2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

The Militarisation of Cyberspace: Why Less May Be Better

Myriam Dunn Cavelty
Center for Security Studies
ETH Zurich / Swiss Federal
Institute of Technology
CH- 8092 Zürich, Switzerland
dunn@sipo.gess.ethz.ch

Abstract: Cyber security is seen as one of the most pressing national security issues of our time. Due to sophisticated and highly publicised cyber attacks, it is increasingly framed as a strategic-military concern and many states have or at least want to acquire offensive cyber "weapons". The aim of this paper is to show that particular ways of framing threats are not only a matter of choice but also come with political and social effects. Focusing on the strategic-military aspects of cyber security means subjecting it to the rules of an antagonistic zero-sum game, in which one party's gain is another party's loss. This invokes enemy images even though there is no identifiable enemy, centres too strongly on national security measures instead of economic and business solutions, and wrongly suggests that states can establish control over cyberspace. This creates an unnecessary atmosphere of insecurity and tension in the international system - one that is based on misperceptions of the nature and level of cyber risk and on the feasibility of different protection measures in a world characterised by complex, interdependent risk. While it is undisputed that the cyber dimension will play a substantial role in future conflicts of all grades and shades, threat-representations must remain well informed and well balanced at all times in order to rule out policy (over-) reactions with unnecessary costs and uncertain benefits.

Keywords: *cyber security, cyber war, vulnerability-based planning, threat framing*

1. INTRODUCTION

As a result of increasingly sophisticated cyber incidents and intensifying media attention over the last few years, cyber security issues have moved in two directions: upwards, from the expert level to executive decision-makers and politicians; and 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. On the national level, several governments have released or updated cyber security strategies in 2011.[1] Internationally, there is heightened attention on the strategic-military aspects of the problem – indicated by the growing number of conferences that address the issue,

1 Examples are France, Germany, India, the Netherlands, the United Kingdom, the United States and Switzerland.

efforts to obtain offensive capabilities, and attempts to come to an international agreement on the military (mis)use of cyberspace.

Though the heightened attention on cyber threats coupled with the overall sense of urgency to find viable political solutions could easily create the impression that policy-makers are confronted with an altogether 'new' issue, the current episode is just the latest development in the three to four decade long history of cyber threats. From the very beginning of the cyber threat story in the 1980s, there was a national security connotation to it (Dunn Cavelty 2008). However, that particular focus has intensified over the years, in parallel to society's increasing 'cyberification' and the overall impression that cyber incidents are becoming more frequent, more organised, more costly, and altogether more dangerous.

The establishment of cyber threats as a focal point of the current national security debate amongst Western states can be seen as a confluence of two interlinked and mutually reinforcing factors: the perception that modern societies are exposed to an ever-increasing number of potentially catastrophic vulnerabilities (Furedi 2008), and the perception of an increasing willingness of dangerous actors to ruthlessly exploit these vulnerabilities. This pervasive sense of vulnerability comes with a heightened sense of dread and urgency; and has led to a propensity to 'militarise' the cyber security debate.[2] The (unintended side) effects of this particular threat framing are the focus of this paper.

The aim is to show that particular ways of framing threats or risks are not only a matter of choice (within certain boundaries) but also come with political and social effects. Zooming in on the strategic-military aspects of cyber security means subjecting it to the rules of an antagonistic zero-sum game, in which one party's gain is another party's loss. This invokes images of a supposed adversary even though there is no identifiable enemy, is too strongly focused on national security measures instead of economic and business solutions, and wrongly suggests that states can establish control over cyberspace. In all, this creates an unnecessary atmosphere of insecurity and tension in the international system, which is based on misperceptions of the nature and level of cyber risk and on the feasibility of different protection measures in a world characterised by complex, interdependent risk.

