Ralf Bendrath

The Cyberwar Debate
Perception and Politics in U.S. Critical Infrastructure Protection

Published in: *Information & Security: An International Journal*, Vol. 7 (2001): The Internet and the Changing Face of International Relations and Security (ed. by Andreas Wenger), 80-103.

1. The Information Society as Risk Society

"Cyberwar" has become a growth market in the U.S. While ten years ago only a few experts could make sense of this term, attacks on computernetworks and their implications for national security are now a big theme in the mass media. In the broad range of service providers from technical security solutions to policy advisory groups a whole cottage industry has sprung up. Warnings of an "electronic pearl harbor" or a "cyberwar" against the United States' infrastructures by "rogue states" or terrorists are part of the standard repertoire in security policy analyses. Bill Clinton started the process of developing a strategy with his Presidential Commission on Critical Infrastructure Protection in 1996, and the new U.S. government under George W. Bush as well is trying to address the problem.[1]

As with nuclear energy production, the dangers rising from the digital networking of everything and everybody are not easy to see for a non-expert. To detect a virus on your hard drive, you need a virus scanner as a sensoric tool; to find out if there is a cracker in your network, you need an intrusion detection system or a good sysadmin with spare time. For the average user an intentional hacker attack can not be distinguished from a technical failure, like a hardware defect, a software malfunction or a "normal" system crash. In the case of denial-of-service it is not obvious at all if the computer that is not providing its service anymore has just crashed, if the cable connecting it to the internet was physically damaged, or if it is the victim of a targeted flood with packets and requests.

The so called "information society" is thus showing significant signs of a "risk society". The new risks, according to Ulrick Beck, who coined the term in the eighties, can not be perceived immediately anymore, and therefore they are especially open to political interpretation and instrumentation. "It never is clear if the risks have become worse or our look at them just has sharpened."[2] This especially is true for the infrastructural insecurites.

The U.S. National Academy of Sciences as early as 1990 begun a report on computer security with these words: "We are at risk. Increasingly, America depends on computers. [...] Tomorrow's terrorist may be able to do more damage with a keyboard than with a

1 For an overview see Bendrath 2001a.

2 Beck 1986: 73, translation R.B.

bomb."[3] This quote is typical for a whole series of warnings issued by the intelligence community, the FBI and other government agencies in the last ten years. They especially focused on the so called "critical infrastructures" like telecommunication, financial services, electricity and water or fuel supply. A concerted action of qualified hackers with hostile intentions, they feared, could force a whole nation to its knees. The biggest possible damage was named "electronic pearl harbor".[4]

Compared to the traditional security policy threat which consisted of the three dimensions actor, intention and capabilities, in "cyberwar" almost all confidence is lost. First, there is no clearly identifyable *actor* who could become a possible enemy. The cyber attackers can be teenagers, rogue nations, terrorists or disgruntled insiders, even private companies or political activists like the critics of globalisation. This implies secondly, that it is very hard to get verifyable information on the *hostile intentions* of the possible attacker: Does he want to attack the U.S. at all? Is he planning to use cyber attacks? This leads to the third open question: Does the possible enemy have the *capabilities* to wage a large-scale cyber attack against the U.S.? It is far from clear even in the intelligence community if strategic rivals like China or Russia already have the technology and, even more important, the knowledge and qualified personell to hack into computers that control critical infrastructures. Traditional means of intelligence do not help very much in this field, because the capabilities for an attack largely consist of software, commercial-off-the-shelf hardware components and an internet connection. In its 1997 report the President´s Commission on Critical Infrastructure Protection explicitly wrote that the possible enemies are unknown, while the tools for cyber attacks are easily available.[5]

To conclude: In the case of this new cyber risks almost everything is new. The weapons are not kinetic, but software and knowledge; the environment in which the attacks occur is not physical, but virtual; the possible attacker is unknown and is able to hide himself effectively even during an attack.

From a political science point of view this is an extremely interesting case. What does a state do when the strategic context of its security policy has changed radically? Which strategy will be applied to cope with the new insecurities - risks instead of threats? Which agency inside the government will become responsible for countering the risks? Will the security strategy be focused on retaliation, on minimising the possible damage after an attack, or will it aim at preventing an attack in the first place?

