN II (Cerf, 1978). In this project, the modular security architecture of the Arpanet re-appeared. A classified packet security program, also run by Cerf at DARPA, funded the development of modular security technologies. They included a new version of the PLI, the internet PLI, modified to work over an internet (Cerf, 2016), as well as more advanced modular security technologies that did not require manual keying (DuPont and Fidler, 2016). The internet PLI provides a clear link between the security architecture of the Arpanet and that of the internet. Recall that the PLI was used to create secure portions of the Arpanet and secure Arpanet-like networks without altering their foundational protocols. The same strategy was at work here for the internet. Cerf was not only preparing the TCP and other core internetworking technologies for the AUTODIN II. He was also developing security technologies that could transform his internet protocols into truly "dual use" technologies, by adding security to open and unclassified communication protocols. This work was not based on AUTODIN II requirements, but on a separate stream of architectural studies and philosophy that grew out of the internet program.

Whatever Cerf and Kahn's bet, or plan, it paid off. Beginning in the late 1970s, and certainly by 1980, DARPA staff and DARPA-funded engineers became concerned with the development of AUTODIN II. The initial acceptance testing, scheduled for 1980, was considered by many in this community to be a failure. A small, informal coalition of DARPA and Bolt Beranek and Newman personnel – with major agitating and organizing by Bolt Beranek and Newmann engineer Sevcik (2015) – gained influence in calling for its replacement. They were joined by Steve Walker, a former DARPA program manager who now had a senior position within the Office of the Secretary of Defense. In 1981, Walker organized a three-day "fly off" competition between two proposals: the Defense Communication Agency and Western Union's AUTODIN II, and a military version of DARPA's civilian internet (with modular security), named the Defense Data Network, put forward with Bolt Beranek and Newman. The three-day meeting was held in a poorly lit room at the Pentagon. In April 1982, the Office of the Secretary of Defense cancelled AUTODIN II and directed the Defense Communications Agency to build the Defense Data Network (Defense Communications Agency, 1982; Heiden, 2015; Heiden and Duffield, 1982). Consequently, the nascent testbed internet that the IPTO was nurturing around the Arpanet backbone suddenly took on a new significance. Rather than a small network that would eventually be dispersed to AUTODIN II adjuncts and commercial networks, the Arpanet would now serve as a testbed internet for the Defense Data Network. It would continue to grow. Like the Arpanet, the civilian internet was shielded from the need to set policy for and coordinate security architecture (as it might, for example, for assigned numbers), as there was very little security to govern.

By October 1982, this civilian internet was now (in the words of a BBN engineer) "expected to be a continuously expanding system, with more and more hosts on more and more networks participating in it" (Rosen, 1982). This contrasted BBN estimates from 1978 that forecasted an internet of less than 100 networks. In 1983, DARPA converted the Arpanet to the now-finished TCP and IP, formalizing the Arpanet's role as the backbone of this expanding civilian internet. The Arpanet backbone of this civilian internet, however, was subsumed as a part of the Defense Data Network, managed operationally by the Defense Communications Agency. The first two Defense Data program managers report that they continued support for the Arpanet because of its value as a testbed for the Defense Data Network (Heiden, 2015; Maybaum, 2015). The Director of Information Systems at the Office of the Secretary of Defense recalls supporting the internet protocol suite (in contrast to international standards) in part because of the national security gains that would accrue to the USA if it and its allies used their own protocols (Lane, 2015).

As noted, the victory of the Defense Data Network over AUTODIN II also revived the edge cryptography of the early Arpanet. The modular model of the PLI was extended first to the internet PLI and followed by the Black Crypto Red and BLACKER systems of the late 1980s and early 1990s. The internet PLI differed from the PLI in that it could run over inter-networks, and BLACKER did away with the need for manual keying by introducing key distribution centers (Kent, 2015; Swope, 1988; Weissman, 1992). The internet PLI and BLACKER were run from the IPTO's packet security program, and TCP/IP was designed to accommodate them: their influence can be seen today in TCP and IP (v4) packet header security fields (Cerf, 2016; Postel, 1981a, 1981b). Thus, the modular security architecture introduced on the Arpanet was replicated on the early internet. Both the military (Defense Data Network) internet and its Arpanet-based civilian component ran the same core internetworking protocols, the TCP/IP. The Defense Data Network used DARPA's modular security technologies, which were expensive, complex and not meant for the civilian internet.

