Center for Security Studies

STRATEGIC TRENDS 2012

Key Developments in Global Affairs

Editor: Daniel Möckli

Series Editor: Andreas Wenger

Authors: Myriam Dunn Cavelty, Jonas Grätz, An Jacobs, Prem Mahadevan, Daniel Möckli

CSS
ETH Zurich

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

STRATEGIC TRENDS 2012 is also available electronically on the Strategic Trends Analysis website at: www.sta.ethz.ch

Editor STRATEGIC TRENDS 2012: Daniel Möckli

Series Editor STRATEGIC TRENDS: Andreas Wenger

Contact:
Center for Security Studies
ETH Zurich
Haldeneggsteig 4, IFW
CH-8092 Zurich
Switzerland

This publication covers events up to 12 March 2012.

ISSN 1664-0667
ISBN 978-3-905696-36-3

CHAPTER 5

The militarisation of cyber security as a source of global tension

Myriam Dunn Cavelty

Cyber security is seen as one of the most pressing national security issues of our time. Due to sophisticated and highly publicised cyber attacks such as Stuxnet, it is increasingly framed as a strategic issue. The diffuse nature of the threat, coupled with a heightened sense of vulnerability, has brought about a growing militarisation of cyber security. This has resulted in too much attention on the low probability of a large scale cyber attack, a focus on the wrong policy solutions, and a detrimental atmosphere of insecurity and tension in the international system. Though cyber operations will be a significant component of future conflicts, the role of the military in cyber security will be limited and needs to be carefully defined.

Emblem of the United States Cyber Command, an armed forces command that became fully operational in 2011 and is subordinate to the United States Strategic Command

Over the last few years, cyber security has been catapulted from the confined realm of technical experts into the political limelight. The discovery of the industry-sabotaging Stuxnet computer worm, numerous tales of (Chinese) cyber espionage, the growing sophistication of cyber criminals, and the well-publicised activities of hacker collectives have combined to give the impression that cyber attacks are becoming more frequent, more organised, more costly, and altogether more dangerous. As a result, a growing number of countries consider cyber security to be one of the top security issues of the future.

This is just the latest 'surge' of attention in the three- to four-decade-long history of cyber issues. The importance attached to cyber security in politics grew steadily in response to a continual parade of incidents such as computer viruses, data theft, and other penetrations of networked computer systems, which, combined with heightening media attention, created the feeling that the level of cyber insecurity was on the rise. As a result, the debate spread 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 the top of the threat list of more and more countries.

The debate on 'cyber security' originated in the US in the 1970s, built momentum in the late 1980s, and spread to other countries in the late 1990s. Early on, US policy-makers politicised the issue. They presented cyber security as a matter that requires the attention of state actors because it cannot be solved by market forces. As concern increased, they securitised the issue: They represented it as a challenge requiring the urgent attention of the national security apparatus. In 2010, against the background of the Stuxnet incident, the tone and intensity of the debate changed even further: The latest trend is to frame cyber security as a strategic-military issue and to focus on countermeasures such as cyber offence and defence, or cyber deterrence.

Though this trend can easily be understood when considering the political (and psychological) effects of Stuxnet, it nonetheless 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. Not only does this create an unnecessary atmosphere of insecurity and tension in the international system, it is also based on a severe misperception of the nature and level of cyber risk and on the feasibility of different protection

measures. 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 reactions with excessively high costs and uncertain benefits.

This chapter first describes the core elements of the cyber security debate that emerged over the past decades. These elements provide the stage and scenery for the more recent trend of increasing militarisation of cyber security. Five factors responsible for this trend are described in section two. The effects of the discovery of Stuxnet as the culmination point of the cyber threat story are the focus of section three: Though the actual (physical) damage of Stuxnet remains limited, it had very real and irreversible political effects. The fourth section critically assesses the assumptions underlying the trend of militarisation and their negative effects. 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 and the nature of the threat. Finally, it sketches the specific, though limited role that military apparatuses can and should play in reducing the overall level of cyber insecurity nationally and internationally.

The backdrop of the cyber security debate

The combination of telecommunications with computers in the late 1970s and the 1980s – the basis of the current information revolution – marks the beginning of the cyber threat debate. The launch and subsequent spread of the personal computer created a rise in tech-savvy individuals, some of whom started to use the novel networked environment for various sorts of misdeeds. In the 1990s, the information domain became a force-multiplier by combining the risks to cyberspace (widespread vulnerabilities in the information infrastructure) with the possibility of risks through cyberspace (actors exploiting these vulnerabilities). The two core elements of the cyber security debate that provide the stable backdrop for the current trend of militarisation emerged: A main focus on highly vulnerable critical infrastructures as 'referent object' (that which is seen in need of protection) and the threat representation based on the inherent insecurity of the information infrastructure and the way it could be manipulated by technologically skilful individuals.

