Security as a Context, Generative Force, and Policy Concern for the Co-Production of Cyberspace: Historical Overview Since WWII Until the end of the Cold War

Noran Shafik Fouad
University of Sussex, UK
n.fouad@sussex.ac.uk

Abstract: Many cybersecurity literature take the 1990s as a starting point to trace the process of securitising cyberspace; implicitly suggesting that it initially emerged as a non-security sector, which was then securitised. Although it is true that 'cyberspace' and 'cybersecurity' were novel terms at that period, their ontological status cannot be reduced to their mere utterances. If the security of cyberspace as a constructed metaphor signifies the security of computers and networks, with all their associated software, hardware, and data - technologies that have long historical roots - then an ahistorical approach to studying its evolution would be both insufficient and over-simplified. Therefore, this paper aims to prove that security has always been an integral part of the co-production of cyberspace: As a context in which it was developed, as a generative force behind many of its technologies, and as a policy concern in different phases of its evolution, since the emergence of the first computer till the advent of the internet. It seeks to prove that the history of cyberspace is better analysed as a complex process of restructuring, not just technically, but also politically and socially, in which the interests of various actors competed, and security considerations were intertwined with technical ones, and in many respects coproduced them. This analysis is important to show that security was not imposed on cyberspace by political discourses, but has always been intrinsic to the existence of its components and technologies. Besides, it challenges the deterministic accounts of the development of computers and networks, which present them in an idealistic, utopian image as being solely products of civilian and academic efforts.

Keywords: cybersecurity, cyberspace, internet history, computer history, co-production

1. Introduction

The story of cybersecurity is often told as a new one, dating back to the 1990s, when the term was first used in policy circles in the US, after being coined in a science fiction novel in 1984. This periodisation is related to what 'security' and 'sector' are taken to mean in the study of cybersecurity. In the majority of cybersecurity literature, security is tied to questions of survival and existential threats, and is performed by the government as the principal securitising actor. This state-centric approach implies that new sectors are only envisioned as 'security' sectors once they make their way to policymakers' discourses, and that as long as threats are not portrayed as existential, their 'securityness' would not be admitted.

Nevertheless, if this logic of security is relaxed, and a multi-actor approach is adopted, the ontological status of cyberspace as a security sector would necessitate a historical analysis of the conceptual evolution of that *security* since the emergence of the first computer till the advent of the internet. Accordingly, this paper aims to prove that security has always been an integral part of the development of cyberspace: As a context in which it was developed, as a generative force behind many of its technologies, and as a policy concern in different phases of its evolution.

Here, two important points need to be clarified about the historical account this paper is proposing. Firstly, although some roots of cyberspace can be found in other electronic devices before WWII, like punch cards, the development of computers and networks were chosen as starting points given their clearer links to the sort of modern cyberspace that we experience nowadays. Secondly, this paper does not claim to provide a detailed, inclusive historical explanation of the evolution of computers and the internet, it rather aims at briefly re-reading their history through a security lens. This approach challenges the deterministic accounts of the development of information and communication technologies (ICTs), which present them as solely products of civilian and academic efforts. Likewise, we neither deny the validity of this strand of literature entirely, nor do we make a reductionist statement that everything in this history is *security* or security-related.

To that end, this paper will draw on 'co-production' as an idiom developed in the science and technology studies (STS) literature to contextualise the production of scientific knowledge. It thus explores the role security played in the 'co-production of cyberspace', arguing that its history is better analysed as a complex process of restructuring, not just technically, but also politically and socially, in which the interests of various actors

competed, and security considerations were intertwined with technical ones, and in many respects *co-produced* them.

2. Security as a context: The Cold War and the securitisation of science

Studying the development of cyber technologies cannot be done in isolation from the security context of the Cold War, which had far-reaching implications on scientific research as a whole, and the military-civilian partnerships that were formed to advance it. During that period, two main instruments of co-production established a robust link between science and security: Discourses and institutions.