Meanwhile, DARPA expanded the technocratic management system developed for the Arpanet to guide the development of both the Defense Data Network and its civilian (Arpanet-based) component. The civilian internet was meaningfully civilian, but it was also a part of a larger military internet, and managed as such. While DARPA set research and development priorities, routine operational matters were administered by the Defense Data Network Program Management Office at the Defense Communications Agency. Postel, who continued to administer assigned numbers from the Information Sciences Institute, worked closely with Cerf.

Much like the Defense Communication Agency's Arpanet Sponsors Group, Cerf created an informal council, the Internet Configuration Control Board, to draw on the expertise of members of the internet community (Fidler and Russell, 2018). In 1984, after Cerf's departure from DARPA, Barry Leiner expanded the Internet Configuration Control Board, creating the Internet Activities Board, which organized its expanding membership into 10 working groups (Braden, 1998; IAB Executive Editor, 2011). Two years later, the Internet Advisory Board created the Internet Engineering Task Force, which expanded rapidly. The Internet Engineering Task Force (IETF) quickly took on its own unique identity, as outlined below. Its rapid Within the Defense Communications Agency's Defense Data Network Program Management Office, however, it was understood that the IETF would permit the Department of Defense to remain involved in standards development for the Defense Data Network and the internet (Mundy, 2015).

The history of these early management and governance institutions is well documented (Mueller, 2002; SSAC, 2014), and here, I wish to highlight their relationship to security architecture. The transition from lean technocratic management to nascent structures for internet governance marked the beginning of discussions of security for the civilian internet. The foundational protocols of the internet, however, were already in place. The TCP and IP were now Department of Defense standards, and the Exterior Gateway Protocol that linked and established the topology of interconnected networks was already deployed. Similarly, in the early 1980s, the Domain Name System and the Simple Mail Transfer Protocol were already in development as unsecure protocols.

One of the 10 task forces created with the Internet Activities Board in 1984 was “security”, run by Ray McFarland, formerly with the National Security Agency (Cerf, 1976), and at the time representing the Department of Defense (Defense Communications Agency, 1985). Another task force was “privacy”, run by Kent (2015) of Bolt Beranek and Newman, who oversaw research on the modular security architecture for the Defense Data Network. One outcome of these task forces was a series of privacy enhancements for electronic mail (Linn, 1987). During the first few years of IETF meetings, discussions of the heavily secured Defense Data Network, which used both link and end-to-end encryption, included discussions of security but did not delve into its classified components or operations. (Thus, while IETF meetings did discuss security, they did so for military networks, which did not require governance in the way that civilian networks would.) Nonetheless, at the fourth IETF meeting in 1986, a “Long Range Blue Sky Visions” panel noted “security” as a topic of interest, alongside discussions of (far off) internet-connected devices in the range of US$100-US$1,000 (Gross, 1986, p. 4). As both long range and blue sky, security did not appear alongside the more prosaic problems like improving (unsecure) routing and interoperability, which were split between civilian internet and Defense Data Network interest. By the sixth IETF meeting in July 1987 (Gross, 1987), security issues appeared again, but in less of a blue-sky fashion. Here, the issue was to begin to secure internet routing by developing methods of authentication for the gateways (now called routers) that passed data between networks. In this case, the severity was marked as “low”, and its “owner” was the IETF and the Office of the Secretary of Defense. By IETF 11, in 1988, authentication work was well underway and now expanded beyond gateways to internet technologies in general (Gross and Bowers, 1989). All of this was still a long way from *managing* (for example) the key distribution centers that were being built as part of BLACKER for the Defense Data Network. The Internet Assigned Numbers Authority, a governance function funded by a DARPA contract until 1997, the evolving, technocratic structure of the Internet Activities Board and IETF were built to evolve, deploy and manage a small (by today’s or even 1990s standards) internet, comprised of networking, and not security, technologies. What is more, the major architectural decisions regarding the DARPA internet were made in the mid- to late-1970s, and the governance institutions that emerged some years later did not have to contend with proposals that would have significantly altered that architecture.