To make this argument, the paper first describes three alternative ways of framing cyber security. This includes looking back to the 1990s when a well-balanced set of policy-responses took shape that were characterised mainly by a focus on the protection of critical infrastructures by technical means and a limited role of the military. The second subchapter examines recent developments and occurrences (spearheaded by Stuxnet, the Industry-sabotaging super-worm) that have given rise to an increasing focus on and attempts to acquire offensive cyber means. The third section critically assesses both the underlying assumptions behind this trend and the detrimental effects it has on the overall level of security. It is suggested that moving away from the propensity to think about worst-case scenarios and focusing on everyday occurrences like cyber crime and cyber espionage is the solution. The chapter concludes by arguing that military countermeasures will not be able to play a significant role in cyber security due to the nature of the information environment as well as the nature of the threat.

2 I use the term militarisation loosely, to connote the particular focus on the strategic-military dimen-sions of a problem and the adoption of something for use by or in the military.

2. ALTERNATIVE CYBER-IN-SECURITY FRAMINGS

In the evolution of the cyber security debate, we can distinguish between three different, yet closely interrelated and reinforcing discourses.

TABLE 1: THREE ALTERNATIVE CYBER DISCOURSES

	Technical	Crime-Espionage	Military / Civil defence
Main actors	• Computer experts • Anti-virus industry	• Law enforcement • Intelligence community	• National security experts • Military • Civil defence establishment / Homeland security
Main referent object	• Computers • Computer networks	• Private sector (business networks) • Classified information (government networks)	• Networked armed forces (military networks) • Critical (information) infrastructures
Main Threat	• Malware • Network disruptions • Hackers (all kinds)	• Advanced Persistent Threats • Cyber Criminals • Cyber mercenaries • States (foreign intelligence)	• Catastrophic attacks on critical infrastructures • Cyber terrorists • States (cyber commands)

The first is technical and concerned with malware (viruses, worms, etc.) and system intrusions. The second is concerned with cyber crime and cyber espionage. The third is discourse driven and initiated by the US military, initially focusing on matters of cyber war but increasingly also on critical infrastructure protection within the realm of civil defence/protection or homeland security. Each of them is uniquely shaped and dominated by specific actors and revolves around particular 'referent objects' (that which is seen in need of protection, see Buzan et al. 1998) and threats, as summarised in Table 1.

A. Viruses, Worms and Other Bugs (Technical Discourse)

The technical discourse is focused on computer and networks disruptions caused by different types of malware. In 1988, the ARPANET – the precursor of today's Internet – had its first major network incident: the 'Morris Worm'. The worm used so many system resources that large parts of the early Internet went down. The rather devastating technical effect prompted the Defense Advanced Research Projects Agency (DARPA, who was in charge of the network at the time) to set up a centre to coordinate communication among computer experts during IT emergencies and to help prevent future incidents: a Computer Emergency Response Team (CERT) (Scherlis et al. 1990). This centre, now called the CERT Coordination Center, still plays a considerable role in computer security and served as a role model for similar centres around the world. Around the same time, the anti-virus industry emerged, bringing with it techniques and programs for virus recognition, destruction and prevention.

The worm also had a substantial psychological and, subsequent, political impact by making policy-makers aware of the Internet's insecurity and unreliability. While it was acceptable in the 1960s for pioneering computer professionals to hack and investigate computer systems,

the situation changed by the 1980s. Society had become dependent on computing for everyday business practices and other basic functions. Tampering with computers suddenly meant potentially endangering people's careers and property; and some even said their lives (Spafford 1989). Ever since, malware, as 'visible' proof of the persuasive insecurity of the information infrastructure, has remained in the limelight of the cyber security discourse – and provides the back-story for the other two discourses.

B. Cyber Crooks and Digital Spies (Crime-Espionage Discourse)

The cyber crime and technical discourses, respectively, are very closely related. The development of IT law (and, more specifically, Internet or cyber law) in different countries plays a crucial role in the second discourse, largely as it allows the definition and prosecution of a misdemeanour. Not surprisingly, the development of legal tools to prosecute unauthorized entry into computer systems (like the Computer Fraud and Abuse Act of 1986 in the United States) coincided with the first serious network incidents (cf. Mungo and Clough 1993).

