The Routledge Handbook of Security Studies

Edited by
Myriam Dunn Cavelty and Victor Mauer

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

16

Cyber-threats

Myriam Dunn Cavelty

Over the past decade, many public figures have portrayed attacks by means of computers – so called cyber-threats – as one of the gravest threats to national security today (cf. Poulsen 1999; Porteus 2001). What is remarkable about this threat representation is that while viruses, worms or cyber-crime are an undisputed and everyday reality, major disruptive cyber-attacks with grave impact, which would substantiate such reasoning, have remained mere chimeras. This raises at least two questions: first, why this threat representation has gained so much salience and continues to occupy such a prominent position among 'new threats' (as many of the post-Cold War threats are called); and second, to what extent the continued treatment of cyber-threats as a national security issue of highest priority is justified.

From a constructivist viewpoint, national security has always been about the social construction of specific issues as a threat, and about the definition of desirable responses to these issues. In the case of new threats, security professionals face an even greater need to establish a credible link to national security, because the national security dimension is less explicit when the environment, the society or the economy are concerned (Buzan et al. 1998). The necessity to make a convincing case for (national) security is even more pronounced as new threats are often framed as 'risks' (Daase et al. 2002; Rasmussen 2001): risks are indirect, unintended, uncertain and are, by definition, situated in the future, since they only materialize in reality when they are instantiated. Therefore, risks exist in a permanent state of virtuality and are only actualized through anticipation (van Loon 2002: 2). In the case of many new threats, threat images are thus characterized by reference to potential catastrophic occurrences in the future; and anticipation of these future disasters, rather than past experiences or solid justification for the current level of threat, is the main reason for action in the present.

Once this key characteristic has been recognized, the analysis of *threat representations* seems to become inevitable for understanding the politics surrounding new threats. This chapter therefore shows in a first section how the case for security is argued in three instances of cyber-threats – cyber-crime, cyber-terrorism and cyber-war – in particular, how the depiction of the threat is based on building 'threat clusters', in which traditional security issues are discursively interlinked with less typical ones, and which partly explain why these threat representations are so prominent. This chapter then looks at how justified these threat representations are, noting a high tendency for exaggeration due to the uncertainty surrounding the exact level of threat. It also addresses how a feasible 'security threshold' could be established, the need for which is well exemplified in the following quote: 'Setting the security trigger too low on the scale risks paranoia … setting it too high risks failure to prepare for major assaults until too late' (Buzan 1991: 115). In the third section, a glimpse into the future is provided: what can be said about the future potential for cyber-doom? The chapter ends by pointing out likely trends and action that should be taken by the international community to ensure that cyber-doom will never become a reality.

Types of cyber-threat representations

The cyber-threats debate originated in the US in the late 1980s, gained great momentum in the mid-1990s, and spread to other countries in the late 1990s. Both the threat perception and the envisaged countermeasures were shaped by the US over the years, with only little variation in other countries (Brunner and Suter 2008). On the one hand, the debate was decisively influenced by the larger post-Cold War strategic context, in which the notion of asymmetric vulnerabilities, epitomized by the multiplication of malicious actors (both state and non-state) and their increasing capabilities to do harm started to play a key role. On the other hand, discussions about cyber-threats always were and still are influenced by the ongoing information revolution, which is about the dynamical evolution and propagation of information and communication technologies into all aspects of life (Dunn and Brunner 2007). The US is also shaping the information revolution both technologically and intellectually, particularly by discussing its implications for International Relations and security (cf. Alberts and Papp 1997; Arquilla and Ronfeldt 1997; Henry and Peartree 1998) and acting on these assumptions. Against this backdrop, this chapter shows how cyber-threat clusters were formed over the years, looking in particular at cyber-crime, cyber-terrorism and cyber-war – all three of which coexist side by side today – and problematizes these characterizations.

Cyber-crime and the foreign intelligence threat

As the 1970s gave way to the 1980s, the merger of telecommunications with computers theoretically enabled everybody with a PC and a modem at home to exploit these emerging networks. Consequently, the amount of attention given to computer and communications security issues by political actors grew incrementally in response to well-publicized events such as politically motivated attacks, computer viruses and penetrations of networked computer systems for criminal purposes (cf. Bequai 1986; Parker 1983).