Thus, by 1986-1987, emergent internet organizations began to grapple with the challenges posed by security, although primarily in the realm of design.

Ultimately, security was still a new problem in the 1990s when the character of today’s civilian and multistakeholder structures of internet governance took shape. For example, IPsec and public key infrastructure research began in the early 1990s, along with DNSSEC as well, with Secure BGP (BGPsec’s predecessor) emerging in the late 1990s. An alternative model from the early 1980s is visible in early research for the competing Open Systems Interconnect internetworking protocols, developed under the ISO. Here, 1981 saw the publication of a major report on the security requirements and solutions for the future civilian internetwork protocol suite its associated researchers hoped to build (Voydock and Kent, 1981). The report argued that the internet should be built with end-to-end security, public key encryption and a key distribution infrastructure. Open Systems Interconnect was never able to upend DARPA's protocol suite, but remains as an example of how more security might have been included sooner. None of this is to say that the Open Systems Interconnect offered a better set of technologies or even a reasonable system of governance – only that different social and political contexts led to different technological artifacts.

Conclusions: Networks, security and the future of cybersecurity governance

This paper is an effort to outline a social and technical history of the early internet's security architecture. My major claim is that the DARPA-led networking ecosystem created an institutional and technical separation of networks and network security, which had consequences for subsequent design, management and governance. This separation was not wrong or unbeneficial: it was a strategy decided by dedicated and resourceful engineers responding to the technical and organizational challenges they faced. In this final section, I will draw on my historical analysis to provide observations and questions for the future of cybersecurity governance.

My first point is very tentative. I am curious if there was an additional outcome of this early history, in the meaning of computer networks, or even cyberspace. Anthropologist Brian Larkin argues that the politics of infrastructures can be found not only in their technological functions, but in what Larkin calls their "poetics". Poetics, for Larkin, is "a rearrangement of the hierarchy of what signification within the speech event is dominant at any moment. [. . .] In the case of infrastructures, the poetic mode means that form is loosened from technical function" (Larkin, 2013, p. 335). In these terms, a commonly understood characteristic of infrastructures, as systems that remain invisible until they break (Bowker and Star, 2000), is incomplete. Instead, infrastructures perform two functions: not only technical or material, but also in the creation and maintenance of meaning. Depending on one's theoretical commitments, this meaning may be produced with some regularity as a consequence of the technological properties of the infrastructure (Deleuze, 1992), or infrastructures may instead be sites of contestation and negotiation (Leigh Star, 2010), with meaning assigned and re-assigned by actors and broader social forces. I am interested in the former view, that while open to contestation, infrastructures such as the internet produce certain meanings with some regularity.

For over two decades, scholars have called attention to the utopian "myths" of the internet as a political force, often presented as an obfuscation or as ideology (Barbrook and Cameron, 1996; Winner, 1997). However, my question is not about social or political mythology, but rather, what networks are understood to be, not in an extended political form, but as themselves. After all, to serve so well as a space for (to take one example) cyberlibertarianism, there must have been discursive scaffolding to hang it all on. This meaning, I suggest, is associated with a communicative network graph in which each node can speak with any other and in which all are known to the gods-eye observer: this was, at least, the metaphor of the Arpanet maps (Fidler and Currie, 2016). Cryptographic resources may be added to the edges of the network, but they do not belong *within* it, where they might obfuscate the gods-eye view. If the networks in the Arpanet and early internet did maintain a particular meaning, then perhaps these early metaphors remain. Thus, China's Great Firewall and National Security Agency surveillance programs are both understood as distortions of a natural cyber-something order – despite following in obvious fashions from the politics of their societies.

