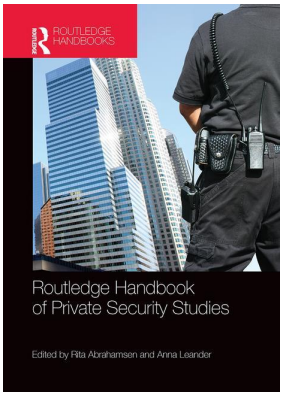

Routledge Handbook of Private Security Studies

Rita Abrahamsen, Anna Leander

Cyber-Security and Private Actors

Publication details
https://www.routledgehandbooks.com/doi/10.4324/9781315850986-10
Myriam Dunn Cavelty
Published online on: 20 Oct 2015

9

CYBER-SECURITY AND PRIVATE ACTORS

Myriam Dunn Cavelty

In the last few years, cyber-security has received much attention internationally. Events and occurrences such as the cyber-attacks on Estonia in 2007; the discovery of Stuxnet, the industry-sabotaging super worm in 2010; numerous instances of cyber-espionage, culminating in the Snowden revelations in 2013; and the growing sophistication of cyber-criminals as evident by their impressive scams served to give the impression that cyber-attacks are becoming more frequent, more organized, more costly, and altogether more dangerous. As a result, cyber-fears have percolated upwards, from the expert level to executive decision-makers and politicians, and diffused horizontally, advancing from mainly being an issue of relevance to the US to one that is at the top of the threat list of more and more countries, resulting in a flurry of government-led and private-led cyber-security initiatives.

Cyber-security research has grown in parallel to this rising prominence (see Figure 9.1) – even if at a much slower pace than could be expected for such a fashionable topic, especially in international relations and security. This chapter will focus on the literature dealing with cyber-security issues of relevance to private security studies. The link between the two topics seems a given: due to privatization and deregulation of many parts of the public sector, almost all critical cyber-assets are in the hands of private enterprise nowadays. This means that the state is incapable of providing the public good of security on its own. To embed this discussion sufficiently, the chapter will show what the particularities of cyber-security as a (national) security issue are and how elusive the concept of cyber-security is, especially since it has different meanings for different stakeholders and over time.

In contrast to a focus on specific threat forms like cyber-crime, cyber-terrorism, or cyber-war (which is predominant in the literature), only a broad understanding of cyber-security as practice involving a multitude of actors inside and outside of government reveals the whole range of effects of cyber-security politics, since multiple actors use different threat representations employing differing political, private, societal, and corporate notions of security to mobilize (or de-mobilize) different audiences. Therefore, a broad definition of cyber-security is used. It understands cyber-security as a multifaceted set of technologies, processes and practices designed to protect networks, computers, programmes and data from attack, damage or unauthorized access, in accordance with the common information security goals: the protection of confidentiality, integrity and availability of information.

The chapter has four parts. It starts with a discussion of concepts, particularly focusing on

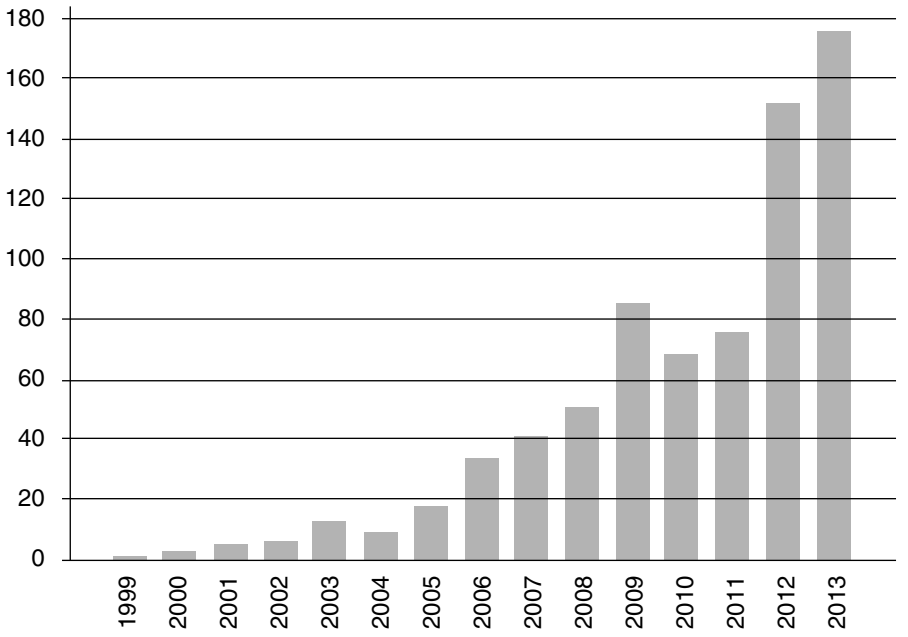

Figure 9.1 Published items in each year with topic cyber-security
Source: Web of Science.