From government networks to critical infrastructures

Initially, the overarching concern of the US was with the classified information residing in government

information systems. As computer networks grew and spread into more and more aspects of everyday life, this focus changed. A link was established in the strategic community between cyber threats and so-called 'critical infrastructures', which is the name given to assets whose incapacitation or destruction could have a debilitating impact on the national security and/or economic and social welfare of the entire nation.

This threat perception was influenced by the larger strategic context that emerged for the US after the Cold War. It was characterised by more dynamic geostrategic conditions, more numerous areas and issues of concern, and smaller, more agile, and more diverse adversaries. As a result of the difficulties to locate and identify enemies, the focus of security policies partly shifted away from actors, capabilities, and motivations to general vulnerabilities of the entire society. In addition, the influence of globalisation on the complex interdependence of societies around the world and their growing technological sophistication led to a focus on security problems of a transnational and/or technological nature. The combination of vulnerabilities, technology, and transnational issues brought critical infrastructures to centre stage, particularly because they were becoming increasingly dependent on the smooth functioning of all sorts of computer-related applications, such as software-based control systems.

The basic nature of the cyber threat

The networked information environment – or cyberspace – is pervasively insecure, because it was never built with security in mind. The dynamic globalisation of information services in connection with technological innovation led to a steady increase of connectivity and complexity. The more complex an IT system is, the more problems it contains and the harder it is to control or manage its security. The commercialisation of the Internet led to an even further security deficit, as there are significant market-driven obstacles to IT security.

These increasingly complex and global information networks seemed to make it much easier to attack the US asymmetrically: Potentially devastating attacks now only required a computer with an Internet connection and a handful of 'hackers', members of a distinct social group (or subculture) who are particularly skilled programmers or technical experts. In the borderless environment of cyberspace, hackers can exploit computer insecurities in various ways. In particular, digitally stored information can be delayed, disrupted, corrupted, destroyed, stolen, or modified.

Intruders can also leave 'backdoors' to come back at a later time, or use the hijacked machine for attacks on other machines. Though most individuals would be expected to lack the motivation to cause violence or severe economic or social harm, large sums of money might sway them to place their specialised knowledge at the disposal of actors with hostile intent like terrorists or foreign states. In addition, attackers have little to fear in terms of retribution. Sophisticated cyber attacks cannot be attributed to a particular perpetrator, particularly not within a short timespan. The main reasons are the often hidden nature of exploits and the general architecture of cyberspace, which allows online identities to be hidden.

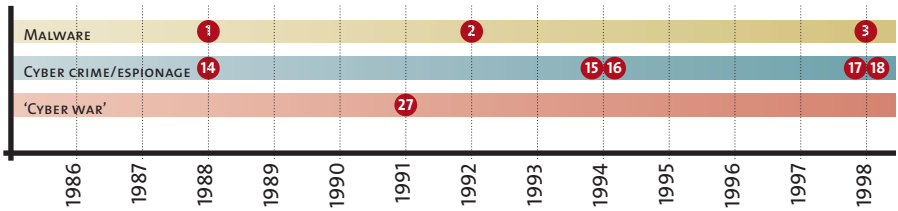
Five developments that speed up militarisation

The basics as described above provided a stable setting for the cyber security debate at least since the mid-1990s, if not before. Five developments as described below have solidified the impression that cyber disturbances are increasingly dangerous and fall under the purview of national security. The discovery of Stuxnet is the culmination point in this evolution. It has brought about a qualitative and irreversible change in how the issue is handled politically: Its discovery has catapulted the cyber issue from the expert level to the diplomatic and foreign policy realm.

First, computer security professionals are increasingly concerned with the rising level of professionalisation coupled with the obvious criminal (or even strategic) intent behind attacks. Tech-savvy individuals (often juveniles) aiming to create mischief or personally enrich themselves shaped the early history of computer-related crime. Today, professionals dominate the field. Actors in the 'cyber crime black market' are highly organised in terms of their strategic and operational vision, logistics, and deployment. Like many legitimate companies, they operate across the globe. As a consequence, the nature of malware has changed. Advanced malware is targeted: A hacker picks a victim, examines the defences, and then designs specific malware to get around them. The most prominent example for this kind of malware is Stuxnet (see below).