Cyber crime has come to refer to any crime that involves computers and networks, like the release of malware or spam, fraud, and many other things. Until today, notions of computer-related economic crimes determined the discussion about computer misuse. However, a distinct national-security dimension was established when computer intrusions (a criminal act) were clustered together with the more traditional and well-established espionage discourse. Prominent hacking incidents – such as the intrusions into high-level computers perpetrated by Milwaukee-based '414s' gang (6 teenagers) – led to a feeling in policy circles that there was a need for action (Ross 1991): If teenagers were able to penetrate computer networks that easily, it was assumed that better organized entities such as states would be even better equipped to do so. Over the years, this discourse has become particularly focused on so-called advanced persistent threats, a cyber attack category which connotes an attack with a high degree of sophistication and stealthiness over a prolonged duration of time. The attack objectives typically extend beyond immediate financial gain.

C. Information Warfare and Critical Infrastructures (Military-Civil Defence Discourse)

The link between information technology and national security was firmly established in military writings in the time after the Second World War (Edwards 1996). But it was the Second Persian Gulf War of 1991 that created a watershed in US military thinking about cyber war. Military strategists saw the conflict as the first of a new generation of conflicts, in which physical force alone was not sufficient, but was complimented by the ability to win the information war and to secure 'information dominance'. As a result, American military thinkers began to publish scores of books on the topic and developed doctrines that emphasized the ability to degrade or even paralyse an opponent's communications systems (cf. Campen 1992).

In the mid-1990s, the advantages of the use and dissemination of Information Communication Technology (ICT) that had fuelled the revolution in military affairs were no longer seen only as a great opportunity providing the country with an 'information edge' (Nye and Owens 1996), but were also perceived as constituting an over-proportional vulnerability vis-à-vis a malicious state and non-state actors (Rattray 2001). This perception was shaped by the larger strategic

context that emerged for the United States after the Cold War. The new environment was characterised by more dynamic geostrategic conditions, numerous areas and issues of concern as well as smaller, more agile and more diverse adversaries. As a result of the difficulties to locate and identify enemies, parts of the focus of security policies shifted away from actors, capabilities, and motivations to general vulnerabilities of the entire society. Global information networks seemed to make it much easier to attack the US asymmetrically, as such attacks no longer required big, specialized weapons systems or an army: borders, already porous in many ways in the real world, were non-existent in cyberspace. It seemed only a matter of time until those actors, likely to fail against American military power, would seek to bring the US to its knees by striking vital points fundamental to the national security and essential functioning of industrialized societies at home (Berkowitz 1997): critical infrastructures.

At the same time, the development of military doctrine for the information domain continued. For a while, information warfare – the new type of warfare in the information age – remained essentially limited to military measures in times of crisis or war. This shifted around the mid-1990s, when the activities began to be understood as actions targeting the entire information infrastructure of an adversary – political, economic, and military, throughout the continuum of operations from peace to war (Brunner and Dunn Cavelty 2009). 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 website defacements, a number of DDoS-attacks[3], and (unsubstantiated) rumours that Slobodan Milosevic's bank accounts had been hacked by the US armed forces (Dunn 2002: 151). The increasing use of the Internet during the conflict gave it the distinction of being the 'first war on the Internet'.

D. Countermeasures

By the end of the 1990s, the three discourses had produced specific types of concepts and actual countermeasures on the national and the international level in accordance with their focus (see Table 2). Worldwide, the protection policies that transpired consisted of a three-pronged approach: A strong law enforcement pillar for countering cyber crime, private-public partnerships for critical infrastructure protection (Dunn Cavelty and Suter 2009), and private and public self-help for the rest of the networked infrastructures. It became a common pragmatic practice that everybody was quasi responsible for 'their own': governments protect government networks, militaries only military ones, companies protect theirs, and every individual out there is in charge of their own computer security.

However, there are some assets in the hands of the private sector considered so crucial to the functioning of society that governments take additional measures to ensure an adequate level of protection. These efforts are usually subsumed under the label of critical (information) infrastructure protection (CIIP). At the core of these practices, we find the strategy of preparation, meaning the preventive protection of critical infrastructures by technical means, namely information assurance practices (May et al. 2004), supplemented by the concept of resilience. Resilience, a concept which accepts that disruptions are inevitable, is commonly defined as the ability of a system to recover from a shock, either returning back to its original

3 Attempts to make a computer or network resource unavailable to its intended users, mostly by satu-rating the target machine with external communications requests so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.

state or to a new adjusted state. Therefore, the concept promises an additional safety net against large-scale, major and unexpected events (Perelman 2007; Dunn Cavelty 2011b).