The United States were the first nation to address the problem of critical infrastructure protection seriously. The government put a lot of effort into thinking about it, and the newly founded agencies and institutions responsible for this task already have some years of experience now. A detailed review of U.S. critical infrastructure protection policy can thus help us understand the possibilities and limits of infrastructure protection in general.

The following analysis will be guided by a framework developed in a project on "international risk policy" which was conducted by the Center on Transatlantic Foreign

---

3 National Academy of Sciences, Computer Science and Telecommunications Board: Computers at Risk: Safe Computing in the Information Age, Washington D.C. 1990, quoted in: Office of the Under Secretary of Defense for Aquisition & Technology 1996: A-1.

4 For the origins of this term see Smith 2001a with many references.

5 PCCIP 1997: 14.

and Security Policy Studies at the Free University of Berlin.[6] It will look at three different sets of factors that might have an influence on the formulation of the risk policy: Risk perception, resources, and norms.

2. Factors influencing the development of the risk policy

2.1. Risk Perception

Capabilities as a Starting Point

The complexity of world society after the end of the Cold War have lead security politicians and experts to focus more on the capabilities of possible enemies than on their intentions. This is the case with nuclear proliferation or ballistic missiles as well as with the "international terrorism". The calculations of insecurity more and more rely on the technical means that might be available for possible enemies. Along these lines the new potential for cyber attacks took its place in the debate.

This change in the general perception of insecurity coincided with growing concerns in the Department of Defense over the vulnerability of the networked military. While the debate on the "Revolution in Military Affairs" (RMA) started extremely euphorically in the early nineties, whith trendy articles and studies on "network centric warfare" or the real-time information flow through the global "system of systems" for C^4ISR[7], since the mid-nineties one finds more and more warnings of the risks. Because a great deal of military communication is traveling through civilian infrastructures, the risks for civil infrastructures from hackers and other intruders were also seen as a threat for military security.[8]

This analysis did not develop by chance - it grew parallel to the development of offensive information warfare capabilities and strategies in the U.S. military (see 2.2.). As the debate on attacks against the information systems of possible enemies went further on, the eventual dangers for the U.S.' own military and civilian data networks as well became a major theme.

What makes the whole debate on the vulnerablility of electronic infrastructures typical for today's risk debates is the lack of experience. Many studies and warnings are filled with only anecdotal collections of well-known hacks, others try to estimate the risk based on simulations with "red teams". The latter can not be compared with reality very well, because the red-team-hackers were members of the attacked institution and therefore had a great deal of knowledge about system architectures or the culture of the operators. Additionally, these simulations and exercises were never held under real conditions, but on simulated systems. During the exercise "Eligible Receiver" in June 1997, which is often taken as evidence for the vulnerabilities of U.S. military data

6 Daase/Feske/Peters 2001.

7 Command, control, communication, computers, intelligence, surveillance, and reconnaissance.

8 The actual percentage is far from clear. While many sources write about 95 percent, others only name 70 percent of the "non-essential" communication.

networks, only unclassified or simulated systems were attacked.[9] Furthermore, one often finds impressing data on the *numbers* of known hacker attacks, but in almost all cases a statement on the *damage* is lacking. A serious risk calculation though would have to include an estimate of the probability of an incident *and* of the possible amount of damage.

All statements on the scope of the danger therefore are more or less speculative. Furthermore, there still are no clear criteria for deciding what is an attack and what is not. Until 1998 the Pentagon counted every attempt to establish a telnet connection (which can be compared with a knock on a closed door) as an electronic attack.[10] Until today there are no standard procedures for identifying and estimating the vulnerablilty of critical infrastructures. These are being developed since June 2000 in the Critical Infrastructure Protection Office's project "Matrix".[11]

Due to these uncertainties the risk estimates always move between paranoia and carelessness, without ever being precise. The relevant studies and analyses are therefore full of terms like "capability", "possibility" or "could".[12]