The distinct national-security dimension was established when computer intrusions were clustered together with the more traditional and well-established espionage discourse. More prominent hacking incidents – such as the numerous intrusions into government or other high-level computers perpetrated by the Milwaukee-based (mostly underage) '414s' (Covert 1983; Ross 1990) – led to a feeling in policy circles that there was a need for action: if teenagers were able to penetrate computer networks that easily, it was highly likely that better organized entities such as states would be even better equipped to do so. Other events, like the Cuckoo's Egg incident – an international KGB effort to connect to computers in the US and copy information from them that was only discovered by chance (Stoll 1989) – indeed made apparent that the threat was not just one of criminals or juveniles playing games, but that classified or sensitive information could be acquired relatively easily by foreign nationals through hackers employed by foreign states.

However, at the time, cyber-threats did not receive much attention from the wider public, nor were they seen as a problem for society at large, as the threat pertained mainly to government networks and to the classified information residing in them. The technological substructure lacked the quality of a mass phenomenon that it would acquire once computer networks turned into a pivotal element of modern society – and which would also move the threat further into the limelight and to the forefront of the security discourse. Nonetheless, cyber-crime remains a driving factor in the discourse at large, as it is the threat representation with the closest link to reality.

Critical infrastructures and cyber-terrorism become an issue

In the mid-1990s, the issue of cyber-threats was truly catapulted onto the security political agendas of many countries when it was established by the strategic community that key sectors of modern society, including those vital to national security and to the essential functioning of industrialized economies, rely on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation (PCCIP 1997). In this way, cyber-threats became to be seen as a threat to society's core values, and to the economic and social well-being of entire nations.

It was further established that because of the technological substructure, harmful attacks could be carried out in innumerable ways, potentially by anyone with a computer connected to the internet, and for purposes ranging from juvenile hacking to organized crime to political activism to strategic warfare. The new enemy was neither clearly identifiable nor associable to a particular state. Hacking tools could easily be downloaded and constantly became both more sophisticated and user-friendly. This diffuse threat-frame and the link to the fundament of society (critical infrastructures) opened the door for turning every small incident into a potential security issue of high urgency.

In particular, the image of cyber-terrorism emerged. Though a link between the cyber-domain and terrorism has been a theme in the US national security literature since the late 1980s (cf. National Academy of Sciences 1991), this cluster became far more convincing once critical infrastructures, the soft underbelly of liberal societies, were added. This threat cluster was pushed by US security officials who no longer only expressed concern about the security of classified data, but also about the possibility that terrorists might use cyber-attacks to counter the US's overwhelming military superiority, thus effectively mixing the asymmetry debate with the debate on vulnerability due to technological dependency. In this threat representation, the fear of random and violent victimization in the case of terrorism and the distrust or outright fear of computer technology, which both capitalize on the fear of the unknown, are combined (Pollitt 1997). The big problem with the use of the term 'cyber-terrorism' in this discourse is that the term has become totally bereft of meaning by its frequent evocation in the media for attacks of any kind with the help of computers, which is exacerbated by similar use of the term by government officials.

Cyber-war

The threat representation of cyber-war is strongly influenced by the increasing technological sophistication of the US military and evolved in parallel with the one of cyber-terrorism. The Second Gulf War of 1990–91, in some circles called the first information war, was followed by a plethora of publications on the strategic use of information and information technology in conflicts (cf. Mahnken 1995; Molander et al. 1996; Campen *et al.* 1996). In its aftermath, the concept of cyber-war was coined (Arquilla and Ronfeldt 1997b) and various aspects of a military doctrine on the use of information in conflicts were developed, which acknowledged that one was striving to gain the 'information edge' (Nye and Owens 1996), while at the same time being disproportionately vulnerable due to high dependence on information technologies. Within the vast family of information warfare concepts, computer network attacks – 'actions taken through the use of computer networks to disrupt, deny, degrade, or destroy infomation resident in computers and computer networks, or the computers and networks themselves' (DoD Dictionary 2008) – are often equated with the initial idea of cyber-war.