Second, the main cyber 'enemy' in the form of a state 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 cyberspace a strategic

Timeline: Major known cyber incidents

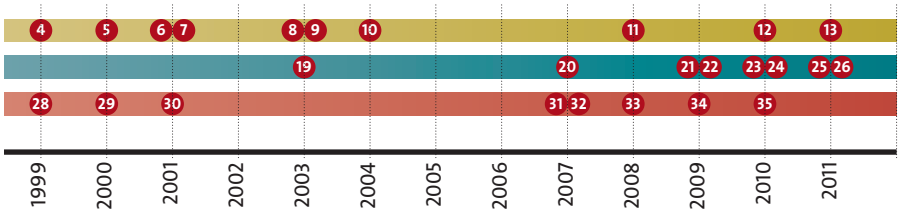


Malware

1	**Morris Worm:** Slowed down machines in the Cyber ARPANET until they became unusable. Huge impact on the general awareness of insecurity.
2	**Michelangelo:** Overwrote the first hundred sectors of the hard disk with nulls. Caused first digital mass hysteria.
3	**Back Orifice:** Tool for remote system administration (Trojan horse).
4	**Melissa:** Shut down Internet mail, clogged systems with infected e-mails.
5	**I Love You:** Overwrote files with copy of itself, sent itself to the first fifty people in the Windows Address Book.
6	**Code Red:** Defaced websites, used machines for DDoS-attacks.
7	**Nimda:** Allowed external control over infected computers.
8	**Blaster:** DDos-attacks against 'windowsupdate.com'. System crash as a side effect. Was suspected to have caused black-out in US (could not be confirmed).
9	**Slammer:** DDoS-attacks, slowed down Internet traffic worldwide.
10	**Sasser:** Internet traffic slow down, system crash.
11	**Conficker:** Forms botnets.
12	**Stuxnet:** Spies on and subverts industrial systems (see also incident 35).
13	**Duqu:** Looks for information useful in attacking industrial control systems. Code almost identical to Stuxnet (copy-cat software).

Cyber crime/espionage

14	**Hanover Hackers (Cuckoo's Egg):** Break-ins into high-profile computer systems in the US.
15	**Rome Lab incident:** Break-ins into high-profile computer systems in the US.
16	**Citibank incident:** US$ 10 m siphoned from Citibank and transferred the money to bank accounts around the world.
17	**Solar Sunrise:** Series of attacks on DoD computer networks.
18	**Moonlight Maze:** Pattern of probing of high-profile computer systems.
19	**Titan Rain:** Access to high-profile computer systems in the US.
20	**Zeus Botnet:** Trojan horse 'Zeus', controlled millions of machines in 196 countries.



21 **GhostNet:** Cyber-spying operation, infiltration of high-value political, economic, and media locations in 103 countries.

22 **Operation Aurora:** Attacks against Google and other companies to gain access to and potentially modify source code repositories at these high-tech, security, and defence contractor companies.

23 **Wikileaks Cablegate:** 251,287 leaked confidential diplomatic cables from 274 US embassies around the world, dated from 28 December 1966 to 28 February 2010.

24 **Operations Payback and Avenge Assange:** Coordinated, decentralised attacks on opponents of Internet piracy and companies with perceived anti-WikiLeaks behaviour.

25 **Sony and other attacks:** Highly publicised hacktivist operations.

26 **Theft of Co_2-Emmission Papers:** Theft of 475,000 carbon dioxide emissions allowances worth € 6.9 m, or US$ 9.3 m.

Main incidents dubbed as 'cyber war'

27 **Dutch hacker incident:** Intrusions into Pentagon computers during Gulf War. Access to unclassified, sensitive information.

28 **Operation 'Allied Force':** 'The first Internet War'. Sustained use of the full-spectrum of information warfare components in combat. Numerous hacktivism incidents.

29 **'Cyber-Intifada':** Email flooding and Denial-of-Service (DoS) attacks against government and partisan websites during the second Intifada.

30 **'Cyber World-War I':** Defacement of Chinese and US websites and waves of DDoS-attacks after US reconnaissance and surveillance plane was forced to land on Chinese territory.

31 **Iraq:** Cyber-attack on cell phones, computers, and other communication devices that terrorists were using to plan and carry out roadside bombs.

32 **Estonia DDoS-attacks:** DDoS-attacks against web sites of the Estonian parliament, banks, ministries, newspapers, and broadcasters.

33 **Georgia DDoS-attacks:** DDoS-attacks against numerous Georgian websites.

34 **GhostNet infiltrations:** GhostNet related infiltrations of computers belonging to Tibetan exile groups.

35 **Stuxnet:** Computer worm that might have been deliberately released to slow down Iranian nuclear program.

domain and that they hope that mastering it will equalise the existing military imbalance between China and the US more quickly (see Chapter 1 in this publication), many US officials readily accuse the Chinese government of perpetrating deliberate and targeted attacks or intelligence-gathering operations. However, because of the attribution problem, these allegations almost exclusively rely on anecdotal and circumstantial evidence. Not only can attackers hide, it is also impossible to know an attacker's motivation or to know a person's affiliation or sponsorship, even if the individuals were known. Therefore, 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 attribution challenge also conveniently allows state actors to distance themselves officially from attacks.