The consequent simplification of this argumentational pattern is the simple claim: "Mr. Chairman, there will be an electronic attack sometime in our future", like then Deputy Secretary of Defense John Hamre said in a Congress hearing in June 1996.[13] With this method the discourse on the cyber dangers has strongly been popularised, because many of the political recommendations from think tanks or staffers were derived from scenarios - and these are nothing else than claims about future events. From the mid-nineties on the RAND Corporation and the Defense Advanced Research Projects Agency (DARPA) ran a series of exercises based on the ‚Day After'-method. In a first step the participants were taken five years into the future and confronted with a number of cyberwar attacks. They had to react under time pressure and, for example, draft a briefing and outline recommendations for the Secretary of Defense or the President. In a second step they were taken back to the present and discussed how to avoid these events in the future by acting today.[14]

The question one completely takes out of the discourse with this method is: How plausible are the scenarios at all? The participants rather learned to deal with them as external, given realities. Looking back, many of the assumptions have proven wrong[15], but the scenarios already had established a specific fear-driven cyber mind set in the

---

9 DoD 1998.

10 McKay 1998. Richard Aldrich, Staff Judge Advocate of the Air Force Office of Special Investigations (AFOSI), in his presentation at the InfowarCon in Washington on 6 September, gave another example: When asked by the Department of Justice about the number of computer security cases in 2000, the AFOSI staff counted 14 for the whole Air Force, whereas the DoD overall count for all services summed up to some 30 000. The latter had counted non-dangerous events like unidentified pings as hacker attacks, while the AFOSI only had considered serious cases.

11 Clarke 2000.

12 The PCCIP (1998) for example wrote in its report: "We found no evidence of an impending cyber attack which could have a debilitating effect on the nation's critical infrastructures. While we see no electronic disaster around the corner, this is no basis for complacency. We did find widespread capability to exploit infrastructure vulnerabilities", p. i; "[W]e also face the possibility that someone will be able to actually mount an attack against other infrastructures by exploiting their dependence on computers and telecommunications", p. 5.

13 Hamre/Campbell 1998.

14 Anderson/Hearn 1996, Molander et al. 1996.

15 For 1999 they expected a Yen-crisis triggered by a computer virus or a "trojan" planted into the software of the Airbus A-330 by Algerian extremsists, Anderson/Hearn 1996, Appendix B.

security policy community. This is a good example of how to establish a threat-based discourse in the absent of a clear danger, where only the risk is present that there might be a threat sometime. In other words, like a member of the syndicate once said to Fox Moulder in the X-Files: The best way to predict the future is to invent it.

This lead to the establishment of the cyber risk on the political agenda. The question still left open was: How to deal with it? Or, maybe more important in the fragmented political landscape of Washington: Who should be in charge? The classical institutions responsible for national security, like the Pentagon or the intelligence agencies? The FBI with its computer crime squads? Or maybe just the private companies running the infrastructures? The answer was at least partly dependent on the specific construction of possible enemies or damages.

Military Rivals

In the Summer of 1995 the National Intelligence Council for the first time wrote a report on the information warfare capabilities of other international actors. The document is classified, but its conclusions were presented to the public. According to them, some states are building up their capabilities for waging information warfare, but mainly focus their efforts on using them in the context of a conventional military conflict. They do not plan to attack national infrastructures, but military communications networks or air defense systems. Even after searching very hard the National Intelligence Council found no evidence of so called "rogue states" developing capabilities for information warfare or recruiting foreign hackers for this task.[16]

In May 1998 President Clinton gave the intelligence community the explicit order to collect and process information about the electronic threat from other nations.[17] Today the intelligence agencies distinguish between two kinds of threats:

> "*The unstructured threat is random and relatively limited. It consists of adversaries with limited funds and organization and short-term goals. While it poses a threat to system operations, national security is not targeted. This is the most obvious threat today. The structured threat is considerably more methodical and well-supported. While the unstructured threat is the most obvious threat today,* for national security purposes we are concerned primarily with the structured threat, since that poses the most significant risk."[18]

The states most often named as possible sources of such a structured threat are China and Russia. The evidence for real capabilities in these countries, though, is thin, it mostly consists of quotations from officers' publications about the new possibilities of cyberwar or asymmetric warfare. [19] Even Timothy L. Thomas of the Pentagon's Foreign Military Studies Office, who probably knows more than any other American about the developments in China and Russia, only lists the specialised infowar units of the People's Liberation Army, but can not provide information on their capabilities. The Russian concept of information warfare, on the other hand, differs significantly from the