the link between cyber-security and cyberspace. The second part shows how a national security connotation has been established and how and why it varies over time. The third and fourth parts discuss the cyber-security literature, with a focus on cyber-security research in 'traditional' and 'critical' security studies and a focus on research more directly dealing with private security issues is identified. In conclusion, it is established that the biggest difference between cyber-security and other private security topics is that the state is not giving away power and authority to private actors in traditional security matters but that the state is increasingly enforcing its authority in cyberspace, which has been almost exclusively dominated and shaped by private actors.

(In)security in/through cyberspace: concepts

In the process of building confidence measures in cyberspace, it has been acknowledged that implementing effective national and supra-national cyber-security policies requires both common knowledge and a shared understanding of what constitutes cyber-security, cyber-threats, or cyber-crises, among many other ubiquitous, but ambiguous terms (OSCE 2013). However, while finding common ground through shared definitions is helpful at the very least, it is also very challenging given the diverse and dynamic contextual factors that influence the development of national cyber-security strategies (Maurer and Morgus 2014). In fact, struggles over common definitions are symptomatic of an issue that mobilizes different stakeholders from different sectors with divergent interests and are an expression of the struggle over influence at the same time.

In the literature, two meanings of cyber-security can be identified: a technical (narrow/precise) one and a national security (broad/vague) one. In the technical sphere, cyber-security usually signifies a set of measures to protect networks, computers, programmes and data from attack, damage or unauthorized access, in accordance with the common information security goals such as the protection of confidentiality, integrity and availability of information (see May *et al.* 2004). In the national security setting, cyber-security can simply be described as the security one enjoys in and from cyberspace (Cornish *et al.* 2009).

A comparison of nationally existing definitions of cyber-security reveals that most states mix technical and national security elements (see Maurer and Morgus 2014). Overall, there seems to be a consensus that cyber-security is closely interlinked with the security of cyberspace. However, defining cyberspace precisely is a challenge, because it is a constantly changing and evolving non/space/place, both in terms of technology and of how the technology is used and how that use is governed. In fact, there is a good argument to be made that no such thing as one unique, singular cyber-space exists (Bingham 1996: 32). Still, at its most basic, cyberspace connotes the fusion of communication networks, databases, and sources of information into a vast, tangled, and diverse blanket of electronic interchange. Thus, a 'network ecosystem' is created, a place that is not part of the normal, physical world. It is virtual and immaterial, a 'bioelectronic environment that is literally universal: It exists everywhere there are telephone wires, coaxial cables, fiber-optic lines or electromagnetic waves' (Dyson *et al.* 1994). Importantly, cyberspace is also grounded in physical reality. As one observer argues, 'the channelling of information flows … occurs within the framework of a "real" geography' (Suteanu 2005: 130) made up of servers, cables, computers, satellites, and so on. Therefore, cyberspace is comprised of both material and virtual elements; it is a 'space of things and ideas, structure and content' (Deibert and Rohozinski 2010: 16).

By implication, cyber-security is as a type of security that works in and through cyberspace/s, and the making and practice of cyber-security is constrained and enabled by this environment and its geography. By implication, the cyber-security discourse has never been static, because the technical aspects and their use of the information infrastructure are constantly evolving and keep influencing various aspects of the debate. This is not to say that its material conditions are outside and above political decisions and discursive processes. But a close look at the cyber-security discourse reveals how material conditions, or rather, possibilities and impossibilities of threat and countermeasures, have been key to determining the shape of the danger discourse (Deibert 1997; Deibert *et al.* 2008). In particular, specifying whose security and what security is at stake becomes a key (political) question.