My second point concerns the global spread of the technical and institutional (and perhaps metaphoric) order outlined above. The DARPA research ecosystem and its design decisions began to spread globally in the late 1980s and early 1990s. We would be remiss, I think, to not note the major geopolitical significance of this part of the postwar order: an unusually uncontested period of global American influence. It was during this time, without technological peer or near-peer competitors, that the network architecture and governance model I describe was adopted globally. Indeed, the “protocol wars” that marked the ascendancy of the DARPA internet protocols over their only major (European) competitor (Russell 2014) were rivalries between nearly homosocial communities distributed across geopolitical allies. Perhaps, this effectively uncontested global spread was aided by the meaning ascribed to internet protocols, which were, emptied of security (and national security) considerations, easy to understand as neutral or emancipatory. The controversy that did exist, such as that surrounding the Domain Name System in the late 1990s (Mueller, 2002), should still be understood in terms of an easy road to global adoption. Internet governance has not faced a peer/near-peer adversary fight for a new name or address space, cryptographic primitives or a next-generation transport layer protocol; it is unreasonable to assume that it never will.

My third and final point concerns the future of cybersecurity governance and new forms of controversy. While the internet’s legacy meaning may invoke open communication, its function, from a security standpoint, is to simultaneously enable various forms of surveillance while also constructing different modes of privacy. In other words, the shadow no longer resembles the substance. The technical, political and metaphoric separations between networks and security need not be maintained. Our technologies, politics and metaphors may be reconfigured before they fracture in the face of a different era. After all, much like the name and number space, new cybersecurity technologies will also require central points of authority, and ultimately, governance. Those questions will be asked and answered in a world where ICANN is much more the focus of international competition than it was in the late 1990s. If the cultural and political traditions of the internet are worth protecting – as I believe they are – then it is better to accelerate this shift. This means that new computer networking textbooks, clean-slate internet architectures, governance methods and metaphors should all reflect the inseparable link between networks and security.

There are obvious signs that this process is already underway, and it is best to get in front of it. In the field of future (or next-generation) internet architectures, work is underway in the USA, Europe, Japan and China (Krekel *et al.*, 2012; Pan *et al.*, 2011). Many, if not all, of these programs challenge the network and security separation, if not technologically then metaphorically or rhetorically (Chen and Mizero, 2015), as most claim to approach security in a more fundamental way than the TCP/IP. What is more, unless the TCP and IP, for example, will last another four decades, the effort to replace them may uncontested veer into international or geopolitical competition. This is not least because altering fundamental internet technologies will also alter the requirements of governance. There is not enough experience with bodies such as the Governmental Advisory Committee at the ICANN to understand how such competitions might play out, especially when the very technical and governmental fabric of cyberspace would be at stake. Much like the future internet architectures, novel cybersecurity governance may alter the requirements of governance and bring more national security considerations to the fore. Whether these changes generate light or heat, cybersecurity will alter internet governance in a profound way.

Note

1. I would like to acknowledge the work of Paul Ruizendaal, who located, digitized and analyzed early TCP implementations. In part through exchanges with Michael Wingfield, Ruizendaal discovered the link between the AUTODIN II and the Wingfield (University of California, Los Angeles) TCP implementation. Craig Partridge at Bolt Beranek and Newman organized the release of supporting documentation. Previously, Wingfield donated his code to the University of California, Los Angeles, Special Collections, which is where Ruizendaal located them. Our extensive exchanges on the relationship between TCP implementation code, the AUTODIN II and early internet extended and clarified my argument.

References

Abbate, J. (1999), *Inventing the Internet*, MIT Press, Cambridge, MA.

Barber, D.L.A. (1975), "Cost Project 11: a European informatics network", *SIGCOMM Computer Communication Review*, Vol. 5 No. 3, pp. 12-15.