Third, there has been an increase in 'hacktivism' – a portmanteau word that combines 'hacking' and 'activism'. WikiLeaks, for example, has added yet another twist to the cyber debate. Acting under the hacker maxim that 'all information should be free', this type of activism deliberately challenges the self-proclaimed power of states to keep information considered vital for national security secret. Hacker collectives such as Anonymous or LulzSec engage in related activities of a multifaceted nature. They creatively play with anonymity in an age obsessed with control and surveillance and humiliate high-visibility targets by so-called DDoS attacks, which saturate the target machine with external communications requests so that it cannot respond to legitimate traffic, or by break-ins and release of sensitive information. These events are perceived as pressing cyber security issues in government because data is stolen in digital form and/or made available to the whole world through multiple Internet sites. In addition, media attention has been and will likely remain great; the reputational damage has been high. The more obsessed governments become with cyber security, the more embarrassing it is when they become the public target of break-ins.

Fourth, the term 'cyber war' is used more and more frequently in the media but also in policy circles. Originally, the term was coined together with its twin concept 'netwar' in the early 1990s to signify a set of new operational techniques and a new mode of warfare in the information age. Both have since become part of official (US) military information operations doctrine in modified form. But 'cyber war' also leads a colourful life outside the military discourse: The popular

usage of the word has come to refer to basically any phenomenon involving a deliberate disruptive or destructive use of computers, which has prompted US President Barack Obama's cyber security czar Howard Schmidt to repeatedly call it a 'terrible metaphor'. For example, the media proclaimed the first cyber World War in 2001. The cause was an incident in which a US reconnaissance and surveillance plane was forced to land on Chinese territory after a mid-air collision with a Chinese jet fighter. Soon after, defacements of Chinese and US websites and waves of DDoS attacks began. Individuals from many other nations joined in on both sides. The US government and military stated that they had sharply stepped up network security. Other sources reported that the Navy was at INFOCON ALPHA, a cyber version of real-world military Defense Readiness Level (DEFCON). Beyond the hype factor, the true effect of these online activities is close to zero.

Another, even more prominent example is the case of the Estonian 'cyber war'. When the Estonian authorities removed a bronze statue of a World War II-era Soviet soldier from a park, a three-plus-week wave of DDoS attacks started. It downed various websites, among them the websites of the Estonian parliament, banks, ministries, newspapers, and broadcasters. Even though it was not possible to provide sufficient evidence for who was behind the attacks, various officials readily and publicly blamed the Russian government. Also, despite the fact that the attacks had no truly serious consequences for Estonia other than (minor) economic losses, some officials even openly toyed with the idea of a counter-attack in the spirit of Article 5 of the North Atlantic Treaty, which states that 'an armed attack' against one or more NATO countries 'shall be considered an attack against them all'. The Estonian example is one of the cases most often referred to in government circles to prove that there is a need for action and the age of 'cyber war' has begun. Similar claims were made in the confrontation between Russia and Georgia of 2008.

Fifth, the discovery of the computer worm Stuxnet in 2010 changed the overall tone and intensity of the debate even further. 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 from which to launch further attacks. 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 per cent of the infected computers worldwide were in Iran. It was also reported that the Iranian nuclear programme had been delayed as some centrifuges had been damaged.

The picture that emerges from the pieces of the puzzle seems to suggest that only one or several nation states – the *cui bono* ('to whose benefit') 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 programme. However, the one big problem with the Stuxnet story is, once again, that it is entirely based on speculation: The evidence for Stuxnet being a government-sponsored cyber weapon directed at Iran, though convincing and plausible, is entirely circumstantial. Due to the attribution problem, it is impossible to know who gave the order, who actually programmed Stuxnet, and the real intent behind it. Rather than making the problem less serious, however, this fact is at the heart of current fears. The cyber domain has emerged as a realm in which states see their control and power challenged from all sides, but in which they are forced to position themselves as forcefully as possible, too.

Unravelling the Stuxnet effect

Whatever the 'truth' may be: The Stuxnet incident is a manifestation of longstanding fears. It is a targeted attack affecting the control system of a super-critical infrastructure, invisible and untraceable until it hits. Since so little about the worm is known for certain, however, the actual effects in form of damage are impossible to uncover, as is shown in the first subsection below. Other effects, though also partially speculative, have manifested themselves more clearly. One of these fears, covered in the second subsection, is the fear of proliferation and copycat attacks. Another more salient one is psychological and has real political consequences: Many security experts and decision-makers do believe that one or several state actors created the computer worm. For those people, the digital first strike has been delivered, and this marks the beginning of the unchecked use of cyber weapons in military-like aggressions. Cyber security now clearly comes under the purview of diplomats, foreign policy analysts, the intelligence community, and the military. These reactions and their severe consequences

for international relations and security are the focus of the third subsection.