Linking 'cyber' to critical infrastructures

In a computing context, the term security implies a technical concept ('information security'). Arguably, this has little in common with the type of security concepts security scholars are interested in (Hansen and Nissenbaum 2009: 1160; Buzan and Hansen 2009: 15; Buzan *et al.* 1998: 25). However, specific security connotations are created in this realm through the connection of the cyber-prefix to other security-relevant issues like terror, espionage, war, weapons, or deterrence. To make such a link possible, an insecurity argument needs to be made first. This is easy in the case of cyberspace, since it is fundamentally insecure.

As is well known, today's version of cyberspace emerged out of the Advanced Research Projects Agency Network (ARPANET), which was funded by the Defense Advanced Research Projects Agency (DARPA) of the United States Department of Defense (DoD) from 1962 onwards, mainly for optimized information exchange between the universities and research

laboratories involved in DoD research. When building the network, the designers emphasized robustness and survivability over security, simply because there was no apparent need for a focus on security at that time, given that information systems were being hosted on large proprietary machines that were connected to very few other computers. This turned into a legacy problem.

What makes systems so vulnerable today is the confluence of the following factors: the same basic packet-switching technology (not built with security in mind), the shift to smaller and far more open systems (not built with security in mind) and the rise of extensive networking at the same time (Libicki 2000), which resulted in a sprawling network with a very large numbers of insecure machines connected through insecure data distribution mechanisms. In addition, there are significant market-driven obstacles to IT-security, which came into play when the commercialization of the internet set in: There is no direct return on investment, time-to-market impedes extensive security measures, and security mechanisms often have a negative impact on usability so that security is often sacrificed for functionality (Anderson and Moore 2006).

Against this basic backdrop of technological insecurity, changes in the technical environment altered what was seen 'in need of protection' in the policy debate – the so-called referent object of security (Dunn Cavelty 2008). In the 1970s and 1980s, cyber-security (though not yet under that name) was mainly about those parts of the private sector that were becoming digitalized and also about government networks and the classified information residing in it. This relatively limited referent object was changed in crucial ways in the mid-1990s with the growth and spreading of computer networks into more and more aspects of life. In the early days (1970s and 1980s), mainly the hacking sub-culture, computer scientists, and later exponents of the anti-virus industry set the boundaries of the danger discourse (Dunn Cavelty 2013). In the mid-1990s, a diverse set of security professionals – mainly from law enforcement, the intelligence and the civil defence community as well as think tankers and military experts – built a more distinct national security connotation on top of this (Warner 2012).

In the contemporary political debate, some infrastructures are now regarded as 'critical' by the authorities because their prolonged unavailability could result in social instability and major crisis. The most frequently listed examples of critical infrastructures encompass banking and finance, government services, telecommunication and information and communication technologies, emergency and rescue services, energy and electricity, health services, transportation, logistics and distribution, and water supply (Abele-Wigert and Dunn 2006: 386–9). Today, these critical infrastructures mostly take the form of interconnected, complex, and increasingly virtual systems; in fact, the topic of cyber-security and critical infrastructure protection are often handled as one and the same. Because critical infrastructure systems combine symbolic and instrumental values, attacking them becomes integral to a modern logic of destruction that seeks maximum impact. In other words, cyberspace can become a force-multiplier by combining the risks to cyberspace with the possibility of risks through cyberspace (Deibert and Rohozinski 2010).

This combination has proven a key condition for promoting cyber-security to the forefront of current strategies for providing security. As a result, the link between national security and cyberspace has become an uncontested 'truth' with budgetary and political consequences. In this particular policy discourse, information technology is emerging as the common factor upon which all sectors of security converge, as most security issues and measures today have cyber (or computerized) components. The cyber-realm emerges as two things: it is an attack vector potentially threatening things of value for different actors (state, business, and individuals) and a dimension in which countermeasures against various sorts of threats – not only

cyber-related – can be situated. This way, cyber-security is not just about the 'security of cyber', but is also 'security through cyber' (Betz and Stevens 2011).

Cyber-security in security studies

This section situates and classifies literature at the intersection of cyber-security and national security. Since this Handbook is interested in private security issues, I start by discussing literature in security studies, using the well-established differentiation between positivists/rationalists (or traditional security studies, with a strong nod towards non-academic research) on the one side and post-positivist or 'critical/reflexive' approaches on the other (Buzan and Hansen 2009; CASE Collective 2007: 561–5). Since private security aspects are not all too well developed in both, a third type of research that mainly uses economic models and explanations is discussed in the next section.