Barbrook, R. and Cameron, A. (1996), "The Californian ideology", *Science as Culture*, Vol. 6 No. 1, pp. 44-72.

Bowker, G. and Star, S.L. (2000), *Sorting Things Out: Classification and its Consequences*, MIT Press, Cambridge, MA.

Braden, B. (1998), "The end-to-end research group - internet philosophers and "Physicists", available at: www.ietf.org/proceedings/41/slides/plenary-braden/

Brunton, F. (2013), *Spam: A Shadow History of the Internet*, MIT Press, Cambridge, MA.

Campbell-Kelly, M. and Garcia-Swartz, D.D. (2013), "The history of the internet: the missing narratives", *Journal of Information Technology*, Vol. 28 No. 1, pp. 18-33.

Cerf, V. (1973), *A Partial Specification of An International Transmission Protocol*, Stanford University, Stanford, CA.

Cerf, V.G. (1976), "SCCU/MCCU characteristics for AUTODIN II", DSL Technical Note, Defense Advanced Research Projects Agency Information Processing Techniques Office.

Cerf, V. (1978), "The Catenet model for internetworking", Internet Experiment Note, Defense Advanced Research Projects Agency Information Processing Techniques Office.

Cerf, V. (1980), "DoD protocol standardization", Internet Experiment Note, Defense Advanced Research Projects Agency Information Processing Techniques Office, Washington, DC.

Cerf, V. (2016), "Vinton G Cerf", interview by Bradley Fidler, available at Center for Oral History Research, University of California Los Angeles Library Special Collections.

Cerf, V. and Kahn, R. (1974), "A protocol for packet network internetworking", *IEEE Transactions Communications*, Vol. 22 No. 5, pp. 627-641.

Chen, S. and Mizero, F. (2015), "A survey on security in named data networking", arXiv:1512.04127 [cs], available at: http://arxiv.org/abs/1512.04127

Corrigan, M. (2015), "Interview with Michael Corrigan", interview by Bradley Fidler, available at Center for Oral History Research, University of California Los Angeles Library Special Collections.

Defense Communications Agency (1982), *Defense Data Network Program Plan*, Defense Communications Agency Command and Control Technical Center, Washington, DC.

Defense Communications Agency (1985), *ARPANET Information Brochure*, Defense Communications Agency, Washington, DC.

Deleuze, G. (1992), "Postscript on the societies of control", *October*, Vol. 59, pp. 3-7.

DeNardis, L. (2009), *Protocol Politics: The Globalization of Internet Governance*, MIT Press, Cambridge, MA.

DeNardis, L. (2012), "Hidden levers of Internet control: an infrastructure-based theory of Internet governance", *Information, Communication & Society*, Vol. 15 No. 5, pp. 720-738.

DeNardis, L. (2015), "The internet design tension between surveillance and security", *IEEE Annals of the History of Computing*, Vol. 37 No. 2, pp. 72-83.

Dinneen, G. (1978), "Host-to-host protocols for data communications networks", Under Secretary of Defense for Research and Engineering, Washington, DC.

Dinneen, G. (1980), "Host-to-host data communications protocols", Assistant Secretary of Defense, Communications, Command, Control, and Intelligence, Washington, DC.

DuPont, Q. and Fidler, B. (2016), "Edge cryptography and the codevelopment of computer networks and cybersecurity", *IEEE Annals of the History of Computing*, Vol. 38 No. 4, pp. 55-73.

Elsam, E. (1980), "COINS II/ARPANET: Private Line Interface (PLI) operations manual", Final Report, Bolt Beranek and Newman, Cambridge, MA.

Fidler, B. and Currie, M. (2016), "Infrastructure, representation, and historiography in BBN's Arpanet maps", *IEEE Annals of the History of Computing*, Vol. 38 No. 3, pp. 44-57.

Fidler, B. and Russell, A. (2018), "Infrastructure maintenance at the defense communications agency: recasting computer networks in the history of technology", *Technology and Culture*, Vol. 59 No. 4.