TABLE 2: SET OF COUNTERMEASURES AT THE END OF THE 1990S

	Technical	Crime-Espionage	Civil defence	Strategic-military
Basic Protection concept	Information Assurance			
National level	• CERTs	• Computer law	• Critical (information) infrastructure protection	• Cyber defence (for military networks) • Resilience
International level	• International CERTs • Information security standards	• Harmonization of law • Mutual judicial assistance procedures	• Resilience	• (Cyber arms control)

Particularly interesting about these policy solutions is the relatively small role of the state. The consequences of cyber vulnerabilities for the well-being of a nation are very high – at least in theory. Therefore, a national security connotation seemed a natural given as soon as the link to critical infrastructure was made in the third discourse. But while military documents and strategists were influential in shaping general threat perceptions and in bringing the issue of cyber threats to the attention of a broad audience, the reality of the main referent object – critical infrastructures, most of them in the hand of the private sector – and the nature of the threat made it impossible for the traditional national security bodies, especially the military, to play a larger role in countering it.

For example, high-level cyber attacks against infrastructure targets would likely be the culmination of long-term, subtle, systematic intrusions. The preparatory phase could take place over several years. When – or rather if – an intrusion is detected, it is often impossible to determine whether it was an act of vandalism, computer crime, terrorism, foreign intelligence activity, or some form of strategic military attack. The only way to determine the source, nature, and scope of the incident is to investigate it. This again might take years, rendering highly uncertain results. The military notion of striking back electronically or kinetically is therefore unusable in most cases.

In addition, cyber threats defy the well-proven concept of deterrence. Deterrence works if the one party is able to successfully convey to another that it is both capable and willing to use a set of available (often military) instruments against him if the other steps over the line. This requires an opponent that is clearly identifiable as an attacker and has to fear retaliation – which is not the case in the cyber domain because of the so-called attribution problem; the architecture of cyberspace makes it difficult to clearly determine those initially responsible for a cyber attack as well as to identify motivating factors. Attacks and exploits that seemingly benefit states might well be the work of third-party actors operating under a variety of motivations. At the same time, the challenges of clearly identifying perpetrators gives state actors convenient

'plausible deniability and the ability to officially distance themselves from attacks' (Deibert and Rohozinski 2009: 12). Blame on the basis of the 'cui bono'-logic (which translates into 'to whose benefit') on the other hand is not sufficient proof for political action (in most cases). Therefore, deterrence and retribution do not work in cyberspace and will not, unless its rules are changed in substantial ways, with highly uncertain benefits (Libicki 2009). Though fears of future cyber wars existed at the time, efforts to control the military use of computer exploitation through arms control or multilateral behavioural norms like agreements that might pertain to the development, distribution, and deployment of cyber weapons, or to their use, remained limited (Denning 2001), at least until recently.

3. THE 'STUXNETIFICATION' OF THE DEBATE

The set of practices as described above remained fairly stable for more than a decade. More recently, however, the threat perception has changed – and with it how some governments address the issue. Four recent trends and developments have solidified the impression that cyber disturbances are increasingly dangerous and aggressive and that governments should react more forcefully to them – particularly by enhancing their own offensive capabilities.

First, there is heightened concern with the rising level of professionalization coupled with the obvious criminal (or even strategic) intent behind attacks. Advanced malware is targeted: A hacker picks a victim, scopes the defences and then designs malware to get around them (Symantec 2010). The most prominent example for this kind of malware is Stuxnet (addressed below). This development goes in sync with the development of the cyber crime market, which is driven by the huge sums of money available to criminal enterprises at low risk of prosecution (Panda Security 2010).