In traditional security studies, the majority of books, articles, and reports on cyber-security (and closely related issues) remains policy-oriented, centred on the US and does communicate little with more general international relations theory and research to this day. In other words, most of the work is not strictly academic. The two main questions that are being tackled are who (or what) is the biggest danger for an increasingly networked nation/society/military/business environment, and how to best counter the new and evolving threat (Gombert and Libicki 2014; Farwell and Rohozinski 2011). The threat-form that has triggered the biggest body of literature is cyberwar (exemplary, for a vast literature, see Arquilla and Ronfeldt 1993; Rid 2013). This is not surprising, given the potentially devastating impact of a full-fledged cyber-aggression and the long tradition in international law and military ethics to address new forms of warfare and weapons systems under legal and ethical viewpoints (Barrett 2013).

Apart from literature with an implicit or explicit problem-solving or purely conceptual orientation, theoretically guided or empirically sound academic research is still quite rare. Recently, however, a few cyber-security related articles have been published in high-ranking political science journals like *International Security* (Gartzke 2013; Kello 2013) or *Journal of Peace Research* (Valeriano and Maness 2014), which could indicate the beginning of a more sustained focus on cyber-conflict issues in the traditional security domain (see also Axelrod and Iliev 2013; Eun and Abmann in press). However, given the orientation of these journals, more or less aggressive forms of cyber-war and/or questions of international cooperation will likely remain at the centre of attention.

The importance and prominence of these publications notwithstanding, the growing body of literature on war in and through cyberspace falls short of capturing the diversity of cyber-security issues. Specifically, it fails to capture malicious cyber-activities that are not destructive and war-like but fall under the far more obscure domain of cyber-exploitation (but see Inkster 2013 on intelligence and Grabosky 2013 on crime), arguably the biggest problem in the cyber-domain nowadays. The difference between cyber-attack and cyber-exploitation is that cyber-exploitations do not seek to disturb the normal functioning of a computer system or network from the user's point of view like attacks do – quite the opposite: the best cyber-exploitation is such that the user never notices (Owens *et al*. 2009: 80ff.). How such an elusive phenomenon can be researched is another question altogether.

While private security actors play an important role in all forms of cyber-aggression and countermeasures, this topic is a non-issue in the emerging literature. This is not overly surprising, given the relative newness of the whole field, which has started to tackle the broad and seemingly more important issues first rather than sub-issues. Notable exceptions are publications on the cyber-(military–)industrial complex (Talbot 2011; Brito and Watkins 2011),

which have included thoughts and data on the role of private business (mainly consultants) in the cyber-threat hype. Similarly, Bruce Schneier, a well-known cryptographer, has focused on power dynamics in cyber-security, including private actors (Schneier 2012, 2013). Furthermore, a few op-eds on the question of cyber-mercenaries or cyber-privateers exist (Ford 2010; Singer and Friedman 2014), which look at how private hacking groups are used for strategic purposes by states (i.e. Russia and China).

In critical security studies, three bodies of literature exist. The first focuses on 'postmodern war', a form technical-military interaction that centres on the centrality of information as the 'new metaphysics of power' (Dillon 2002; Hables Gray 2005). In general, this type of research has been interested in the larger shift in war fighting practices rather than specifics and/or focuses on aspects of information war more broadly. Practices of cyber-security are considered on the side, if at all. The second body of literature stems from the Munk School in Toronto, which has focused on issues like (electronic) surveillance and censorship for a considerable number of years and is concerned with the creation of more insecurity by (state) actors through cyber-means (Deibert 1997, 2013; Deibert and Rohozinski 2010). Private security actors and issues are not a particular focus in this literature. The third body of literature uses frameworks inspired by securitization theory (Buzan *et al*. 1998) and is mainly interested in how different actors in politics have tried to argue the link between the cyber-dimension and national security (Eriksson 2001; Dunn Cavelty 2008; Hansen and Nissenbaum 2009). In a similar vein, recent articles have focused on metaphors in the cyber-security discourse to explain political response (Barnard-Wills and Ashenden 2012; Stevens and Betz 2013; Dunn Cavelty 2013). Overall, the focus of this research is restricted in at least two ways. First, most of these studies focus on politically salient speech acts by 'visible' political figures that can be approved (or disproved) by general public. Such a focus reveals the constitutive effects the discursive practices of 'capable actors' have in (world) politics, but it is not sensitive towards how these discursive practices are facilitated or thwarted by preceding and preparatory linguistic and non-linguistic practices of actors that are not as easily visible, also outside of governments (Huysmans 2011: 371). Second, due to the focus on linguistic practices, this literature tends to ignore the technical and material factors important in cyber-security. Therefore, private security issues have sometimes been mentioned but they have not been at the centre of attention.