Fletcher, A.L. (2002), "France enters the information age: a political history of Minitel", *History and Technology*, Vol. 18 No. 2, pp. 103-119.

Gerovitch, S. (2008), "InterNyet: why the Soviet Union did not build a nationwide computer network", *History and Technology*, Vol. 24 No. 4, pp. 335-350.

Gross, P. (1986), *Proceedings of the 15-17 October 1986 Joint Meeting of the Internet Engineering and Internet Architecture Task Forces, MITRE Corporation, McLean, VA*.

Gross, P. (1987), *DRAFT Proceedings of the April 22-24, 1987 Internet Engineering Task Force, The MITRE Corporation, Washington, DC*.

Gross, P. and Bowers, K. (1989), *Proceedings of the Eleventh Internet Engineering Task Force*, Corporation for National Research Initiatives, Ann Arbor, MI, Reston, VA, 17-19 October.

Hafner, K. and Lyon, M. (1999), *Where Wizards Stay Up Late: The Origins of the Internet*, Simon and Schuster, New York, NY.

Heiden, H. (2015), "Interview with Heidi Heiden", interview by Bradley Fidler, available at Center for Oral History Research, University of California Los Angeles Library Special Collections.

Heiden, H.B. and Duffield, H.C. (1982), "Defense data network", *EASCON 82: 15th Annual Electronics and Aerospace Systems Conference, New York, NY*, pp. 61-75.

Herzfeld, C. (1990), "Oral history interview with Charles Herzfeld", available at: http://conservancy.umn.edu/handle/11299/107357 (accessed 19 June 2016).

IAB Executive Editor (2011) "History | Internet architecture board", Internet Architecture Board, available at: www.iab.org/about/history/ (accessed 30 June 2017).

Kahn, D. (1967), *The Codebreakers: The Story of Secret Writing*, Macmillan, New York, NY.

Kahn, R. (1975), *Memorandum for Technical Advisory Committee, Subject: Draft AUTODIN II Report*, Defense Advanced Research Projects Agency, Virginia.

Kent, S. (2015), "Interview with Stephen Kent", interview by Bradley Fidler, available at Center for Oral History Research, University of California Los Angeles Library Special Collections.

Kita, C.I. (2003), "J.C.R. Licklider's vision for the IPTO", *Annals of the History of Computing, IEEE*, Vol. 25 No. 3, pp. 62-77.

Krekel, B.A., Adams, P. and Bakos, G. (2012), *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Northrop Grumman Corporation, Virginia.

Kuerbis, B. and Mueller, M. (2017), "Internet routing registries, data governance, and security", *Journal of Cyber Policy*, Vol. 2 No. 1, pp. 64-81.

Lane, J. (2015), "Oral history with John Lane", interview by Bradley Fidler, available at Center for Oral History Research, University of California Los Angeles Library Special Collections.

Larkin, B. (2013), "The politics and poetics of infrastructure", *Annual Review of Anthropology*, Vol. 42 No. 1, pp. 327-343.

Leigh Star, S. (2010), "This is not a boundary object: reflections on the origin of a concept", *Science, Technology & Human Values*, Vol. 35 No. 5, pp. 601-617.

Licklider, J.C.R. (1963), *Topics for Discussion at the Forthcoming Meeting, Memorandum For: Members and Affiliates of the Intergalactic Computer Network*, Advanced Research Projects Agency, Washington, DC.

Linn, J. (1987), "Privacy enhancement for internet electronic mail: part I: message encipherment and authentication procedures", Request for Comments, BBNCC, available at: www.rfc-editor.org/info/rfc989 (accessed 30 June 2017).

Lipner, S.B. (2015), "The birth and death of the orange book", *IEEE Annals of the History of Computing*, Vol. 37 No. 2, pp. 19-31.

Lyons, R. (1980), "A total AUTODIN system architecture", *IEEE Transactions on Communications*, Vol. 28 No. 9, pp. 1467-1471.