2.1 Discourses of scientific wars and apocalyptic conflicts

The STS literature asserts the significance of language as one instrument of co-production, used to prove the practical relevance of scientific knowledge, and present convincing accounts to 'sceptical audiences' (Jasanoff, 2004). These functions were performed by two discourses in the US during the Cold War: One that portrayed WWII as a 'scientific war', and another that amplified the fear from an apocalyptic conflict with the USSR.

The Second World War was framed as a scientific war won by technological advancements through the military's collaboration with the academia, given the decisive role of the atomic bomb in ending the war and of the radar in winning it (Campbell-Kelly et al., 2013). Following the end of the war, there was a strong belief in both the US and the USSR that science can still win the Cold War for one of them, thus advancement in science and technology became an integral part of their security strategies (Wolfe, 2013).

Together with the fear from an apocalyptic conflict with the Soviet Union (Chernus, 2008), this discourse contributed to raising the R&D budget even higher than the war time, with the biggest share coming from the armed forces. Even after the National Science Foundation (NSF) was established in 1951 as a civilian institution to aid research, only 20% of computer research for instance was funded by it, while 50-70% received funds from the Department of Defence (DoD) (Edwards, 1997). That is what Eisenhower referred to as 'the military-industrial complex' (Eisenhower, 1960), and others called the 'military-industrial-academic complex' (Leslie, 1993).

2.2 Institutions of co-production: ONR and ARPA as examples

Institutions play an important role in validating and accrediting knowledge, testing political culture, and providing credibility for scientific research (Jasanoff, 2004). One important institution that performed those functions during the Cold War was the Office of Naval Research (ONR), established in 1946, as the first military agency to finance basic, unclassified research in academic and industry laboratories. The ONR had the influential role of shaping and legitimising the relationship between governments and science for many years.

Since it was the only federal agency to finance research immediately after the war, the ONR used its contractual authority to shape science policies, by selecting the fields, institutions, and individuals to be funded. Security imperatives were a major consideration for the ONR's contracts, particularly after the 1950s, with the rising congressional pressure to prove the relevance of research to national security and defence purposes (Sapolsky, 1990).

The Advanced Research Projects Agency (ARPA) was another institution that influenced the post-war scientific research, particularly in fields like networking. ARPA was established in 1958, as a research agency affiliated to the DoD, following the surprising launch of the Sputnik satellite by the Soviet Union, creating a fear from a growing 'scientific gap' that could allow the Soviets to attack the US with ballistic missiles. Consequently, ARPA was established with the responsibility of keeping the US more technologically advanced than its adversaries, and preventing any surprising events like Sputnik. And since it did not have its own laboratories, ARPA contracted academic institutions to run scientific projects that combine civilian and military needs (Norberg and O'Neill, 2000).

Hence, it could be argued that ONR and ARPA were products of existing processes of scientific and technological co-production, mediated in part by discourses of the scientific gap and the fear of a Soviet attack. They were also a co-production agent, that shaped the post-war scientific research, combining a complex set of scientific and military interests. That is, security was an integral part of the discursive and institutional tools of the co-

production of scientific and technological research during the Cold War, not just as a *contextual* influence, but also a *generative force*.

3. Security as a generative force: The co-production of computing and internetworking technologies

The academic literature on the history of computers and networks is full of scientifically deterministic approaches that present utopian images of their development by focusing on the success stories of their individual inventors (Hafner & Lyon, 1998; Lavington, 2012), while very few acknowledge the influence of the DoD and security considerations on the process.

Additionally, some studies make an implicit argument that the evolution of computers and networks came naturally and was completely unplanned by their initial inventors. This is true in many respects, since computers started as calculating devices in the 1940s, and were then developed into a 'networked information appliance' by the 1990s (Ceruzzi, 2003). The same applies to the internet, since the first network that resembles today's internet, the ARPANET, was designed to facilitate recourse-sharing among academics, not interpersonal communications (Abbate, 1999).