This doctrinal development was driven by incidents in times of heightened tension or conflict, but it was also influenced by a global online community that started to acquire a voice of its own in times of conflict. NATO's 1999 intervention against Yugoslavia marked the first sustained use of the full-spectrum of information warfare components in combat. Much of this involved the use of propaganda and disinformation via the media (an important aspect of information warfare), but there were also extensive distributed denial-of-service (DDoS) attacks on various websites, as well as rumours that Yugoslav leader Slobodan Milosevic's bank accounts had been hacked by the US armed forces (Dunn 2002: 151). In addition, the increasing use of the internet during the conflict also gave it the distinction of being the 'first war fought in cyberspace' or the 'first war on the internet'.

However, the term 'cyber-war' is similarly plagued by vagueness as the term 'cyber-terror'. The popular usage of the word has come to refer to basically any phenomenon involving a deliberate disruptive or destructive use of computers (and is thus used interchangeably with 'cyber-terrorism'). For example, the cyber-confrontations between Chinese and US hackers in 2001 have been labelled the 'first Cyber World War'. The cause was a US reconnaissance and surveillance plane that was forced to land on Chinese territory after a collision with a Chinese jet fighter. Soon after, large-scale defacements of Chinese and US websites and waves of DDoS attacks began. Individuals from a variety of other nations joined in (Delio 2001) and the event was taken rather seriously by a variety of government officials on both sides – even though the actual effects of the cyber-attacks remained minimal. Recently, the issue of cyber-war gained renewed prominence when a three-week cyber-battle ensued and a wave of DDoS-attacks swamped and disabled various Estonian websites after the Estonian authorities removed a memorial to the Soviet forces of the Second World War. The attacks were readily attributed to the Russian government, and various officials claimed that this was the first known case of one state targeting another using cyber-warfare (Traynor 2007). Similar claims were made in the confrontation between Russia and Georgia of 2008. In all of these cases, it is still doubtful whether there was any direct government involvement and whether the term 'war' should really be invoked.

In search of a security threshold

It can be observed that in these threat representations, the security community – aided by the media – uses threat rhetoric evoking the image of imminent cyber-doom, even though nothing that happened ever came close to having a true and sustained society-threatening impact (the same is true for incidents that show the potential for grave society-wide impact – for example, a virus or worm affecting some critical services, or occasional intrusions into computers that contain classified and potentially harmful data). There always is a great reliance on hypotheses of what might happen and official reports and statements are full of 'could', 'would' and 'maybe' when describing the threat (Bendrath 2003). Even in political hearings, evidence is often anecdotal, and the uncertainty about the identity, actual capabilities and intentions of potential enemies appears very high (Dunn Cavelty 2008).

What remains is the *potential* for grave harm. It has become the norm today that every political tension or conflict is accompanied by heightened activity in cyberspace, and it is the norm that our societies are confronted daily with cyber-crime and all kinds of more or less disruptive cyber-incidents that cause minor and occasionally major inconvenience for private users, businesses and governmental organizations. The crucial question that needs to be asked is: when should these occurrences be treated as a matter of national security?

The danger of overly dramatizing the threat manifests itself in reactions that call for military retaliation (as happened in the Estonian case and in other instances) or other exceptional measures. This kind of threat rhetoric invokes enemy images even if there is no identifiable enemy, favours national solutions instead of international ones and centres on national-security measures instead of economic and business solutions. This is not to say that cyber-threats should under no circumstances be regarded as dangerous. But there needs to be clarity about which tools or measures are appropriate under which circumstances. This, so this chapter argues, can only be achieved with more knowledge about the actor and the intention behind an attack and the impact of the incident. Clearly, the terms as they are used in the discourse cannot serve as an analytical tool – they need to be clarified and sharpened to become useful for meaningful investigation of the issue of cyber-threats.