Damage/cost

Putting a number to the cost of any specific malware is a very tricky thing. Attempts to collect significant data or combine them into statistics have failed due to insurmountable difficulties in establishing what to measure and how to measure it. Numbers that are floating around are usually more or less educated 'guesstimates', calculated by somehow adding downtime of machines and the cost for making them malware-free. The same problem applies to Stuxnet. Shortly after the worm was discovered, Symantec estimated that between 15,000 and 20,000 systems were infected. These numbers increased the longer the worm was known. Siemens on the other hand reported that the worm had infected 15 plants with their SCADA software installed, both in and out of Iran. In the end, Symantec set both the damage and the distribution level of the malware to medium.

Stuxnet is a manifestation of longstanding fears

In the mainstream representation of the Stuxnet story, the Bushehr nuclear plant is the intended target of the attack. Indeed, the operational start of Bushehr was delayed by several months: Iranian officials blamed the hot weather and later a leak for it. Officially, Tehran at first denied the worm infected critical systems at the Bushehr plant, but later said that Stuxnet had affected a limited number of centrifuges. There also seemed to have been some problems at Natanz: A decline in the number of operating centrifuges from mid-2009 to mid-2010 may have been due to the Stuxnet attack, some experts speculate. All in all, knowing the extent of the effect Stuxnet had on the Iranian nuclear programme is impossible; it seems plausible, however, that is has delayed it, though only for a short amount of time. The psychological effect on the Iranian government, though also not easily fathomable, is likely to have been very high.

Proliferation effect

The discovery of Stuxnet and subsequent rumours that its source code was for sale led some experts to fear a rapid proliferation of this type of programming and many so-called piggyback attacks. This would make SCADA systems – computer systems that monitor and control industrial, infrastructure, or facility-based processes – the target of choice in the near to mid-term future for all types of hacks, with potentially grave consequences, also due to unintended side effects. Other analysts have described these fears as groundless, because even if somebody had acquired the source code, they would have to be just as

capable as the initial programmers for the variant to be as successful. Once a piece of malware has been discovered, even if it is a sophisticated specimen, merely copying it will be of little use if the computer vulnerability it exploited has been patched in the meantime.

So far, no proliferation effect has materialised; however, in September 2011, another worm (Duqu) was discovered that is reportedly very similar to Stuxnet, and was probably written by the same authors. It mainly looks for information that could be useful in attacking industrial control systems and does not sabotage any parts of the infrastructure.

Political and psychological effect

The greatest effect the worm has had is clearly psychological: It has left many state officials deeply frightened. This fear has political consequences. First, on the national level, governments are currently releasing or updating cyber security strategies and are setting up new organisational units for cyber defence. Second, internationally, increased attention is being devoted to the strategic-military aspects of the problem. The focus is on attacks that could cause catastrophic incidents involving critical infrastructures. More and more states report that they have opened 'cyber-commands', which are military units for cyber war activities. Though consolidated numbers are hard to come by, the amount of money spent on defence-related aspects of cyber security seems to be rising steadily. The new cyber military-industrial complex that has emerged is estimated to deliver returns of US$ 80 to 150 billion a year, and big defence companies like Boeing and Northrop Grumman are repositioning themselves to service the cyber security market. In addition, some states, particularly those not allied with the US, have ramped up their rhetoric. For example, Iranian officials have gone on the record as condoning hackers who work in the state's interest. As a result, 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. That leads to more insecurity for everyone – specifically because it is impossible to assess another state's cyber capabilities.

Flawed assumptions and detrimental effects

The militarisation of cyber security is first and foremost based on the belief in a massive threat of a large-scale cyber attack. There are two aspects to this perception: In the first subsection, it is shown how and why the past and current level of the threat is overrated. The second subsection places the

future likelihood of cyber war into perspective. It shows that now and in the future, the probability of a large-scale attack is very low. The third subsection looks at an additional reason for how widespread the fear of cyber war has become: Most countries simply follow the threat perception and reasoning of the US, even though the strategic context and disparity in power positions warrant a different threat assessment. The fourth subsection finally criticises the widespread use of vocabulary that is full of military analogies. Such vocabulary insinuates a reality governed by the traditional logic of offense and defence – a reality that does not exist. Even worse, it is decoupled from the reality of the threat and the possibility for meaningful countermeasures and is complicit in solidifying the militarisation of cyber security.