However, this should not lead to a conclusion that such 'unplanned processes' were necessarily accidental, and consequently undermine the analysis of their socio-political context. As argued by Jasanoff, "The design of technology is likewise seldom accidental; it reflects the imaginative faculties, cultural preferences and economic or political resources of their makers and users" (Jasanoff, 2004, p. 14). Scientific research is better thought of as a 'supply' to a 'demand', which goes beyond the endeavours of science (Sarewitz and Pielke, 2007). Consequently, by assuming that computers and the internet were *co-produced* rather than *invented*, this section will highlight the generative influences of security as an inherent part of the demand for these technologies, which necessarily shaped their supply.

3.1 Security and the evolution of computers

From the 1940s till the 1960s, the US military was the main driving force behind technological developments in computers, not just through funding as part of the US grand strategy during the Cold War, but also by being the main customer for computer products. Even though most of computer research was conducted by universities and commercial laboratories, it was funded by the military and guided by its needs.

The first instance of the generative force of security in the development of computers goes back to the Colossus, the first electronic computer, developed in 1943 by scientists contracted by the British government to decrypt adversaries' ciphers. Although the foundational idea behind digital computers was published in 1937, only the defence purposes of the war stimulated its application (Randell, 1982). This emergence of electronic machines gave rise to several computer-related disciplines, including cybernetics and artificial intelligence, and was transferred to other military applications, such as communication, intelligence, and command and control (Edwards, 1997). The Colossus, together with a machine called the 'Bombe' developed to break the Enigma, a German cipher machine, sparked several computer projects outside the UK, particularly in the US, which took the lead in advancing computer research following the end of the war (Randell, 1982).

Another machine that was generated out of the security imperatives of the war is the Electronic Numerical Integrator and Computer (ENIAC). The need for automated ballistic calculations for the army encouraged the development of ENIAC, financed by the Ballistic Research Laboratory (BRL), an army affiliate (Burks, 2014). It is safe to assume here that if it was not for the security needs of the war, the ENIAC would not have been developed, as it was rejected and deemed as overly radical by the scientific community at that time (Flamm, 1988).

The BRL continued to finance the development of the ENIAC into the EDVAC (Electronic Discrete Variable Automatic Computer); another military machine created to aid in a variety of tasks, including the development of a hydrogen bomb. The EDVAC marked the birth of internal programming, unlike the ENIAC which was externally-programmed (Watson, 2012). The ENIAC and the EDVAC presented one big step in the history of government's support of 'big science', especially that the amount of money these projects required was beyond the capacity of the private sector (Edwards, 1997).

Furthermore, the security needs of the military encouraged a sceptical private sector, that did not initially acknowledge the importance of electronic computers, to get involved. For instance, the International Business Machines Corporation (IBM), which later dominated the production of computers, was reluctant to enter the market until the military needs during the Korean war pushed it to develop a computer called 'IBM Defence Calculator' or '701', sold to the military for analysing trajectories (Flamm, 1988).

The ENIAC and EDVAC also gave a boost to a crucial computer project that influenced the development of several technologies afterwards: The Whirlwind. Project Whirlwind was started by MIT to create a flight simulator for pilots training for the US air force. Following the end of the war, it was integrated in the new computer-controlled air defence system, called the Semi-Automatic Ground Environment (SAGE). The sophistication of SAGE led to the development of various technologies that shaped today's computers, such as real-time computing, modems, video and graphical displays (Agar, 2012).

Programming languages was also one significant milestone in computer development, which owes a lot of its success to the military. Two main programming languages were developed since the start of the 1960s: Cobol and Fortan. Fortan was introduced by IBM and proved successful because of IBM's domination of the market (Ceruzzi, 2012). On the other side, though it was a business-oriented language, the DoD not only pushed for the development of Cobol, it also encouraged its standardisation by announcing that 'it would not lease or purchase a computer without a COBOL compiler' (Vee, 2017, pp. 108–109).