As previously noted, the spectrum of perpetrators that can engage in harmful cyber-activities ranges from teenagers to criminals to terrorist to nation-states. One useful way to approach the question of when something should be treated as a national security issue is to partition this wide range of actors into two groups: the first is called an 'unstructured' threat, while the latter is a 'structured' threat (National Academy of Sciences 1991; Minihan 1998). The unstructured threat consists of adversaries with limited funds and organization and short-term goals. The unstructured threat is not considered a danger to national security and is normally not of concern to the national security community. The structured threat, however, is considerably more methodical and better supported. Adversaries from this group have all-source intelligence support, extensive funding, organized professional support and long-term goals.

Another pragmatic and useful way to differentiate is to focus on the intention and the effect of the activities: Dorothy Denning, a US information security researcher, makes a distinction between three classes of politically motivated activity involving the internet – activism, hacktivism and cyber-terrorism (Denning 2001). Only the last of these is a structured effort and a case for national security. In her classification, (cyber-) activism is the normal, non-disruptive use of the internet in support of a (political) agenda or cause. Hacktivism is the marriage of hacking and activism, including operations that use hacking techniques against a target's internet site with the intention of disrupting normal operations. Cyber-terrorism, according to Denning, consists of unlawful attacks against computers, networks and the information stored therein, to intimidate or coerce a government or its people in furtherance of political or social objectives. Such an attack should result in violence against persons or property, or at least cause enough harm to generate the requisite fear level to be considered cyber-terrorism (cf. Conway 2008; Pollitt 1997; Devost *et al.* 1997).

In a similar vein, Bruce Schneier, a renowned security technologist and author, differentiates between cyber-vandalism, which includes the defacing of websites; cyber-crime, which includes theft of intellectual property and extortion based on the threat of DDoS attacks; cyber-terrorism, which refers to the hacking into a computer system to cause havoc by causing a nuclear power plant to melt down, floodgates to open, or two airplanes to collide; and cyber-war, which refers to the use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems (Schneier 2007). The first two represent an unstructured threat, while the second group would be considered a structured threat. The narrower and more precise the terms are defined and used, the better the phenomenon can be grasped. A narrow and precise definition also helps to circumvent other dangers inherent in the terms 'war' or 'terrorism', like exculpating the victims of an attack from their own responsibility for the consequences of their negligence in terms of computer security, or creating pressure to forcefully retaliate against 'hackers', real or imagined (Libicki 1997: 38).

Both Denning's and Schneier's classifications construct a cyber-threat escalation ladder: from rung to rung, the potential effects are increasingly serious. The advantage of such a 'severity of effects' view is that it helps policymakers to prioritize. Only computer attacks whose effects are sufficiently destructive or disruptive should be regarded as a national security issue. Attacks that disrupt non-essential services, or that are mainly a costly nuisance, should not. At the same time, not every successful internet attack, no matter how deadly, is necessarily an act of cyber-war. The tools and tactics used by armies, terrorists and criminals in cyberspace are the same, but the ultimate goals of these groups are different. Schneier captures the distinction well when he writes that

> just as every shooting is not necessarily an act of war, every successful Internet attack, no matter how deadly, is not necessarily an act of cyberwar. A cyberattack that shuts down the power grid might be part of a cyberwar campaign, but it also might be an act of cyberterrorism, cybercrime, or even – if it's done by some fourteen-year-old who doesn't really understand what he's doing – cybervandalism. Which it is will depend on the motivations of the attacker and the circumstances surrounding the attack … just as in the real world.
>
> (Schneier 2007)

Therefore, the only way to determine the source, nature and scope of an incident is to investigate. The authority to investigate and to obtain the necessary court orders or subpoenas clearly resides with law enforcement. Other actors, namely the military, should be involved only when there is sufficient proof that an attack was targeted directly and deliberately at national security assets by another state, when its effects are widespread and not localized, or when special technical expertise is required that others do not have.