An overrated threat

There is no denying that different political, economic, and military conflicts have had cyber(ed) components for a number of years now. Furthermore, criminal and espionage activities involving the use of computers happen every day. It is a fact that cyber incidents are continually causing minor and only occasionally major inconveniences: These may be 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 and have, theoretically at least, the potential to reduce public confidence in the security of Internet transactions and e-commerce if they become more frequent.

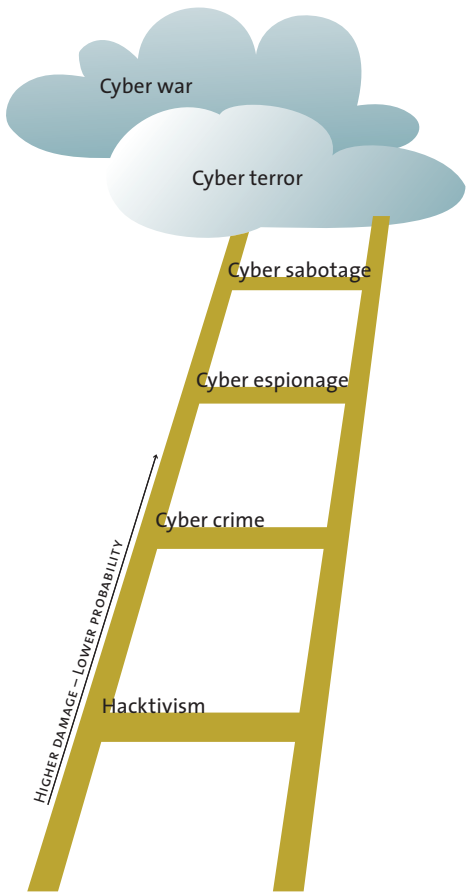
However, in the entire history of computer networks, there are no examples of cyber attacks that resulted in actual physical violence against persons (nobody has ever died from a cyber incident), and only very few had a substantial effect on property (Stuxnet being the most prominent). So far, cyber attacks have not 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 such as financial risks.

These facts tend to be almost completely disregarded in policy circles. There are several reasons why the threat is overrated. First, as combating cyber threats has become a highly politicised issue, official statements about the level of threat must also be seen in the context of competition for resources and influence between various bureaucratic entities. This is usually done by stating an urgent need

for action and describing the overall threat as big and rising.

Second, psychological research has shown that risk perception, including the perception of experts, is highly dependent on intuition and emotions. Cyber risks, especially in their more extreme form, fit the risk profile of so-called 'dread risks', which are perceived as 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 the willingness to bear high costs of uncertain benefit.

Types of cyber conflict



Cyber war: The use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems. The term is also used loosely for cyber incidents of a political nature.

Cyber terror: 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'. The term is also used loosely for cyber incidents of a political nature.

Cyber sabotage: The deliberate disturbance of an economic or military process for achieving a particular (often political) goal with cyber means.

Cyber espionage: The unauthorised probing to test a target computer's configuration or evaluate its system defenses, or the unauthorised viewing and copying of data files.

Cyber crime: A criminal activity done using computers and the Internet.

Hacktivism: The combination of hacking and activism, including operations that use hacking techniques against a target's Internet site with the intention of disrupting normal operations.

Third, the media distorts the threat perception even further. There is no hard data for the assumption that the level of cyber risks is actually rising – beyond the perception of impact and fear. Some IT security companies have recently warned against overemphasising sophisticated attacks just because we hear more about them. In 2010, only about 3 per cent of all incidents 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. These types of incidents tend to remain under the radar of the media and even law enforcement.

Cyber war remains unlikely

Since the potentially devastating effects of cyber attacks are so scary, the temptation is very high not only to think about worst-case scenarios, but also to give them a lot of (often too much) weight despite their very low probability. However, most experts agree that strategic cyber war remains highly unlikely in the foreseeable future, mainly due to 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. Indeed, it is hard to see how cyber attacks could ever become truly effective for military purposes: It is exceptionally difficult to take down multiple, specific targets and keep them down over time. The key difficulty is proper reconnaissance and targeting, as well as the need to deal with a variety of diverse systems and be ready for countermoves from your adversary.

Furthermore, nobody can be truly interested in allowing the unfettered proliferation and use of cyber war tools, least of all the countries with the offensive lead in this domain. Quite to the contrary, strong arguments can be made that the world's big powers have an overall strategic interest in developing and accepting internationally agreed norms on cyber war, and in creating agreements that might pertain to the development, distribution, and deployment of cyber weapons or to their use (though the effectiveness of such norms must remain doubtful). 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 information infrastructure. 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 could 'blow back' through the interdependencies that are such an essential feature of the environment. Even relatively harmless viruses and worms would cause considerable random disruption to businesses, governments, and consumers. This risk would most likely weigh much heavier than the uncertain benefits to be gained from cyber war activities.