To conclude, the security context of WWII, followed by the Cold War, encouraged the government to invest in computer projects that seemed risky and unsellable for the private sector. Yet, focusing on the security imperatives in the co-production of computers does not deny the other forces that influenced this process. What this section and the following one aim to achieve, on the contrary, is illuminating an often-ignored role of security as one significant generative force behind those technologies.

3.2 Security and the evolution of the internet

The development of the internet can be described as an 'organised chaos', produced by the overlapping interests of ARPA, NSF, programmers, developers, and even users (Marson, 1997). Both military and academic interests contributed to the evolution of a civilian internet, while corporate networking was initially sponsored by the state (Murphy, 2002).

Although the first network that resembles today's internet, the ARPANET, was not developed as a military network, the technology upon which it was based was generated out of security considertions. ARPANET was enabled by packet-switching, originally developed in the 1960s to secure the survivability of military communications by distributing them among different nodes to survive on redundancy in case of a strike (Ryan, 2010). Yet, the radical nature of the idea hindered its immediate application; only in the 1970s when ARPANET was created did packet-switching appear as a sound foundation for networking. ARPA financed the ARPANET project as the first version of a distributed network to allow its contracted academic institutions to remotely share their expensive computers (Brendon, 2001). However, despite not being a military network, ARPANET was used for seismology and defence-oriented climate research, and was not entirely an 'academic' network, given the participation of the Army and the Air Force in it (Abbate, 1999).

Security needs also encouraged the application of packet-switching to two communication technologies used by the military in the 1970s: Radio and satellites. A network called PRNET was established by ARPA to secure the military's command and control through radio packets, and another one under the name SATNET was created for the transfer of the military's seismic data. The existence of three heterogeneous networks - ARPANET, PRNET, and SATNET - and the needs to connect them was a stimulating idea for the development of internetworking protocols, TCP/IP, as one cornerstone of the modern internet's architecture (Ryan, 2010).

Furthermore, the military had an important role in the expansion of the network by obliging academic institutions contracted by ARPA to join it and mandatorily implement TCP/IP, despite the resistance of some to the idea of resource-sharing and internetworking (Ruttan, 2006). Additionally, the military's interest in a tightened security system for authentication and information-sharing was a first step towards the civilian internet. This was done by breaking the network down into two distinct ones: A military network, MILNET, where

a strict security system was implemented, and ARPANET continuing as a research network, and thus facilitating its expansion in the 1980s (Abbate, 1999).

The final and most critical step in opening the internet to the public was the privatisation of its backbone and the permission of its commercial use. The internet privatisation was neither easy nor inevitable, and was influenced by several technical, social, and political aspects, as well as the security considerations of the Cold War. The privatisation process was facilitated by the national security strategy of the US, and the perceived scientific gaps between the US and other international actors. This period witnessed wide congressional debates on funding supercomputers and networking, particularly in 1982, after Japan launched a project to supersede the US in artificial intelligence research. Consequently, data networking became an integral part of the national policy agenda, and the Congress endorsed the public access of the internet. This all facilitated the process of privatising the internet's backbone, which was completed by 1993 (Abbate, 2010).

That is to say, the military's support, both in providing funds and creating a market demand, proved crucial in the evolution of the internet, starting from the early days of ARPA's adoption of packet-switching, to the development of the new technologies of satellite and radio switching, all facing a highly sceptical academic community. Moreover, the diversity of the military operations produced a philosophy of decentralisation and heterogeneity in dealing with the network, as opposed to the industry's sponsored centralisation (Hicks, 1998).

If military security had influenced the co-production of cyberspace as argued, the question now is: Has the security of cyberspace per se been considered as a policy concern since the early stages of its development? The following section will explain why the answer to this question is certainly *yes*.