Cyber-security and economics

In both types of security studies, aspects of private security issues are dealt with on the margins, if at all. What about other types of literature? While it is impossible to speak about all cyber-security research with authority, there is research in other disciplines that focuses much more directly on private security actors and mechanisms. In this section, I briefly discuss two bodies of research with more or less direct bearing on the topic: research on the economics of information security and research on public-private partnerships, influenced by network governance literature.

Economics of information security research is mainly the brainchild of Ross Anderson, a security engineer and cryptographer at Cambridge University, who joined forces with Hal Varian, an economics professor (Anderson 2012). More recently, psychological research was brought in (i.e. Schneier 2008; Moore and Anderson 2011). The gist of this multifaceted research is that security failures are often due to perverse incentives or psychological factors such as heuristics and biases, but also emotions and culture rather than to the lack of suitable technical protection mechanisms. In his classic paper on the subject, Anderson (2001) shows how economic analysis explains many phenomena that security researchers had previously

found perplexing, for example why mass-market software products contain so many security bugs, why their security mechanisms are so difficult to manage, why so many specialist security products are second rate, with bad ones driving good ones out of the market, and also, why government agencies concerned with information warfare concentrate on offence rather than defence.

In particular, Anderson and colleagues show convincingly that the reason for the continued existence and constant new creation of vulnerabilities in our information infrastructure is that security is constantly 'under-produced' in a market dominated by the so-called network effect, under which the benefits of a product increase when the number of users increases, and the 'winner takes it all', since large costs to users from switching technologies leads to lock-in quasi-monopolies and time pressures lead to a focus on fast delivery in commercial software development. Quality criteria, like security, therefore play only a minor role (Anderson and Moore 2006). In terms of strategic action, he explains the current insecurity conundrum through asymmetric information:

> Suppose that you head up a US agency with an economic intelligence mission, and a computer scientist working for you has just discovered a beautiful new exploit on Windows 2000. If you report this to Microsoft, you will protect 250 million Americans; if you keep quiet, you will be able to conduct operations against 400 million Europeans and 100 million Japanese.
>
> *(Anderson 2001: 5)*

In other words, intelligence services of this world are making cyberspace more insecure directly; in order to be able to have more access to data, and in order to prepare for future conflict (Greenwald and MacAskill 2013; Dunn Cavelty 2014). Since cyber-security is always also about technical insecurities, research that focuses on technical aspects of security can have considerable explanatory powers also for forms of national security.

Overall similar, but focused on a broader governance issue, is research on public private partnerships. As mentioned in the introduction, one of the key challenges for any cyber-security efforts from the view of the state arises from the privatization and deregulation of many parts of the public sector since the 1980s and the globalization processes of the 1990s, which have put almost all critical (information) infrastructure in the hands of private enterprise. This creates a situation in which market forces alone are not sufficient to provide security in critical sectors (also due to the perverse incentives described by Anderson *et al.*). At the same time, the state is incapable of providing the public good of security on its own, since an overly intrusive market intervention is considered a flawed and undesirable option, especially since the same infrastructures that the state aims to protect are also the foundation of the competitiveness and prosperity of a nation. Therefore, any policy trying to get more security in cyberspace must absorb the negative outcomes of liberalization, privatization, and globalization, without cancelling out the positive effects.