Second, the main cyber 'enemy' has been singled-out: there is an increase in allegations that China is responsible for cyber espionage in the form of high-level penetrations of government and business computer systems in Europe, North America, and Asia. Because Chinese authorities have stated repeatedly that they consider cyber space to be a strategic domain and by mastering it they may be able to equalise the existing military imbalance between China and the US more quickly, many US officials readily accuse the Chinese government of deliberate and targeted attacks or intelligence gathering operations (Ball 2011).

Third, there is an increase in sophisticated hacktivism activities. WikiLeaks, for example, has added yet another twist to the cyber espionage discourse. Acting under the hacker-maxim 'all information should be free', this type of activism deliberately challenges the self-proclaimed power of states to keep information, which they think could endanger or damage national security, secret. Related are the multifaceted activities of hacker collectives such as Anonymous or LulzSec, who humiliate high-visibility targets by DDoS-attacks, break-ins and release of sensitive information. In addition, more and more conflicts of political or economic nature have a cyber(ed)-component these days (Deibert et al. 2012; Demchak 2010), which often includes hacktivism activities. Perhaps the most prominent example is the Estonian 'cyber war' case of 2007.

Fourth, the discovery of the computer worm Stuxnet in 2010 changed the overall tone and intensity of the debate once and for all. Stuxnet is a very complex programme. It is likely that writing it took a substantial amount of time, advanced-level programming skills and insider knowledge of industrial processes. Therefore, Stuxnet is probably the most expensive malware ever found. In addition, it behaves differently from the normal criminal-type malware: it does not steal information and it does not herd infected computers into so-called botnets to launch further attacks from (Gross 2011). Rather, it looks for a very specific target: Stuxnet was written to attack Siemens' *Supervisory Control and Data Acquisition* (SCADA) systems that are used to control and monitor industrial processes. In August 2010, the security company Symantec noted that 60% of the infected computers worldwide were in Iran. Moreover, reports alleged that the Iran nuclear program had been delayed as some centrifuges had been damaged. The picture that materializes from the pieces of this puzzle seems to suggest that only one or several nation states – the 'cui bono' logic pointing either to the US or Israel – would have the capability and interest to produce and release Stuxnet in order to sabotage the Iranian nuclear program (Farwell and Rohozinski 2011).

4. UNINTENDED SIDE-EFFECTS: CAUSES AND REMEDIES

This 'story', which is indeed convincing and plausible, has seized to be a mere story: it has become the truth, despite the fact that the evidence for Stuxnet being a government-sponsored cyber weapon directed at Iran is purely circumstantial. It may in fact never be possible to know for certain who gave the order to program Stuxnet, who actually did it, and what the intent behind it was. However, this is strangely irrelevant: The only thing that does matter in this instance is what states make of it – because it is their actions and reactions that create political reality.

The reaction is that more and more states are opening up or enhancing 'cyber commands', which are military units for cyber war activities, because just the possibility that one or several state actors are behind the computer worm means that this *could* mark the beginning of the unchecked use of cyber weapons in open or more clandestine military aggressions. Though consolidated numbers are hard to come by, the amount of money spent on defence-related aspects of cyber security is rising. The new cyber military-industrial complex, for instance, is estimated to make returns between $80-billion and $150-billion US dollars a year, with big defence companies like Boeing and Northrop Grumman repositioning themselves to service the expanding cyber security market (Deibert and Rohozinski 2011).

Following the strategic logic, several states have ramped up their rhetoric. For example, Iranian and Indian officials have gone on public record condoning hackers who work in the state's interest. The White House's new International Strategy for Cyberspace of 2011 states that the United States reserves the right to retaliate against hostile acts in cyberspace with military force. Because cyber capabilities cannot be divulged by normal intelligence gathering activities, uncertainty and mistrust are on the rise. The first signs of a 'cyber security dilemma' are discernible: Although most states still predominantly focus on cyber defence issues, measures

taken by some nations are seen by others as covert signs of aggression by others, and will likely fuel more efforts to master 'cyber weapons'.