16 Deutch 1996.
17 White House 1998.
18 Minihan 1998, my emphasis.
19 Serabian 2000.

U.S. view, aiming more at psychological manipulations and less on comuter network attacks.[20]

Another group of actors concerning the intelligence community are international terrorists.[21] The National Infrastructure Protection Center (NIPC) for example warned of Osama bin Laden possibly planning a computerised version of the Oklahoma bombing.[22] Until today terrorists, though, have not been very active in cyberspace. All that is known is that they make use of computers, the internet or cryptography for organisational purposes.[23] "We have yet to see a significant instance of 'cyber terrorism' with widespread disruption of critical infrastructures", then FBI-director Louis Freeh had to tell the Senate in February 2000.[24] Johan Ingles-le Nobel, deputy edititing director of Jane's Intelligence Review, after extensive research and debates among hackers as well came to the conclusion: "In theory, cyberterrorism is very plausible, yet in reality it is difficult to conduct anything beyond simple 'script-kiddy' DoS attacks."[25]

What is left are the hacker attacks, in terms of the intelligence community an unstructured and limited threat which does not pose a danger to national security. So far there has been no case where hackers really damaged critical infrastructures.

Yet, this military-like discourse had much influence in Washington's security policy establishment. Then CIA director John Deutch for example since the mid-nineties regularly warned of a threat to national security from cyber attacks. Asked in a Senate hearing to compare the danger with nuclear, biological or chemical weapons, he answered, "it is very, very close to the top".[26] These dangers, according to the security policy agencies and departments, not only rose from states. Jaques Gansler, then Assistant Secretary of Defense for Aquisition and Technology, even called teenagers a "real threat environment" for national security.[27] George Smith of the Crypt Newsletter was probably right when he wrote: "Teenagers are transformed into electronic bogeymen with more power at their fingertips than the Strategic Command".[28]

A very important metaphor in this social construction of the threat was the "electronic Pearl Harbor". This term connected a historical trauma of the American society to the new risks and thus almost forced the polical elite to repsond somehow. The mass media thankfully took up the term and featured it prominently in almost every report on the issue.[29] The "electronic Pearl Harbor" had a great impact on the U.S. debate, because it both constructed an agent and a structure.

In the agent dimension it implies a danger coming from an enemy that is geographically and morally located outside of the United States. This picture of a dangerous "other" reproduces the idea of the nation as a collective self. Common

---

20 Thomas 2001.
21 Arquilla et al. 1998.
22 Smith 2001a.
23 Serabian 2000.
24 Freeh 2000.
25 Ingles-le Nobel 1999.
26 CNN 1996.
27 Madsen 1998.
28 Smith 2001a.
29 Infowar enthusiast Winn Schwartau, who coined the term more than ten years ago, recently even wrote a novel titled "Pearl Harbor.Com". It will be published on 7 December 2001.

phrases like “our computers”[30] or “our infrastructures”[31] even amplify this effect. The reference object of security then is the whole American society. The logical agent of security policy acting on behalf of it of course is the state - not the single computer user or network provider. The defense against cyber attacks, this being the logical and political implication, is a task for national security policy.

In the other dimension the “*electronic Pearl Harbor*” implicitly draws a structure for security policy. Because the image is taken from war history, it implies a strategy based on analogies to physical warfare. The terms “cyberwar” or “information warfare”, which became popular in the mid-nineties, also furthered the idea of the Pentagon being the natural defender of the nation’s infrastructures. For example, the Defense Science Board in its 1996 study proposed setting up a center for defensive information warfare at the Defense Information Systems Agency (DISA). It should be responsible for the infrastructural security of the other departments and even of the private sector.[32] Then Deputy Secretary of Defense John Hamre on several occasions made this strategy more than clear: “Cyperspace ain't for geeks, it's for warriors”.[33] In his last annual report to the Congress, President Clintons Defense Secretary William Cohen as well wrote about a role for the DoD in fighting cyber terrorism.[34] This perception is typical for the military and national security policy establishment and has not changed very much under the presidency of George W. Bush. His national security advisor, Condoleezza Rice, in March 2001 for example called cyberwar “a classic deterrence mission”.[35]