McKenzie, A. (2011), "INWG and the conception of the internet: an eyewitness account", *IEEE Annals of the History of Computing*, Vol. 33 No. 1, pp. 66-71.

Mackenzie, D. (2001), *Mechanizing Proof: Computing, Risk, and Trust*, The MIT Press, Cambridge, MA.

Mathison, S.L., Roberts, L.G. and Walker, P.M. (2012), "The history of telenet and the commercialization of packet switching in the US", *IEEE Communications Magazine*, Vol. 50 No. 5, pp. 28-45.

Maybaum, L. (2015), "Interview with Lee Maybaum", interview by Bradley Fidler, available at Center for Oral History Research, University of California Los Angeles Library Special Collections.

Medina, E. (2011), *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*, MIT Press, Cambridge, MA.

Metz, C. (2012), "Meet the man who invented the instructions for the internet", *Wired*, available at: www.wired.com/2012/05/steve-crocker/ (accessed 19 June 2016).

Misa, T.J. (2016), "Computer security discourse at RAND, SDC, and NSA (1958-1970)", *IEEE Annals of the History of Computing*, Vol. 38 No. 4, pp. 12-25.

Mueller, M.L. (2002), *Ruling the Root: Internet Governance and the Taming of Cyberspace*, MIT Press, Cambridge, MA, available at: https://books.google.com/books?hl=en&lr=&id=Vy1mDQAAQBAJ&oi=fnd&pg=PR5&dq=milton+mueller&ots=dBb3szd2GR&sig=8NHhLiZeaRldyUCMZG6CndipvnQ (accessed 22 April 2017).

Mueller, M.L. (2010), *Networks and States: The Global Politics of Internet Governance*, MIT Press, Cambridge, MA, available at: https://books.google.com/books?hl=en&lr=&id=qH3TAvkAtsEC&oi=fnd&pg=PP1&dq=milton+mueller&ots=3KoLA8who2&sig=KCdcZt3V9daAAgQBWekv_fOLLMc (accessed 22 April 2017).

Mueller, M., Schmidt, A. and Kuerbis, B. (2013), "Internet security and networked governance in international relations", *International Studies Review*, Vol. 15 No. 1, pp. 86-104.

Mundy, R. (2015), "Interview with Russ Mundy", interview by Bradley Fidler, available at Center for Oral History Research, University of California Los Angeles Library Special Collections.

Norberg, A.L. (1996), "Changing computing: the computing community and DARPA", *Annals of the History of Computing, IEEE*, Vol. 18 No. 2, pp. 40-53.

Norberg, A.L., O'Neill, J.E. and Freedman, K.J. (1999), *Transforming computer technology: information processing for the Pentagon, 1962-1986*, Johns Hopkins University Press, Baltimore.

Pan, J., Paul, S. and Jain, R. (2011), "A survey of the research on future internet architectures", *IEEE Communications Magazine*, Vol. 49 No. 7, pp. 26-36.

Park, D. (2015), "Social life of PKI: sociotechnical development of Korean public-key infrastructure", *IEEE Annals of the History of Computing*, Vol. 37 No. 2, pp. 59-71.

Pearson, D.E. (2000), *The World Wide Military Command and Control System Evolution and Effectiveness*, DIANE Publishing, Collingdale, PA.

Peters, B. (2016), *How Not to Network a Nation: The Uneasy History of the Soviet Internet*, The MIT Press, Cambridge, MA.

Postel, J. (1978a), "Internet Meeting Notes - 30 & 31 October 1978", Internet Experiment Note.

Postel, J. (1978b), "Internet Meeting Notes - 14 & 15 July 1977", Internet Experiment Note.

Postel, J. (1981a), "Internet Protocol", Request for Comments, University of Southern California Information Sciences Institute, California, available at: www.rfc-editor.org/info/rfc791 (accessed 30 June 2017).

Postel, J. (1981b), "Transmission control protocol", Request for Comments, University of Southern California Information Sciences Institute, California, available at: www.rfc-editor.org/info/rfc793 (accessed 30 June 2017).