The future likelihood of cyber-doom

It was argued above that cyber-attacks resulting in deaths and injuries have remained fiction. But what about the future? Schneier states unequivocally that 'there should be no doubt that the smarter and better-funded militaries of the world are planning for cyber-war, both attack and defense' (Schneier 2007). There are various indications that this is indeed the case. The US, for example, is reportedly developing national-level guidance for determining when and how to launch cyber-attacks against enemy computer networks (Bradley 2003). More recent reports discuss the founding of the US Air Force Cyber Command, which is tasked with both offensive and defensive cyber-activities (Kenyon 2007). US strategy experts assert that strategic rivals such as China and Russia have offensive information warfare programmes and are ready to use them (Thomas 2004; Mulvenon and Yang 1998; FitzGerald 1994).

It seems clear that until cyber-war is proven to be ineffective, states and non-state actors who have the ability to develop such 'weapons' will most likely try to do so, because they appear cost-effective, more stealthy and less risky than other forms of armed conflict. However, the mere existence of these capabilities does not necessarily mean that they will be used – or can be used. First of all, it is unclear whether such options are technologically feasible at all: many of the more tech-savvy political advisors and journalists have written about the practical difficulties of a serious cyber-attack or the inability of bureaucracies like militaries or intelligence agencies as well as many terrorist groups to really acquire the skills needed to become successful hackers (Ingles-le Nobel 1999; Green 2002; Shea 2003). Others observe that, for any capability beyond annoying hacks, the barriers to entry are quite high (CSTIW 1999). Some experts would even say that cyber-terrorism remains a far-fetched prospect because technology is simply not essential to many of the objectives of terrorist groups and therefore does not generate enough interest to be employed as a weapon of choice (Barak 2004: 95). In addition, even though it is often claimed that hacking tools are simple to use, inexpensive and widely available on computer bulletin boards and various websites, sophisticated cyber-weapons would need to be a lot more powerful than that to be effective and to deliver 'effect' to a particular geographic conflict zone or enemy. We would need to see a qualitative leap in the ability to penetrate and manipulate ICT, but also to control aspects of the information infrastructure directly (Eriksson and Giacomello 2007).

But even if the technology existed and could be targeted specifically at enemy infrastructures, its use raises legal, ethical, but also strategic issues, especially as far as its use by state actors is concerned. Cyber-war experts Arquilla and Libicki believe that the Pentagon actually did hack into Serbian computers to spy during the Kosovo conflict, but refrained from causing chaos principally for strategic reasons: widespread use of these new weapons and tools would probably have accelerated and focused foreign military research on them and threaten to deprive the US of its information warfare edge in a field where foes could catch up quickly and cheaply (Borger 1999).

Furthermore, nobody can be truly interested in allowing the unfettered proliferation and use of cyber-war tools, not even (or maybe least of all) the country with the offensive lead in this domain. Quite the contrary, very strong arguments can be made that the world's big powers have an overall strategic interest in developing and accepting internationally agreed norms on the use and non-use of cyber-war, i.e. computer network attacks, and in creating agreements that might pertain to the development, distribution and deployment of cyber-weapons or to their use (Denning 2001). The most obvious reason is that the countries that are currently openly discussing the use of cyber-war tools are precisely the ones that are the most vulnerable to cyber-warfare attacks due to their high dependency on infomation infrastructure. A similar argument can be made for terrorists: most terrorist organizations depend on the information infrastructure for conducting their 'daily business'.

In addition, the features of the emerging information environment make it extremely unlikely that any but the most limited and tactically oriented instances of computer attacks could be contained. More likely, computer attacks by the military could 'blow back' through the interdependencies that characterize the environment. Even relatively harmless viruses and worms would cause considerable random disruption to businesses, governments and consumers. Awareness that global information networks are routinely exploited by military actors would probably severely undermine the ongoing efforts to foster a reliable information society (Rathmell 2001), a key goal of many Western states. This loss would most likely weigh much heavier in the end than the uncertain benefits to be gained from cyber-war activities.