As pointed out in the introduction, reacting this way is not inevitable (though arguably understandable). It is a matter of choice, or at least a matter of a political process that has produced this particular outcome. Unfortunately, it is making both the virtual but also the real world less and not more safe. The overall aim of cyber security policy is to reduce the risks in and through cyberspace. If certain reactions or policy approaches are becoming complicit in creating more insecurity, then they should be corrected. The good news is that there are alternatives both in framing the issue and in countering it, and that both these frames and these countermeasures are already in place, as shown above. For a reframing to become possible, however, skewed threat perceptions that are the outcome of government circles to focus too much on high-impact, low-probability events need to be corrected.

A. Why the Threat is Persistently Overrated

Every political, economic and military conflict nowadays has a cyber(ed)-component. Furthermore, criminal and espionage activities with the help of computers happen every day. It is a fact that cyber incidents are continually causing minor and occasionally major inconveniences in the form of lost intellectual property or other proprietary data, maintenance and repair, lost revenue, and increased security costs. Beyond the direct impact, badly handled cyber attacks have also damaged corporate (and government) reputations. However, in the entire history of computer networks, cyber attacks have never caused serious long-term disruptions. They are risks that can be dealt with by individual entities using standard information security measures and their overall costs remain low in comparison to other risk categories like financial risks.

Despite this, the threat keeps being 'hyped' in policy circles. There are several reasons for this: First, psychological research has shown that risk perception is highly dependent on intuition and emotions, also the perceptions of experts (Gregory and Mendelsohn 1993). Cyber risks, especially in their more extreme form, fit the risk profile of so-called 'dread risks', which appear uncontrollable, catastrophic, fatal, unknown and basically uncontrollable. There is a propensity to be disproportionally afraid of these risks despite their low probability, which translates into pressure for regulatory action of all sorts and willingness to bear high costs of uncertain benefit.

Second, combating cyber threats has become a highly politicised issue. Therefore, official statements about the threat must also be seen in the context of different bureaucratic entities that compete against each other for resources and influence or of politicians taking up this new and politically 'hot' issue. This is usually done by stating an urgent need for action and describing the overall threat as big and rising. Furthermore, being a cyber-expert has become a lucrative market, but only if the problem is continuously portrayed as grave.

Third, the media loves the idea of cyber-'anything' in connection with disaster, and routinely features sensationalist headlines that cannot serve as a measure of the problem's scope. By reporting only on a certain type of cyber-issue, they distort the threat perception. Some IT security companies have recently warned against overemphasizing so called advanced persistent threat attacks just because we hear more about them (Verizon 2010: 16). Only about 3% of all

incidents in 2010 were considered so sophisticated that they were impossible to stop. The vast majority of attackers go after low hanging fruit, which are small to medium sized enterprises with bad defences and little security awareness (Maillart and Sornette 2010).

B. From Vulnerability Assumptions to Threat Assessments

Since the effects of cyber attacks are potentially devastating, the temptation to not only think about worst-case scenarios but also give them a lot of (or rather too much) weight, despite their low probability, is high. This problem is aggravated by a broader tendency in security politics. The handling of issues is directly linked to level of knowledge, but more importantly non-knowledge about threats. Traditional threat analysis looked at the capability or potential of enemies and their intent or motivation, in addition to one's own vulnerability. Cyber threats, however, are highly diffuse and many aspects are unknowable. There is no reliable data for loss or damage estimation within our current cyber pattern of cyber usage and it is very unlikely that there will ever be satisfactory solutions to this data problem. Attempts to collect it have failed due to insurmountable difficulties in establishing what to measure, how to measure it, and what to do about incidents that are discovered very late, or not at all (Sommer and Brown 2011: 12).

Missing knowledge of this sort has led to increasing use of vulnerability-based analysis, based solely on the identification of weaknesses (Jenkins 2006: 120). When looking at vulnerabilities, the follow-up question is: 'what could go wrong?' and the natural answer is: 'everything'. This almost automatically leads to worst-case scenarios. However, these scenarios have a habit to become reified in the political process. When this happens, they are turned into real threats, not potentials, based not on knowledge about the intentions and capabilities of potential adversaries but mainly on policy-makers' fears (Furedi 2008: 652).