Certainly, thinking about (and planning for) worst-case scenarios is a legitimate task of the national security apparatus. Also, it seems almost inevitable that until cyber war is proven to be ineffective or forbidden, states and non-state actors who have the ability to develop cyber weapons will try to do so, because they appear cost-effective, more stealthy, and less risky than other forms of armed conflict. However, cyber war should not 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.

Cyber crime and cyber espionage will remain the biggest cyber risks

Europe is not the US

The cyber security discourse is American in origin and American in the making: At all times, the US government shaped both the threat perception and the envisaged countermeasures. Interestingly enough, there are almost no variations to be found in other countries' cyber threat discussions – even though the strategic contexts differ fundamentally. Many of the assumptions at the heart of the cyber security debate are shaped by the fears of a military and political superpower. The US eyes the cyber capabilities of its traditional rivals, the rising power of China and the declining power of Russia, with particular suspicion. This follows a conventional strategic logic: The main question is whether the cyber dimension could suddenly tip the scales of power against the US or have a negative effect on its ability to project power anywhere and anytime. In addition, due to its exposure in world politics and its military engagements, the US is a prime target for asymmetric attack.

The surely 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 will be

exploited – particularly not for the majority of states in Europe. The existence of the cyber realm seems to lead people to assume that because they have vulnerabilities, they will be exploited. But in security and defence matters, careful threat assessments need to be made. Such assessments require that the following question be carefully deliberated: 'Who has an interest in attacking us and the capability to do so, and why would they?' For many democratic states, particularly in Europe, the risk of outright war has moved far to the background and the tasks of their armies have been adapted to this. Fears of asymmetric attacks also rank low. The same logic applies to the cyber domain. The risk of a warlike cyber attack of severe proportions is minimal; there is no plausible scenario for it. Cyber crime and cyber espionage, both political and economic, are a different story: They are here now and will remain the biggest cyber risks in the future.

The limits of analogies

Even if the cyber threat were to be considered very high, the current trend conjures up wrong images. Analogies are very useful for relating non-familiar concepts or complex ideas with more simple and familiar ones. But when taken too far, or even taken for real, they begin to have detrimental effects. Military terms like 'cyber weapons', 'cyber capabilities', 'cyber offence', 'cyber defence', and 'cyber deterrence' suggest that cyberspace can and should be handled as an operational domain of warfare like land, sea, air, and outer space (cyberspace has in fact been officially recognised as a new domain in US military doctrine). Again, this assumption clashes with the reality of the threat and the possibilities for countermeasures.

First, calling offensive measures cyber weapons does not change the fact that hacker tools are not really like physical weapons. They are opportunistic and aimed at outsmarting the technical defences. As a result, their effect is usually not controllable in a military sense – they might deliver something useful or they might not. Also, even though code can be copied, the knowledge and preparation behind it cannot be easily proliferated. Each new weapon needs to be tailored to the system it is supposed to attack. Cyber weapons cannot be kept in a 'silo' for a long time, because at any time, the vulnerability in the system that it is targeted at could be patched and the weapon would be rendered useless.

Second, thinking in terms of attacks and defence creates a wrong image of immediacy of cause and effect. However, high-level cyber attacks against infrastructure targets will 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, with highly uncertain results. The military notion of striking back is therefore useless in most cases.

Third, deterrence works if 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 the other side if the latter 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 cyber security because of the attribution problem. Attribution of blame on the basis of the *cui bono* logic is not sufficient proof for political action. Therefore, deterrence and retribution do not work in cyberspace and will not, unless its rules are changed in substantial ways, with highly uncertain benefits. Much of what is said in China and in the US about

Types of cyber malware and attack modes

Malware: A collective term for all types of malicious code and software

Exploit	Taking advantage of computer vulnerability to cause unintended or unanticipated behaviour. This includes gaining control of a computer system.
Virus/worm	Computer programmes that replicate functional copies of themselves with varying effects ranging from mere annoyance and inconvenience to compromise of the confidentiality or integrity of information. Viruses need to attach themselves to an existing program, worms do not.
Spyware	Malware that collects information about users without their knowledge.
Trojan horse	Malicious program that acts in an automatic manner. Trojan horses can make copies of themselves, steal information, or harm their host computer systems, or allow a hacker remote access to a target computer system.
DDoS-attack	Attempt to make a computer or network resource unavailable to its intended users, mostly by saturating 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.
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.
Botnets (or bots)	A collection of compromised computers connected to the Internet. They run hidden and can be exploited for further use by the person controlling them remotely.

their own and the other's cyber capabilities is (old) deterrence rhetoric – and must be understood as such. The White House's new International Strategy for Cyberspace of 2011 states that the US reserves the right to retaliate to hostile acts in cyberspace with military force. This 'hack us and we might bomb you' statement is an old-fashioned declaratory policy that preserves the option of asymmetrical response as a means of deterrence, even though both sides actually know that following up on it is next to impossible.