Conclusion

One of the main reasons why the issue of cyber-threats has gained so much attention in recent years is the fact that in the process of threat politics, US officials have convincingly argued that they threaten the very fabric of modern societies. It must be noted, however, that the defining characteristic of cyber-threats is their unsubstantiated nature: none of the worst-case scenarios have materialized, not even in part. The last few years suggest, instead, that computer network vulnerabilities are an increasingly serious business problem, but that their threat to national security has, in general, been overstated. At the heart of the issue lies the fact that we are dealing with a threat whose dimensions remain altogether uncertain – opening up a broad margin for political bargaining.

Does that mean that the cyber-dimension does not present a danger for national security at all? An answer in the affirmative would require knowledge of the future. But in light of the fact that the threat is frequently overstated and that this might result in detrimental countermeasures, a well-tempered approach as well as a careful estimation of a changing threat picture is in order. While it can be rightly argued that the future is unclear and the threat cannot be completely shrugged off, decision-makers and experts must be particularly careful not to foment unnecessary 'cyber-angst'. To forestall this, the level of threat should not be assessed by members of the strategic community alone, but by technical experts and infrastructure owners who have inside knowledge about exactly how vulnerable their assets are to a cyber-attack.

Probably the biggest issue that needs to be addressed, however, is the underlying tension between the desire of military establishments to exploit cyberspace for military advantages, and concerns about the dependency of governments, economies and societies on networked information systems. This contradiction needs to be addressed carefully before a conclusive international regime for the protection of cyber-space can be developed. Not only should international law enforcement agreements and capacities be strengthened, but a ban on the use of cyber-weapons by nation-states should also be given serious consideration, despite all the likely difficulties that such a regime would encounter, particularly in terms of enforcement. Cyberspace is too valuable an asset for the entire world to jeopardize it in the name of national security.

References

Alberts, D.S. and Papp, D.S. (eds) (1997) *The Information Age: An Anthology of Its Impacts and Consequences (Vol. I)*, Washington: National Defense University Press.

Arquilla, J. and Ronfeldt, D.F. (eds) (1997a) *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica: RAND.

——(1997b), 'Cyberwar is coming!', in Arquilla, J. and Ronfeldt, D.F. (eds) *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica: RAND, pp. 23–60.

Barak, S. (2004) 'Between violence and "e-jihad": Middle Eastern terror organizations in the information age', in Nicander, L. and Ranstorp, M. (eds) *Terrorism in the Information Age – New Frontiers?* Swedish National Defence College, pp. 83–96.

Bendrath, R. (2003) 'The American cyber-angst and the real world – Any link?' in Latham, R. (ed.) *Bombs and Bandwidth: The Emerging Relationship between IT and Security*, New York: The New Press, pp. 49–73.

Bequai, A. (1986) *Technocrimes: The Computerization of Crime and Terrorism*, Lexington: Lexington Books.

Borger, J. (1999) 'Pentagon kept the lid on cyberwar in Kosovo', *The Guardian*, 9 November. Available online at: www.guardian.co.uk/Kosovo/Story/0,2763,197391,00.html (accessed 9 January 2009).

Bradley, G. (2003) 'Bush orders guidelines for cyber-warfare: Rules for attacking enemy computers prepared as U.S. weighs Iraq options', *Washington Post*, 7 February, p. A01.

Brunner, E. and Suter, M. (2008) *The International CIIP Handbook 2008: An Inventory of Protection Policies in 25 Countries and 6 International Organizations*. Zurich: Center for Security Studies.

Buzan, B. (1991) *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, 2nd edn, Brighton: Harvester Wheatsheaf.

Buzan, B., Wæver, O. and de Wilde, J. (1998) *Security: A New Framework for Analysis*, Boulder: Lynne Rienner.

Campen, A.D., Dearth, D.H. and Goodden, T. (eds) (1996) *Cyberwar: Security, Strategy and Conflict in the Information Age*, Fairfax, AFCEA International Press.

Conway, M. (2008) 'The media and cyberterrorism: A study in the construction of "reality"', in Dunn Cavelty, M. and Kristensen, K.S. (eds) *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation*, London: Routledge, pp. 109–29.