Such thinking distracts attention from the highly relevant questions of 'what can' and 'what is likely' to happen (Furedi 2008: 653). The correct assumption that modern societies and their armed forces depend on the smooth functioning of information and communication technology does not automatically mean that this dependence or vulnerability *will* be exploited. Patching all the vulnerabilities of modern societies is outright impossible and also not politically or economically desirable. Therefore, the policy community must return to level-headed threat assessments that ask 'who has the interest and the capability to attack us and why would they?'

At the moment, most experts agree that strategic cyber war (and catastrophic attacks) remains highly unlikely in the foreseeable future, mainly due the uncertain results such a war would bring, the lack of motivation on the part of the possible combatants, and their shared inability to defend against counterattacks (Sommer and Brown 2011). Cyber crime and cyber espionage, both political and economic, are a different story: they are here and will remain the biggest cyber risks in the future. Very clearly, they deserve the full attention of the policy community much more than their unlikely counterparts.

5. CONCLUSION

Thinking about (and planning for) worst-case scenarios is a legitimate task of the national security apparatus. However, catastrophic incidents should never receive too much attention at the expense of more plausible and possible cyber problems. Using too many resources for high impact, low probability events – and therefore having less resources for the low to middle impact and high probability events – does not make sense, neither politically, nor strategically and certainly not when applying a cost-benefit logic.

Despite the increasing attention cyber security is getting in security politics, computer network vulnerabilities are mainly a business and espionage problem. Further militarising cyberspace based on the fear of other states' cyber capabilities is pointless. While it is undisputed that the cyber dimension will play a substantial role in future conflicts of all grades and shades, threat-representations must remain well informed and well balanced at all times in order to rule out policy (over)reactions with too high costs and uncertain benefits. Regardless of how high we judge the risk of a large-scale cyber attack, military-type countermeasures will not be able to play a substantial role in cyber security because of the nature of the attacker, the nature of the attacked, and the nature of the cyber(ed)-environment. Investing too much time talking about them or spending increasing amounts of money on them is not going to make cyberspace more secure – quite the contrary.

Cyberspace is only in parts controlled or controllable by state actors. At least in the case of democracies, power in this domain is in the hands of private actors, especially the business sector. Much of the expertise and many of the resources required for taking better protective measures are located outside governments. The military – or any other state entity for that matter – does not own critical (information) infrastructures and has no direct access to them. Protecting them as a military mandate is an impossibility and considering cyberspace as an occupation zone is an illusion. Militaries cannot defend the cyber space of their country – it is no space where troops and tanks can be deployed because the logic of national boundaries does not apply.

Undoubtedly, however, attacks on information technology, manipulation of information, or espionage can have serious effects on the present and/or future of defensive or offensive effectiveness of one's own armed forces. First and foremost, militaries should therefore focus on the protection and resilience of their information infrastructure and networks, particularly the critical parts of it, at all times. Beyond this, governments and military actors should acknowledge that their role in cyber security can only be a limited one, even if they consider cyber attacks to be a major national security threat. Cyber security is and will remain a shared responsibility between public and private actors. Governments should maintain their role in protecting critical infrastructure where necessary, while determining how to best encourage market forces to improve the security and resilience of company owned networks.

REFERENCES

Ball, D. (2011), 'China's Cyber Warfare Capabilities', *Security Challenges*, 7/2: 81–103.

Berkowitz, B.D. (1997), 'Warfare in the Information Age', in Arquilla, J. and Ronfeldt, D.F. (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: RAND), 175–90.

Brunner, E. and Dunn Cavelty, M. (2009), 'The Formation of In-Formation by the US Military', *Cambridge Review of International Affairs*, 22/4: 629–646.

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

Campen, A.D. (1992) (ed.), *The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War* (Fairfax: AFCEA International Press).

Deibert, R. and Rohozinski, R. (2011), 'The new cyber military-industrial complex', The Globe and Mail, March 28, 2011. Accessed 3 March 2012, http://www.theglobeandmail.com/news/opinions/opinion/the-new-cyber-military-industrial-complex/article1957159/.