Fourth, 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 impossible, and conceiving of cyberspace as an occupation zone is an illusion. Militaries cannot defend the cyberspace of their country – it is not a space where troops and tanks can be deployed, because the logic of national boundaries does not apply.

The role of the military in cyber security

Future conflicts between nations will most certainly have a cyberspace component, but this will just be an accompanying element of the battle. 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 and the nature of the attacked. Investing too much time talking about them or spending increasing amounts of money on them will not make cyberspace more secure – quite the contrary. These findings are not particularly new: Most experts had come to the same conclusion in the late 1990s, when the debate was not yet as securitised. At the time, the issue was discussed under the heading of critical infrastructure protection rather than cyber security, but the basic premises were the same. The role for the military as conceptualised then hardly differs from the role the military should take on today.

Undoubtedly, 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. All the successful attacks on military and military-affiliated networks over the last few years are less a sign of impending cyber-doom than a sign of low information security prowess in the military. In case the unfortunate label 'cyber defence' should stick, it will be crucial to make sure that everybody – including top-level decision-makers – understand that cyber defence is not much more than a fancy word for standard information assurance and risk management practices. Furthermore, information assurance is not provided by obscure 'cyber commands', but by computer security specialists, whether they wear uniforms or not.

The cyber dimension is also relevant in military operations insofar as an adversary's critical infrastructure is deemed to be a major centre of gravity, i.e., a source of strength and power that needs to be weakened in order to prevail. However, intelligence-gathering by means of cyber espionage must be treated with utmost care: In an atmosphere fraught with tension, such activities, even if or especially because they are non-attributable, will be read as signs of aggression and will add further twists to the spiral of insecurity, with detrimental effects for everybody. The implication of this is that military staff involved in operative and military strategic planning and the intelligence community will have to be aware of cyber issues too. However, in the future, decisive strikes against critical (information) infrastructure will most likely still consist of kinetic attacks or traditional forms of sabotage rather than the intrusion of computer systems.

Recent national strategies for cyber security

United States	Department of Defense, 'Strategy for Operating in Cyberspace' (2011)
	The White House, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World' (2011)
	Department of Homeland Security, 'Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise' (2011)
UK	'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World' (2011)
France	Premier ministre, 'Défense et sécurité des systèmes d'information: Stratégie de la France' (2011)
Germany	Federal Ministry of the Interior, 'Cyber Security Strategy for Germany' (2011)
The Netherlands	'The National Cyber Security Strategy (NCSS): Success through cooperation' (2011)
India	Department of Information Technology, 'Cyber Security Strategy' (2011)

As for the things the military should not do when it comes to the realm of cyberspace, two major points come to mind. First, particularly as long as the ability to withstand cyber intrusions of military networks or civilian networks remains low, it is unwise to declare the development or possession of offensive measures. It does not have a credible deterring effect, the actual use would bring unclear benefits and high risks, and again, it adds to the cyber security dilemma.

Second, the military cannot take on a substantial role in ensuring the cyber security of a whole country. Due to privatisation and deregulation of many parts of the public sector in most of the developed world, between 85 and 95 per cent of the critical infrastructure are owned and operated by the private sector. Given that overly intrusive market interventions are not deemed a valid option, states have but one option: to try to get the private sector to help in the task of protecting these assets. What emerged from this in the late 1990s already was a focus on critical infrastructure protection, with one particularly strong pillar: public-private partnerships. A large number of them were (and still are) geared towards facilitating information exchange between companies themselves, but also between companies and government entities, which are usually *not* part of the military or intelligence establishment. This is complemented by measures taken to ensure that the damage potential of a successful attack is constantly decreasing, for example by augmenting the resilience of information networks and critical infrastructures.

In conclusion, governments and military actors should acknowledge that their role in cyber security can only be a limited one, even if they consider cyber threats 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 best to encourage market forces to improve the security and resilience of company-owned networks. Threat-representation must remain well informed and well balanced in order to prevent overreactions. 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 or trying to solve the attribution problem will have detrimental effects on the way humankind uses the Internet; and the overall cost of these measures will most likely outweigh

the benefits. What is most needed in the current debate is a move away from fear-based doomsday thinking and a move towards more level-headed threat assessments that take into account the strategic context.