Covert, C. (1983) 'Seven curious teenagers wreak havoc via computer', *Detroit Free Press*, 28 August, Section: WWL, p. 1F.

CSTIW, Center for the Study of Terrorism and Irregular Warfare (1999) *Cyberterror: Prospects and Implications*, White Paper.

Daase, C., Feske, S. and Peters, I. (eds) (2002) *Internationale Risikopolitik: Der Umgang mit neuen Gefahren in den internationalen Beziehungen*, Baden-Baden: Nomos Verlagsgesellschaft.

Delio, M. (2001) 'Is this World Cyber War I?' *Wired*, 1 May.

Denning, D. (2001) 'Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy', in Arquilla, J. and Ronfeldt, D. (eds) *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica: RAND, pp. 239–88.

DOD Dictionary of Military and Associated Terms (2008). Available online at: www.js.mil/doctrine/jel/doddict/data/c/01183.html (accessed 9 January 2009).

Devost, M.G., Houghton, B.K. and Pollard, N.A. (1997) 'Information terrorism: Political violence in the information age', *Terrorism and Political Violence* 9, 1: 72–83.

Dunn, M. (2002) *Information Age Conflicts: A Study on the Information Revolution and a Changing Operating Environment*. Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 64, Zurich: Center for Security Studies.

Dunn Cavelty, M. (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, London: Routledge.

Dunn Cavelty, M. and Brunner, E. (2007) 'Information, power, and security: An outline of debates and implications', in Dunn Cavelty, M., Mauer, V. and Krishna-Hensel, S.-F. (eds) *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, Aldershot: Ashgate, pp. 1–18.

Eriksson, J. and Giacomello, G. (2007) 'Conclusion: Digital-age security in theory and practice', in Eriksson, J. and Giacomello G. (eds) *International Relations and Security in the Digital Age*, London: Routledge, pp. 173–84.

FitzGerald, M.C. (1994) 'Russian views on electronic signals and information warfare', *American Intelligence Journal* 15, 1: 81–87.

Green, J. (2002) 'The myth of cyberterrorism', *Washington Monthly*, November 2002. Available online at: www.washingtonmonthly.com/features/2001/0211.green.html (accessed 9 January 2009).

Henry, R. and Peartree, E.C. (eds) (1998) *Information Revolution and International Security*, Washington: Center for Strategic and International Studies.

Ingles-le Nobel, J.J. (1999) 'Cyberterrorism hype', *Jane's Intelligence Review*, 21 October.

Kenyon, H.S. (2007) 'Cyberspace command logs in', *Signal* 61, 12: 35–38.

Libicki, M. (1997) *Defending Cyberspace*, Washington, DC: National Defense University.

van Loon, J. (2002) *Risk and Technological Culture: Towards a Sociology of Virulence*, London: Routledge.

Mahnken, T.G. (1995) 'War in the information age', *Joint Force Quarterly* 10: 39–43.

Minihan, K. (1998) *Statement of Lieutenant General Kenneth Minihan, USAF, Director, NSA to the Senate Governmental Affairs Committee Hearing on Vulnerabilities of the National Information Infrastructure*, 24 June 1998. Available online at: www.senate.gov/~govt-aff/62498minihan.htm (accessed 9 January 2009).

Molander, R.C., Riddle, A.S. and Wilson, P.A. (1996) *Strategic Information Warfare: A New Face of War*, Santa Monica: RAND.

Mulvenon, J.C. and Yang, R.H. (eds) (1998) *The People's Liberation Army in the Information Age*, Santa Monica: RAND.

National Academy of Sciences (1991) Computer Science and Telecommunications Board, *Computers at Risk: Safe Computing in the Information Age*, Washington, DC: National Academy Press.

Nye, J.S. Jr. and Owens, W.A. (1996) 'America's information edge', *Foreign Affairs* 75, 2: 20–36.

Parker, D.B. (1983) *Fighting Computer Crime*, New York: Charles Scribner's Sons.

PCCIP, President's Commission on Critical Infrastructure Protection (1997) *Critical Foundations: Protecting America's Infrastructures*, Washington, DC: US Government Printing Office.