Deibert, R. and Rohozinski, R. (2009), 'Tracking GhostNet: Investigating a Cyber Espionage Network', Information Warfare Monitor (Toronto: The Munk School of Global Affairs).

Deibert, Ronald J., Rohozinski, R. and Crete-Nishihata, M. (2012), 'Cyclones in cyberspace : informatoin shaping and denial in the 2008 Russia-Georgia war', Security Dialogue 43/3: 3-24.

Demchak, C. (2010), 'Cybered Conflict as a New Frontier', *New Atlanticist*,. Accessed 3 March 2012, http://www.acus.org/new_atlanticist/cybered-conflict-new-frontier.

Denning, D. (2001), 'Obstacles and Options for Cyber Arms Controls', paper presented at the Arms Control in Cyberspace Conference, Heinrich Böll Foundation, Berlin, 29-30 June 2001. Accessed 3 March 2012 http://www.cs.georgetown.edu/~denning/infosec/berlin.doc.

Dunn, M. (2002), *Information Age Conflicts: A Study of the Information Revolution and a Changing International Operating Environment* (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. (2011a), 'Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture', *IP Global Edition*, 12/3: 11–15.

Dunn Cavelty, M. (2011b), 'Systemic cyber/in/security – From risk to uncertainty management in the digital realm', *Swiss Re Risk Dialogue Magazine*, 15 September.

Dunn Cavelty, M. and Suter, M. (2009), 'Public-Private Partnerships are no Silver Bulled: An Expanded Governance Model For Critical Infrastructure Protection', *International Journal of Critical Infrastructure Protection*, 2/4: 179–87.

Edwards, P.N. (1996), *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press).

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

Furedi, F. (2008), Fear and Security: A Vulnerability-led Policy Response. Social Policy & Administration, 42: 645–661.

Gregory, R. and Mendelsohn, R. (1993), 'Perceived Risk, Dread, and Benefits', *Risk Analysis* 13/3: 259–64.

Gross, M.J. (2011), 'Stuxnet Worm: A Declaration of Cyber-War', *Vanity Fair*, April.

Jenkins, M. J. (2006), 'The new age of terrorism', in: Kamien, D (ed.), *McGraw-Hill Homeland Security Handbook* (New York: McGraw-Hill).

Libicki, M.C. (2009), *Cyberdeterrence and Cyberwar* (Santa Monica: RAND).

Maillart, T. and Sornette, D. (2010), 'Heavy-Tailed Distribution of Cyber-Risks', *The European Physical Journal* B, 75/3: 357–64.

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

Mungo, P. and Clough, B. (1993), *Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals* (New York: Random House).

Nye, J.S. Jr. and Owens, W.A. (1996), 'America's Information Edge', *Foreign Affairs*, March/April: 20–36.

Panda Security (2010), *Panda Security Report: The Cyber-crime Black Market*: Uncovered (Bilbao).

Perelman, L.J. (2007), 'Shifting Security Paradigms: Toward Resilience', in J.A. McCarthy (ed.), 'Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience', *CIP Program Discussion Paper Series* (Washington: George Mason University), 23–48.

Rattray, G. (2001), *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press).

Ross, A. (1991), 'Hacking Away at the Counterculture', in C. Penley and A. Ross (eds.), *Technoculture* (Minneapolis: University of Minnesota Press), 107–34.

Scherlis, W.L., Squires, S.L. and Pethia, R.D. (1990), 'Computer Emergency Response,' in P. Denning (ed.), *Computers Under Attack: Intruders, Worms, and Viruses* (Reading: Addison-Wesley), 495–504.

Sommer, P. and Brown, I. (2011), *Reducing Systemic Cyber Security Risk*, Report of the International Futures Project, IFP/WKP/FGS(2011)3 (Paris: OECD).

Spafford, E.H. (1989), 'The Internet Worm: Crisis and Aftermath', *Communications of the ACM*, 32/6: 678–87.

Symantec (2010), Internet Security Threat Report, Vol. 16 (Mountain View).

Verizon (2010), 2010 Data Breach Investigations Report: A Study Conducted by the Verizon RISK Team in cooperation with the United States Secret Service (New York).