Computer Crime

The risk perception of the law enforcement agencies is structured differently. Many critics of a military involvement argued the “electronic Pearl Harbor” - should it ever happen - would take place inside the United States. Thus the agencies better suited for fighting it or hunting the attackers were the Federal Emergency Management Agency (FEMA) or the FBI. Additionally, the FBI had already been involved in investigating computer crime and had set up a special Computer Crime Squad in the early nineties. On the basis of the Computer Fraud and Abuse Act of 1986 this unit had investigated more than 200 cases until the mid-nineties and along this way learnt a great deal about the practical problems of the risk. Dealing with hacker-intrusions, data theft and similar things had led to a more differentiated, but as well less dramatic view of the risk. One point FBI officials very often make is the practical impossibility of identifying an attacker before a thorough investigation has been conducted. “The trouble is that when an attack occurs we have no way of knowing if this is a kid in middle America or a serious foreign threat,” said Michael Vatis, until March 2001 the director of the FBI’s National Infrastructure Protection Center.[36]

---

30 Then Deputy Secretary of Justice Jamie Gorelick, in: ABC Nightline 1997.

31 PCCIP 1997, passim.

32 Office of the Under Secretary of Defense for Aquisition & Technology 1996:6-7.

33 Inside the Army, 22.4.1999, quoted in Smith 2001b.

34 “DoD combats transnational threats through its activities to prevent terrorism and reduce U.S. vulnerability to terrorist acts [...]. Such activities include efforts to [...] protect critical infrastructure (including combating cyber–terrorism)”, Cohen 2000.

35 Quoted in Poulsen 2001.

36 Quoted in McKay 1998.

One key experience, afterwards called "Solar Sunrise", had a strong influence on this point of view. In February 1998, more than 500 electronic break-ins into computer systems of the US government and the private sector were detected. The hackers got access to at least 200 different computer systems of the U.S. military, the nuclear weapons laboratories, the Department of Energy and NASA. Exactly at the same time the US forces were building up troops in the Middle East because of the tensions with Iraq over the UN arms inspections. The fact that some of the intrusions could be traced back to internet service providers in the Gulf region led to the initial conclusion that the Iraq government must be behind the attacks. A closer investigation of the case later brought up the real attackers: Two teenagers from Cloverdale in California and another teen from Israel. The law enforcement agencies took this as one more proof that one can not respond militarily to a cyber attack as long as the attacker is not clearly identified. Then FBI director Louis Free told the Senate afterwards:

> *"Solar Sunrise thus demonstrated to the interagency community how difficult it is to identify an intruder until facts are gathered in an investigation, and why assumptions cannot be made until sufficient facts are available."*[37]

Even intruders who try to bring down whole networks are not called "terrorists" and their activities are not dubbed "war" by law enforcement agencies. They rather call them "criminals" or "digital outlaws", as did then attourney general Janet Reno at the Cybercrime Summit 2000.[38]

Interestingly, law enforcement's perception of the problem is now being structured as well by private actors. Since 1996, the San-Francisco-based Computer Security Institute works together with the FBI's Computer Intrusion Squad in conducting the annual Computer Crime and Security Survey, a widely recognised study on dangers, cases and countermeasures in IT security.[39] Here, one finds a private-public partnership that already is influencing the risk perception.

Economic Loss

Because many of the critical infrastructures are run by the private sector, the companies' perception of the risk was very important as well. A striking fact are the completely different criteria for measuring and weighing risks in the private sector. The service providers normally do not see the national implications of the new vulnerabilities, and they do not care very much about tracking down the suspects. Therefore it is not very important to them *who* breaks into their computers. Their main goal is to keep the systems up and runnning and to avoid data theft by competitors or intelligence agencies. When a hacker attack is over and the systems are restored, the companies only have limited interest in informing the police at all.[40] Rather than cooperating with government agencies they prefer contracting specialised IT security service providers. These normally work more efficiently and less bureauratically and help solving the important day-to-day problems.[41]

---

37 Freeh 2000.

38 Reno 2000.

39 Power 2000:1.

40 According to the Crime and Security Survey 2000 only 25 percent of the attacked companies reported these attacks to the law enforcement agencies, Power 2000:13.