4. Security as a policy concern: From computer and internet security to cybersecurity

As a policy concern, the security of computers and networks has long historical roots, since the introduction of the very first computer. In each stage, this security was conceptualised differently, with diverse threat perceptions, referent objects, and utterances that reflect the technology's development state.

4.1 Physical security, unauthorised access, and software bugs

In its early stages, computer security was mainly focused on three main issues: Physical security, unauthorised access, and software bugs; such threats defined what constituted a 'computer crime' at that time. This conceptualisation of security reflected a belief in the controllability of machines, i.e. threats are external to the machines and are calculable and controllable, and therefore defendable.

Among the early perceived threats to the physical security of computer systems was the electronic radiations emanating from mainframe computers, that allowed spies to decipher communications over computer systems (Yost, 2007). Therefore, during the 1950s, the government announced its first security standards for emanation levels, and the DoD obliged vendors to abide by them before they can sell any computer equipment to the government (Russell and Gangemi, 1991). Computer sabotage and manipulation did exist at that time, but were mainly physical and performed by insiders (Brenner, 2007).

The growth of time-sharing in the late 1960s was perceived as an additional threat that could intensify unauthorised access. Therefore, a task force was established by the Defence Science Board in 1967 to examine ways through which the computer security standards of military environments could be applied to open environments. With resource-sharing also came the concerns over data privacy. As a result, national standards for cryptography were announced, and several companies began to invest heavily in encrypting their communications (Yost, 2007).

Another important security concern in that period was software bugs. As more people were getting involved in the process of software design, 'program correctness', or fixing buggy software, became an important field of computer security, which in turn was established as an independent field of research in 1974 (Meijer et al., 2007).

On the legal and policy side, there were some attempts to face the rising threat of computer crimes, defined at that time as any physical destruction or unauthorised access to computer systems. This includes the Federal

Computer Systems Protection Act, introduced in the Congress in 1977. Though it was not adopted, it marked the first step towards recognising the security aspects of computer systems by the legislature (Easttom, 2011).

4.2 Malicious hacking and malware

During the 1960s and 1970s, hacking was approached positively, as part of the process of developing computer technologies. However, the emergence of networking, the commodification of information, and the 'digital fences' implemented in computer systems with increased privatisation, created a 'cyber e-capital' that required protection. Therefore, the hacking culture started to be met with resistance, and a distinction was made between hackers (explorers) and crackers (robbers) (Dyer-Witheford, 2002).

Similarly, since the 1950s, viruses and worms were part of the architecture of internetworking, as an essential tool for testing and experimenting the network. Nevertheless, many incidents starting the 1980s shifted the emphasis of computer security to malicious hacking and malwares as a security threat to networks and computers (Parikka, 2007). This transformed security conceptualisation in the field towards threats emanating from the machine, characterised by uncertainty and incalculability. Consequently, the logics of risk-management, governance, and resilience began to go side-by-side with the logics of defence, creating a security-risk nexus in the conceptualisation of cybersecurity.

Examples include the first malicious virus to ever be reported in 1981/1982, infecting Apple II computer system; the 'Brain virus' targeting Microsoft's DOS in 1986 (Skoudis and Zeltser, 2004); Ian Murphy's hacking into the AT&T system (Brenner, 2007); and the Morris worm in 1988, which infected an estimated number of 6000 computers and led to the establishment of a Computer Emergency Response Team (CERT) by the DoD (DeNardis, 2007).

As those operations were becoming more frequent and sophisticated, legislations to counter them were also developing. The first federal legislation on cybercrimes under the title "Computer Fraud and Abuse Act" was issued in 1986 (Easttom, 2011). Several publications in that period also mark this rising concern over computer and internet security, such as 'the orange book': A report published by the DoD in 1983, creating a common language for communication over computer security (Yost, 2007). The academic literature of the 1980s also reveals this shift from physical security towards software and hardware vulnerabilities, and the belief in the uncontrollability of machines (Fine, 1982).