Public–private partnerships (PPP), a form of cooperation between the state and the private sector, are widely seen as a panacea for the problem of cyber-(in-)security. In specific, most existing PPPs serve the function of information-sharing. There are four different levels of information-sharing: information shared within the government, between different governments, between different companies, and between the government and the private sector (Prieto 2006; Dunn Cavelty and Suter 2009; Gal-Or and Ghose 2005). However, public-private information-sharing has proven to be difficult to establish: Companies are reluctant to share information on their vulnerabilities and security breaches, since public dissemination could

result in new attempts by hackers to exploit the vulnerabilities, and above all, in a loss of reputation. Economic analyses have shown that the public announcement of security breaches is negatively correlated with the market value of the targeted firm (Campbell *et al.* 2003; Cavusoglu *et al.* 2004). Additionally, sharing information on incidents is risky, because public dissemination of secret information could also violate laws in the context of the protection of privacy (Branscomb and Michel-Kerjan 2006). For the government, releasing information on malicious actors is no less sensitive, as it is possible that the release of such material can seriously compromise intelligence activities and investigations (Moteff and Stevens 2003). Therefore, how incentives structures and costs can be adjusted to create more favourable conditions is the main focus of literature on public-private partnerships. This includes defining win-win situations for both public and private actors (Personick and Patterson 2003), how trust can be established and maintained (Branscomb and Michel-Kerjan 2006; Cukier *et al.* 2005; Aviram 2006), or the questions which conditions are conducive to an optimal involvement of the state in networks of cooperation (Suter 2007, 2012).

Conclusion

Cyber-security research is steadily growing, but in international relations and security studies, it is not a mature field yet. Apart from a few exceptions, research remains fragmented, is biased towards just one expression (cyber-war), and struggles to tap into existing funding resources. Given this relative weakness, many important issues remain under-researched. The importance of 'the private' in the establishment of the topic as national security issue is one of those issues. Following Leander (2010), research on this topic could be developed in three areas:

- discovering/denouncing/documenting private security;
- explaining and understanding private security; and
- debating the consequences of private security.

However, and importantly: cyber-security has always been a field of practice much defined by non-state (private) actors, as should have become obvious in this chapter. In contrast to many other security issues, private actors are not the ones that are increasingly pushing into in traditional (state) security fields in cyber-security – it is the state that is trying to (re)establish its authority in a space cultivated by innovative practices of companies and consumers on the one hand and criminal actors on the other. For research falling into the category of private security research, this is a challenge, because many of the assumptions about authority and necessary governance structures need to be questioned.

Bibliography

Abele-Wigert, I. and Dunn, M. (2006) *The International CIIP Handbook 2006: An Inventory of Protection Policies in 20 Countries and 6 International Organizations*, vol. I. Zurich: Center for Security Studies.

Anderson, R. (2001) 'Why Information Security is Hard – An Economic Perspective', in IEEE Computer Society (ed.), *Proceedings of the 17th Annual Computer Security Applications Conference*, Washington, DC: IEEE Computer Society, pp. 358–65.

Anderson, R. (2012) 'Security Economics: A Personal Perspective', paper presented at the Annual Computer Security Applications Conference (ACSAC) 2012, www.acsac.org/2012/openconf/modules/request.php?module=oc_program&action=view.php&a=&id=252&type=4.

Anderson, R. and Moore, T. (2006) 'The Economics of Information Security', *Science* 314(5799): 610–13.