41 Mendoza 2000.

As important as the top management's risk perception is that of the group of persons who often work in the basement, namely the system administrators and IT experts. They almost daily have to deal with hacking attempts, and for them, the problem breaks down to single, concrete challenges. They install new virus scanners on the company's network, take care of the users changing their passwords on a regular basis, try to take workload from a server during a denial-of-service attack, or restore deleted files from the backup tapes after a hacker break-in. In this technical expert community the problem now discussed as a "national security threat" has existed since computers became networked in the first place. Here it is mainly seen as a technical and practical problem, less as a political thing and much less as a problem for national security policy. The lead ideas are "computer security" or "IT security", not "national security". Because these experts often are the only ones in an organisation who can really estimate the details and challenges, their perception as well influences the way the management deals with IT security.

2.2. Resources

The Military

The U.S. armed forces are the most advanced in the world in developing offensive information warfare capabilities. They are planned as "another arrow in the quiver"[42] in conventional military operations, but shall as well give the government deterrence and strike-back capabilities in countering the cyber-threat. The idea is to prevent an attack through strength. It was John Hamre again who made it very clear: "That really was the message of Pearl Harbor. It wasn't that we got hit. It was that we were ready to respond", he told the public in August 1999 at the opening ceremony of the Joint Task Force - Computer Network Defense Operations Center, the central coordination point for the security of all U.S. military networks.[43]

The U.S. military has already been active in digital electronic warfare since the eighties, when the armed services started their own research in computer viruses.[44] In the early nineties the development gained more momentum, when the Gulf war showed the importance of information systems and communications lines for fighting a short, effective war. In 1994 a special School for Information Warfare and Strategy was set up at the National Defense University. Since 1998 the U.S. military has its own Joint Doctrine for Information Operations (Joint Pub. 3-13), which as well includes computer network attacks on civilian infrastructures.[45] The central coordination point for these activities, the Joint Task Force - Computer Network Attack, was set up and subordinated to U.S. Space Command in October 2000. More units are located at the Air Intelligence

42 Then Comander of U.S. Space Command and now Chairman of the Joint Chiefs of Staff, General Richard B. Myers, quoted in UPI 2000.

43 Garamone 1999.

44 Graham 1998.

45 Joint Chiefs of Staff 1998.

Agency in San Antonio/Texas, among them the Air Force Information Warfare Center with more than 1000 personell and the Joint Information Operations Center.[46]

In spite of the growing interest and the strong effort put into this field, the U.S. military has not reached the capability to successfully wage a large-scale cyberwar yet. The few cyber-missions during the Kosovo war showed this quite clearly. The Air Force had waged some cyber attacks on the Serbian air defense system[47], but afterwards came under heavy criticism for the inefficiency of these measures.[48] Especially the cascading effects of information attacks are complicated to estimate, because one not only needs the know-how and technology to get into the enemy's computer systems, but as well has to know how they are embedded in his social organisation and strategy.

Law Enforcement

The law enforcement agencies have been dealing with computers for some years now, because normal criminals as well tend to make more and more use of modern technologies. This already lead to the establishment of the National Computer Crimes Squad at the FBI in February 1992. In the same year the Computer Analysis and Response Team (CART) was set up, a specialised unit for computer forensics. Since 1998 every one of the 56 FBI field offices has its own Computer Crimes Squad.[49] The several activities in this field have been coordinated by the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) since 1996. The efforts still are comparably weak. Only 243 of a total of 11 639 FBI agents are designated for the investigation of computer crimes. Even this number has not been reached yet, and many of them are not really prepared for their task.[50]

In spite of these difficulties the FBI's buid-up of specialised computer units altogether has shown some results. In the last year, some spectacular cases of hacking or computer fraud have been solved within very short time. These sucesses as well led to a more stable self-confidence of law enforcement agencies. After the FBI had caught a student who only a week before had circulated a fake stock exchange message intended to manipulate stock values, federal attourney Alejandro Mayorkas told the press in September 2000: "We in law enforcement can navigate the 'information superhighway' just as we can beat the pavement to detect and apprehend criminals".[51]