5. Conclusion

This paper challenged the idea that cyberspace emerged as a purportedly non-securitised sphere which was then securitised. It did so by demonstrating how security has been an important contextual influence, generative force, and policy concern in different stages of the evolution of 'cyberspace'. It used the idiom of co-production to refute the perception of science and security as necessarily antagonistic, which drove many literature on computer and internet history to present deterministic arguments on their development, by overlooking the influence of the military and the security imperatives of the Cold War.

As a context, security was an indispensable element of the discursive and institutional tools of the co-production of scientific knowledge during the Cold War, which the internetworking and computing research was part of. Perceptions of the 'scientific gap' and discourses that weaponised science were institutionalised, such as in the cases of the ONR and ARPA, and utilised by those institutions in legitimising the influence the military exerted on scientific research, even on what academics regarded as 'pure science'.

As a generative force, security contributed to the evolution of computers and the internet, not just through the funding power of the military, but also by creating a market demand that shaped the supply of both technologies, and consequently their development path, for many years. The foundational ideas that modern computers and the internet are based on, such as digital computations and packet-switching, were primarily generated by the war and post-war security needs, in a context of scepticism by both the scientific community and the private sector.

As a policy concern, the security of computers and networks was always present, though with different conceptualisation. Originally, when computers operated in controlled environments, there was an understanding of machines as necessarily controllable, and of threats as always extrinsic to them. Yet, following

the advent of networking and the dissemination of computers, the machines themselves began to be perceived as possibly threatening through software and hardware vulnerabilities.

However, arguing that cybersecurity is not new or ahistorical does not undermine the significant influences of 'cyberspace' as an unorthodox metaphor emerging in the 1990s. On the contrary, it further acknowledges this influence, but as more of *transformational* than *creational* for cybersecurity. Cyberspace as a discourse exerts a territorial influence on the spatial connotations of 'computer networks' and the place-less underpinnings of 'virtual reality'. Yet, this does not deny the fact that the security of cyber technologies is as old as those technologies themselves.

Acknowledgements

This paper is part of my PhD research, which is funded by the University of Sussex's Chancellor International Research Scholarship. I would also like to thank my PhD supervisors, Prof. Stefan Elbe and Dr. Stefanie Ortmann, for their feedback.

References

Abbate, J. (2010) "Privatizing the Internet: Competing Visions and Chaotic Events, 1987–1995", *IEEE Annals of the History of Computing*, Vol. 32, No. 1, pp 10-22.

Abbate, J. (1999) *Inventing the Internet, Inside technology*, MIT Press.

Agar, J. (2012) *Science in the 20th Century and Beyond*, Polity.

Brendon, L.K. (2001) "ARPANET: An Efficient Machine as Social Discipline", *Science as Culture*, Vol. 10, No. 1, pp 73–95.

Brenner, S.W. (2007) "History of Computer Crime", in: de Leeuw, K.M.M., Bergstra, J. (Eds.), *The History of Information Security. Elsevier Science*, B.V., Amsterdam, pp 705–721.

Burks, A.W. (2014) "From ENIAC to the Stored-Program Computer: Two Revolutions in Computers, in: Metropolis, N. (Ed.), *History of Computing in the Twentieth Century*, Elsevier, pp 311–344.

Campbell-Kelly, M. et al (2013) *Computer: A History of the Information Machine,* Routledge.

Ceruzzi, P. (2012) *Computing: A Concise History*, MIT Press.

Ceruzzi, P.E. (2003) *A History of Modern Computing*, MIT Press.

Chernus, I. (2008) *Apocalypse Management: Eisenhower and the Discourse of National Insecurity*, Stanford University Press.

DeNardis, L. (2007) "A History of Internet Security", in: de Leeuw, K.M.M., Bergstra, J. (Eds.), *The History of Information Security*, Elsevier Science B.V., pp 681–704.

Dyer-Witheford, N. (2002) "E-Capital and the Many-Headed Hydra", in: Elmer, G. (Ed.), *Critical Perspectives on the Internet*, Rowman & Littlefield, pp 129–164.