Pollitt, M.M. (1997) 'Cyberterrorism – Fact or fancy?' *Proceedings of the 20th National Information Systems Security Conference*, pp. 285–89.

Porteus, L. (2001) 'Feds still need to define role in tackling cyberterror, panelists say', *GovExec.com*, 15 May 2001. Available online at: www.govexec.com/dailyfed/0501/051501td.htm (accessed 9 January 2009).

Poulsen, K. (1999) 'Info war or electronic sabre rattling?' *ZDNet*, 8 September. Available online at: http://news.zdnet.com/2100–9595_22–515631.html?legacy=zdnn (accessed 9 January 2009).

Rasmussen, M.V. (2001) 'Reflexive security: Nato and international risk society', *Millennium: Journal of International Studies* 30, 2: 285–309.

Rathmell, A. (2001) 'Controlling computer network operations', *Information & Security: An International Journal* 7, pp. 121–44.

Ross, A. (1990) 'Hacking away at the counterculture', in Penley, C. and Ross, A. (eds) *Technoculture*, Minneapolis: University of Minnesotta Press, pp. 107–34.

Schneier, B. (2007), 'Schneier on security: A blog covering security and security technology'. Available online at: www.schneier.com/blog/archives/2007/06/cyberwar.html (accessed 9 January 2009).

Shea, D.A. (2003) *Critical Infrastructure: Control Systems and the Terrorist Threat*, Congressional Research Report for Congress, RL31534, 21 February, Washington, DC: Congressional Research Service.

Stoll, C. (1989) *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*, New York: Doubleday.

Thomas, T.L. (2004) *Dragon Bytes: Chinese Information-War Theory and Practice*, Ft Leavenworth: Foreign Military Studies Office.

Traynor, I. (2007) 'Russia accused of unleashing cyberwar to disable Estonia', *The Guardian*, 17 May.

Shorrok, T. (2008) *Spies for Hire: The Secret World of Intelligence Outsourcing*, New York: Simon and Schuster.

Silverstein, K. (2000) *Private Warriors*, New York and London: Verso.

Singer, P.W. (2003) *Corporate Warriors: The Rise of the Privatized Military Industry*, Ithaca, NY and London: Cornell University Press.

Spearin, C. (2008) 'Private, armed and humanitarian? States, NGOs, international private security companies and shifting humanitarianism', *Security Dialogue* 39, 3: 363–82.

Spicer, T.L.C. (1999) *An Unorthodox Soldier: Peace and War and the Sandline Affair*, Edinburgh: Mainstream.

Susman, G. and O'Keefe, S. (eds) (1998) *The Defense Industry in the Post-Cold War Era: Corporate Strategies and Public Policy Perspectives*, Oxford: Pergamon.

Thomson, J. (1994) *Mercenaries, Pirates, and Sovereigns: State-building and Extraterritorial Violence in Early Modern Europe*, Princeton: Princeton University Press.

Tiefer, C. (2007) 'The Iraq debacle: The rise and fall of procurement-aided unilateralism as a paradigm of foreign war', *University of Pennsylvania Journal of International Economic Law* 29: 1–56.

UN (2009) 'The UN working group on the use of mercenaries as a means of violating human rights and impending the exercise of the right of peoples to self-determination'. Available online at: www2.ohchr.org/english/issues/mercenaries/wgstandards.htm (accessed 24 February 2009).

Verkuil, P. (2007) *Outsourcing Sovereignty: Why Privatization of Government Functions Threatens Democracy and What We Can Do about It*, Cambridge: Cambridge University Press.

War on Want (2006) *Corporate Mercenaries*. Available online at: www.waronwant.org/Corporate%20Mercenaries%2013275.twl (accessed 28 February 2009).

Young Pelton, R. (2006) *Licensed to Kill: Hired Guns in the War on Terror*, New York: Crown Publishers.

Zamparelli, C.S.J. (1999) 'Competitive sourcing and privatization: Contractors on the battlefield', *Air Force Journal of Logistics*, XXIII: 1–17.