Private Infrastructure Service Providers

Because almost all critical infrastructures are run by private or local entities, these from the beginning on had a strong position in the cyber security debate. Only here the technical expertise is available one needs to successfully defend against an attack. The

46 For an overview see Bendrath 2001b.
47 Becker 1999.
48 Verton 2000.
49 Owens 1997.
50 Suro 1999.
51 Quoted in PC World 2000.

companies that run the systems can much more easily focus on “hardening” them than on striking back. They install firwalls, redundant emergency systems, backup facilities and other defensive systems. With this practice they already help to secure the U.S. from a large-scale cyber attack, often without viewing this as part of a national security policy strategy at all.

More importantly, the strategic ressources in the hand of the infrastructure providers are not only their people and their firewalls, but the virtual landscape itself in which a cyber attack would occur. It is not a public good, like the territorial border or the national coastline, but private infrastructures providing public services through the market. In a significant difference to classical territorial defense, the defense against attacks in cyberspace is inseparably connected to controlling the systems of which it consists. Delegating it to the state is difficult, if not practically impossible.

2.3. Norms

Neo-Liberalism and the ‚Californian Ideology ‘

A number of strong norms limited the efforts of the traditional security policy institutions to expand their fields of action into cyberspace. These norms had less to do with questions of national security and more with the general relationship between the state and society. The so-called “neo-liberalism” that had gained much acceptance among the elites of western societies in the nineties calls for the smallest possible role of the state, especially in economic affairs. In the field of new technologies two more aspects added to this: First, a big majority in Washington strictly was against disturbing the dynamic of the ‚new economy‘ by government interventions or regulations. “Government has largely taken a hands-off approach to the new economy”, as the report “State of the Internet 2000” concluded.[52]

Secondly, high political hopes were put into the digital communications media. Many expected that they would help the development of decentralised and self-organised social structures. This so called “Californian ideology‘ [53] that became popular in Washington as well in the mid-nineties promised an era of the free and non-hierarchical association of electronically networked citizens. Within this technology-deterministic and anti-etatistic norms framework to which many of the high-tech companies’ leaders subscribed, a strong role for the state in solving problems was hardly the right thing.

In terms of security policy theory, the debate circled around the question for the reference object of security. In plain english: What is to be secured? While the security policy elites saw “national security” in danger, the other side was concerned about the security of single computer systems and their users. Here the civil rights organisations played an important role, because they warned of the unintended consequences of a risk policy based on military strength or repression - mainly the dangers for privacy.

---

52 United States Internet Council 2000: 29.

53 Barbrook/Cameron 1997.

Military Identity and Professionalism

The idea of waging war in cyberspace as well seemed odd for many military officers in the first place. Cyberspace implies a completely different concept of space and body, because the space here only consists of symbols and their links. Because there are no linear distances like in the cartesian physical space, there is no frontline anymore. The actors in cyberpace are not physically present, but are instead represented by symbols. In this bodyless cyberspace there is no room for physical violence. The application and organisation of physical violence, though, is part of the professional military identity until today. "As soon as things start to look different than killing people and smashing things, the military start to point at others", a Pentagon advisor decribed this.[54]
Only recently the armed forces seem to accept computer network operations as part of their professional duties, because these have been - at least officially - limited to two tasks: The protection of their own networks and attacks against military enemies in times of war.[55]

Legal Norms

Experts in international law still are debating if cyber attacks can be considered an act of war at all.[56] But if this is the case, a strategy based on cyber-counter attacks could break the law of armed conflict. Military cyber attacks for example would ignore the rule that a regular soldier has to wear a uniform, but would also get in conflict with more important norms codified in the Hague and Geneva conventions. These international treaties for example prohibit perfidous or unneccessary attacks, the use of the territory of neutral states, attacks on civilian populations or weapons that do not distinguish between combattants and non-combattants.[57] The fact that the U.S. armed forces only reluctantly made use of their cyber arsenal was partly due to these concerns. In the Kosovo war 1999 some originally planned cyber attacks against Serbia did not take place because the Pentagon's own lawyers vetoed them after having studied the international jurisdictional difficulties of cyberwar.[58]