Arquilla, J. and Ronfeldt, D. (1993) 'Cyberwar is Coming!', *Comparative Strategy* 12(2): 141–65.
Aviram, A. (2006) 'Network Responses to Network Threats: The Evolution into Private Cyber-Security Associations', in M. F. Grady and F. Parisi (eds), *The Law and Economics of Cybersecurity*, Cambridge: Cambridge University Press, pp. 143–92.
Axelrod, R. and Iliev, R. (2013) 'Timing of Cyber-Conflict', *Proceedings of the National Academy of Sciences* 111(4): 1298–1303.
Barnard-Wills, D. and Ashenden, D. (2012) 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk', *Space and Culture* 15(2): 110–23.
Barrett, E. T. (2013) 'Warfare in a New Domain: The Ethics of Military Cyber-Operations', *Journal of Military Ethics* 12(1): 4–17.
Betz, D. and Stevens, T. (2011) *Cyberspace and the State: Toward a Strategy for Cyber-Power*, London: The International Institute for Strategic Studies.
Bingham, N. (1996) 'Object-ions: From Technological Determinism towards Geographies of Relations', *Environment and Planning D: Society and Space* 14(6): 635–57.
Branscomb, L. M and Michel-Kerjan, E. O. (2006) 'Public–Private Collaboration on a National and International Scale', in P. E. Auerswald, L. M. Branscomb, T. M. La Porte and E. O. Michel-Kerjan (eds), *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, Cambridge: Cambridge University Press, pp. 395–403.
Brito, J. and Watkins, T. (2011) *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, working paper no. 11-24, April, Arlington, VA: Mercatus Center, George Mason University.
Buzan, B. and Hansen, L. (2009) *The Evolution of International Security Studies*, Cambridge: Cambridge University Press.
Buzan, B., Wæver, O. and de Wilde, J. (1998) *Security: A New Framework for Analysis*, Boulder, CO: Lynne Rienner.
Campbell, K., Gordon, A. L., Loeb, M. P. and Zhou, L. (2003) 'The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market', *Journal of Computer Security* 11: 431–48.
CASE Collective (2007) 'Europe, Knowledge, Politics Engaging with the Limits: The CASE Collective Responds', *Security Dialogue* 38(4): 559–76.
Cavusoglu, H., Birendra, M. and Raghunathan, S. (2004) 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers', *International Journal of Electronic Commerce* 9: 69–104.
Cornish, P., Hughes, R. and Livingstone, D. (2009) *Cyberspace and the National Security of the United Kingdom. Threats and Responses*, London: Chatham House.
Cukier, K. N, Mayer-Schoenberger, V. and Branscomb, L. M. (2005). *Ensuring (and Insuring?) Critical Information Infrastructure Protection*, faculty research working paper RWP05-055, Cambridge, MA: John F. Kennedy School of Government.
Deibert, R. J. (1997) *Parchment, Printing, and Hypermedia: Communication in World Order Transformation*, New York: Columbia University Press.
Deibert, R. J. (2013) *Black Code: Inside the Battle for Cyberspace*, Toronto: McClelland & Stewart
Deibert, R. J. and Rohozinski, R. (2010) 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology* 4(1): 15–32.
Deibert, R. J., Palfrey, J.G., Rohozinski, R. and Zittrain, J. (2008) *The Practice and Policy of Global Internet Filtering*, Cambridge, MA: MIT Press
Dillon, M. (2002) 'Network Society, Network-Centric Warfare and the State of Emergency', *Theory, Culture, and Society* 19(4): 71–9.
Dunn Cavelty, M. (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Abingdon: Routledge.
Dunn Cavelty, M. (2013) 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', *International Studies Review* 15(1): 105–22.
Dunn Cavelty, M. (2014) 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities', *Science and Engineering Ethics* 20(3): 701–15.
Dunn Cavelty, M. and Suter, M. (2009) 'Public-Private Partnerships Are No Silver Bullet: an Expanded Governance Model for Critical Infrastructure Protection', *International Journal of Critical Infrastructure Protection* 2(4): 179–87.
Dyson, E., Gilder, G., Keyworth, G. and Toffler, A. (1996) 'Cyberspace and the American Dream: A Magna Carta for the Knowledge Age', *The Information Society* 12(3): 295–308.

Eriksson, J. (2001) 'Cyberplagues, IT, and Security: Threat Politics in the Information Age', *Journal of Contingencies and Crisis Management* 9(4): 200–10.

Eun, Y.-S. and Abmann, J. S. (in press) 'Cyberwar: Taking Stock of Security and Warfare in the Digital Age', *International Studies Perspectives* doi:10.1111/insp.12073.

Farwell, J. P. and Rohozinski, R. (2011) 'Stuxnet and the Future of Cyber War', *Survival* 53(1): 23–40.

Ford, C. (2010) 'Here Come the Cyber-Privateers?', New Paradigms Forum, www.newparadigmsforum.com/NPFtestsite/?p=277.

Gal-Or, E. and Ghose, A. (2005) 'The Economic Incentives for Sharing Security Information', *Information Systems Research* 16(2): 186–208.

Gartzke, E. (2013) 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security* 38(2): 41–73.

Gombert, D. and Libicki, M. (2014) 'Cyber Warfare and Sino-American Crisis Instability', *Survival: Global Politics and Strategy* 56(4): 7–22.

Grabosky, P. (2013) 'Organized Crime and the Internet', *RUSI Journal* 158(5): 18–25.