Easttom, C. (2011) *Computer Crime, Investigation, and the Law*, Cengage Learning.

Edwards, P.N. (1997) *The Closed World: Computers and the Politics of Discourse in Cold War America*, MIT Press.

Eisenhower, D.D. (1960) *Public Papers of the Presidents of the United States, Dwight D. Eisenhower: Containing the Public Messages, Speeches, and Statements of the President, January 20, 1953 to January 20, 1961*. U.S. Government Printing Office.

Fine, L.H. (1982) "The Total Computer Security Concept and Security Policy", *EDPACS*, Vol. 10, pp 1–20.

Flamm, K. (1988) *Creating the Computer: Government, Industry, and High Technology*, Brookings Institution Press.

Hafner, K., Lyon, M. (1998) *Where Wizards Stay Up Late: The Origins of the Internet*, Simon & Schuster.

Hicks, C.R. (1998) "Places in the Net: Experiencing Cyberspace", *Cultural Dynamics*, Vol. 10, No.1, pp 49–70.

Jasanoff, S. (Ed.) (2004) *States of Knowledge: The Co-production of Science and the Social Order*, Routledge.

Lavington, S. (2012) *Alan Turing and His Contemporaries: Building the World's First Computers*, BCS.

Leslie, S. (1993) *The Cold War and American Science: The Military-Industrial-Academic Complex at MIT and Stanford*, Columbia University Press.

Marson, S.M. (1997) "A Selective History of Internet Technology and Social Work", C*omputers in Human Services*, Vol. 14, pp 35–49.

Meijer, H. et al (2007) "Computer Security Through Correctness and Transparency", in: de Leeuw, K.M.M., Bergstra, J. (Eds.), *The History of Information Security,* Elsevier Science B.V., pp 637–653.

Murphy, B.M. (2002) "A Critical History of the Internet", in: Elmer, G. (Ed.), *Critical Perspectives on the Internet*, Rowman & Littlefield, pp 27–48.

Norberg, A.L., O'Neill, J.E. (2000) *Transforming Computer Technology: Information Processing for the Pentagon, 1962-1986*, Johns Hopkins University Press.

Parikka, J. (2007) *Digital Contagions: A Media Archaeology of Computer Viruses*, Peter Lang Publishing Inc.

Randell, B. (1982) "Colossus: Godfather of the Computer", in: Randell, B. (Ed.), *The Origins of Digital Computers, Texts and Monographs in Computer Science*, Springer, pp 349–354.

Russell, D., Gangemi, G.T. (1991) *Computer Security Basics*, O'Reilly Media, Inc.

Ruttan, V.W. (2006) *Is War Necessary for Economic Growth?* Oxford University Press.

Ryan, J. (2010) *A History of the Internet and the Digital Future*, Reaktion Books.

Sapolsky, H.M. (1990) *Science and the Navy: The History of the Office of Naval Research*, Princeton University Press.
Sarewitz, D., Pielke, R.A. (2007) "The Neglected Heart of Science Policy: Reconciling Supply of and Demand for Science", *Environmental Science and Policy*, Vol. 10, pp 5–16.
Skoudis, E., Zeltser, L. (2004) *Malware: Fighting Malicious Code*, Prentice Hall Professional.
Vee, A. (2017) *Coding Literacy: How Computer Programming is Changing Writing*, MIT Press.
Watson, I. (2012) T*he Universal Machine: From the Dawn of Computing to Digital Consciousness*, Springer Science & Business Media.
Wolfe, A.J. (2013) C*ompeting with the Soviets: Science, Technology, and the State in Cold War America*, Johns Hopkins University Press.
Yost, J.R. (2007) "A History of Computer Security Standards", in: de Leeuw, K.M.M., Bergstra, J. (Eds.), *The History of Information Security,* Elsevier Science B.V., pp 595–621.