Postel, J.B., Garlick, L.L. and Rom, R. (1976), *Transmission Control Protocol Specification*, Stanford Research Institute Augmentation Research Center, Melno Park, CA.

Pouzin, L. (1973), *Interconnection of Packet Switching Networks*, International Packet Network Working Group (INWG), Reseau Cyclades.

Rosen, E.C. (1982), "Exterior Gateway Protocol (EGP)", Request for Comments, Bolt Beranek and Newman, Cambridge, available at: www.rfc-editor.org/info/rfc0827 (accessed 30 September 2015).

Ruizendaal, P. (2017), "BBN Unix release OK", 9 May 2017.

Russell, A.L. (2014), *Open Standards and the Digital Age: History, Ideology, and Networks*, Cambridge University Press, New York, NY.

Russell, A.L. and Schafer, V. (2014), "In the shadow of ARPANET and internet: Louis Pouzin and the cyclades network in the 1970s", *Technology and Culture*, Vol. 55 No. 4, pp. 880-907.

Salus, P.H. (1995), *Casting the Net: From ARPANET to INTERNET and Beyond*, 1 edition, Addison-Wesley Professional, Reading, MA.

Sevcik, P. (2015), "Interview with Peter Sevcik", interview by Bradley Fidler, available at Center for Oral History Research, University of California Los Angeles Library Special Collections.

Slayton, R. (2015), "Measuring risk: computer security metrics, automation, and learning", *IEEE Annals of the History of Computing*, Vol. 37 No. 2, pp. 32-45.

SSAC (2014), "Overview and history of the IANA functions", ICANN Security and Stability Advisory Council, Internet Corporation for Assigned Names and Numbers.

Strazisar, V. and Perlman, R. (1978), "Gateway routing: an implementation specification", Internet Experiment Note.

Swope, R.L. (1988), "Modeling the merger of the classified networks of the DDN (Defense Data Network): BLACKER", DTIC Document, available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA206176 (accessed 3 April 2015).

Taylor, R.W. (1989), "Oral history interview with R. W. Taylor", available at: http://conservancy.umn.edu/handle/11299/107666 (accessed 19 June 2016).

Timberg, C. (2015), "Quick fix for an early Internet problem lives on a quarter-century later", *Washington Post*, 31st May, available at: www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/ (accessed 17 January 2016).

Voydock, V.L. and Kent, S.T. (1981), *Security in Higher Level Protocols: Approaches, Alternatives, and Recommendations*, Bolt Beranek and Newman, Cambridge, MA.

Warner, M. (2015), "Notes on the evolution of computer security policy in the US Government, 1965-2003", *IEEE Annals of the History of Computing*, Vol. 37 No. 2, pp. 8-18.

Weissman, C. (1992), "BLACKER: security for the DDN examples of A1 security engineering trades", *Research in Security and Privacy, Proceedings, IEEE Computer Society Symposium, on IEEE*, pp. 286-292, available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=213253 (accessed 3 April 2015).

Winner, L. (1997), "Cyberlibertarian myths and the prospects for community", *ACM SIGCAS Computers and Society*, Vol. 27 No. 3, pp. 14-19.

Yost, J.R. (2015), "Computer security [Guest editors' introduction]", *IEEE Annals of the History of Computing*, Vol. 37 No. 2, pp. 6-7.

Yost, J.R. (2016), "Computer security, Part 2", *IEEE Annals of the History of Computing*, Vol. 38 No. 4, pp. 10-11.

Further reading

McKenzie, A., Cosell, B.P., McQuillan, J.M. and Thorpe, M.J. (1972), "The network control center for the ARPA network", *Proceedings of the First International Conference on Computer Communication, Washington, DC*, pp. 185-191.

About the author

Bradley Fidler is Assistant Professor of Science and Technology Studies at the Stevens Institute of Technology. He is a historian of computing, and studies internet protocols, architecture and security. He is online at brfidler.com. Bradley Fidler can be contacted at: bradley.reuben.fidler@gmail.com