Greenwald, G. and MacAskill, E. (2013) 'Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks', *The Guardian* 7 June, www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

Hables Gray, C. (2005) *Peace, War, and Computers*, Abingdon: Routledge.

Hansen, L. and Nissenbaum, H. (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly* 53(4): 1155–75.

Huysmans, J. (2011) 'What's in an Act? On Security Speech Acts and Little Security Nothings', *Security Dialogue* 42(4–5): 371–83.

Inkster, N. (2013) 'Chinese Intelligence in the Cyber Age', *Survival: Global Politics and Strategy* 55(1): 45–66.

Kello, L. (2013) 'The Meaning of the Cyber Revolution', *International Security* 38(2): 7–40.

Leander, A. (2010) 'The Privatization of International Security', in M. Dunn Cavelty and V. Mauer (eds), *The Routledge Handbook of Security Studies*, Abingdon: Routledge, pp. 200–10.

Libicki, M. C. (2000) *The Future of Information Security*, Washington, DC: Institute for National Strategic Studies.

Maurer, T. and Morgus, R. (2014) *Compilation of Existing Cybersecurity and Information Security Related Definitions*, October, Washington, DC: New America Foundation, www.newamerica.org/downloads/OTI_Compilation_of_Existing_Cybersecurity_and_Information_Security_Related_Definitions.pdf.

May, C. *et al*. (2004) *Advanced Information Assurance Handbook*, CMU/SEI-2004-HB-001, Pittsburgh, PA: CERT/CC Training and Education Center, Carnegie Mellon University.

Moore, T. and Anderson, R. (2011) *Economics and Internet Security: A Survey of Recent Analytical, Empirical and Behavioral Research*, Cambridge, MA: Computer Science Group, Harvard University, ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf.

Moteff, J. D. and Stevens, D. D. (2003) *Critical Infrastructure Information Disclosure and Homeland Security*, report for Congress, RL31547, 29 January, Washington, DC: Congressional Research Service.

OSCE (2013) 'Permanent Council Decision No. 1106', OSCE Plenary, 3 December, www.osce.org/pc/109168.

Owens, W. A., Dam, K. W. and Lin, H. (eds) (2009) *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*, Washington, DC: National Academy Press.

Personick, S. D. and Patterson, C. A. (2003) *Critical Information Infrastructure Protection and the Law: An Overview of Key Issues*, Washington, DC: National Academy Press.

Prieto, D. B. (2006) 'Information Sharing with the Private Sector: History, Challenges, Innovation, and Prospects', in P. E. Auerswald, L. M. Branscomb, T. M. La Porte and E. O. Michel-Kerjan (eds), *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, Cambridge: Cambridge University Press, pp. 404–28.

Rid, T. (2013) *Cyber War Will Not Take Place*, London: Hurst & Company.

Schneier, B. (2008) 'The Psychology of Security (Part 1 and 2)', www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html.

Schneier, B. (2012) 'When It Comes to Security, We're Back to Feudalism', *Wired*, www.wired.com/opinion/2012/11/feudal-security.

Schneier, B. (2013) 'The Battle for Power on the Internet', *The Atlantic*, www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824.

Singer, P. W. and Friedman A. (2014) *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford: Oxford University Press.

Stevens T. and Betz, D. J. (2013) 'Analogical Reasoning and Cyber Security', *Security Dialogue* 44(2): 147–64.

Suteanu, C. (2005) 'Complexity, Science and the Public: The Geography of a New Interpretation', *Theory, Culture and Society* 22(5): 113–40.

Suter, M. (2007) 'Improving Information Security in Companies: How to Meet the Need for Threat Information', in M. Dunn, V. Mauer and F. Krishna-Hensel (eds), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, Aldershot: Ashgate, pp. 129–50.

Suter, M. (2012) 'The Governance of Cyber Security: An Analysis of Public–Private Partnerships in a New Field of Security Policy', dissertation, ETH Zurich, Switzerland.

Talbot, D. (2011) 'The Cyber Security Industrial Complex', MIT Technology Review, www.technologyreview.com/news/426285/the-cyber-security-industrial-complex.

Valeriano, B. and Maness, R. C. (2014) 'The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11', *Journal of Peace Research* 51(3): 347–60.

Warner, M. (2012) 'Cybersecurity: A Pre-History', *Intelligence and National Security* 27(5): 781–99.