U.S. domestic law as well produced headaches for the lawyers of the armed forces, because an attack to American infrastructures could originate in Iraq as well as in the United States. A military counter-strike through cyberspace therefore unwillingly could lead to an operation of U.S. armed forces on domestic territory. This is prohibited by the Posse Comitatus act of 1878.[59]

On the other hand, there have been laws against computer crime since the eighties. The most important one is the Computer Fraud and Abuse Act of 1984, which since then

54 Quoted in Carlin 1997.

55 U.S. Space Command 2000.

56 For a sceptical position see Aldrich (1996: 102f); for the opposite interpretation see Marauhn/Stein (2000: 3-6).

57 Aldrich 1996: 104-109.

58 Associated Press 1999.

59 The text says: "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both", 18 U.S. Code § 1385.

has been amended three times.[60] On this basis electronic break-ins into computer systems have been treated as crimes, and the FBI quickly used this for building up structures able to deal with them. The domestic laws thus enabled a strong position of law enforcement agencies in fighting cyber attacks.

One of the oldest laws for computer security, the Computer Security Act of 1987[61], points in another direction. With it, the different departments of the government were directed to formulate their own plans for IT security. Here we can see an early example of handling the risks of information technology in a decentralised, preparative manner.

The legal norms in sum prevented a more important role of the armed forces in protection critical infrastructures, while giving law enforcement new tasks. Moreover, decentralised preventive measures were already taken in the eighties. This is reflected today in the cooperation efforts with the private sector.

3. The Policy

3.1. First Studies

In June 1995 President Clinton set up a special study group, the Presidential Commission on Critical Infrastructure Protection (PCCIP), to deliver a comprehensive report on the security of all infrastructure systems in the United States. While this included not only information and telecommunication networks, but as well the financial sector, energy supply, transportation and the emergency services, the main focus was on cyber risks. This had two reasons. First, these were the least known because they were so new, and secondly, many of the other infrastructures depend on data and communication networks. The PCCIP included representatives of all relevant government departments, not only from the traditional security policy establishment. Additionally, the private sector was involved. This was based on the assumption that security policy in this field is no longer only a duty of the government, but a "shared responsibility".[62] This decision opened up the realm of possible strategies far beyond the core measures of security policy - physical violence and repression.

Together with the PCCIP Clinton set up the Infrastructure Protection Task Force (IPTF) to deal with the more urgent problems in infrastructure protection until the report was published. Only representatives of the FBI, the Department of Defense and the NSA - the state's classical security policy institutions - were members of the IPTF.[63] Insofar the IPTF can be understood as a compromise between a completely cooperative approach - including the private sector and other departments as well - and a classical security policy approach - giving the task to the FBI *or* the Department of Defense. The IPTF was chaired by and located at the Departement of Justice to make use of the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) which

60 18 U.S. Code § 1030, amended 1986, 1994 and 1996, see United States Congress 1996.
61 United States Congress 1988.
62 White House 1996.
63 White House 1996.

had been set up shortly before at the FBI.[64] Obviously, the institutional resources of the FBI had been decisive here. A more militant approach still was an option then, shown for example by the appointment of former Air Force General Robert T. Marsh as PCCIP chairman.

3.2. Setting Up an Institutional Structure

The PCCIP presented its report in the fall of 1997.[65] President Clinton followed most of their recommendations in May 1998 with his Presidential Decision Directives (PDD) 62 and 63. With them, he created up the position of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism at the National Security Council, who is supported by the newly founded Critical Infrastructure Assurance Office (CIAO). The Office of Computer Investigations and Infrastructure Protection (OCIIP), which had been built at the FBI on the basis of the CITAC, was expanded to the inter-agency National Infrastructure Protection Center (NIPC). The NIPC is located at the FBI headquarters and is mainly staffed with FBI agents, but representatives and agents from other departments and the intelligence agencies work there as well. The NIPC is responsible for early warning as well as for law enforcement and is coordinating the different government and private sector activities. The NIPC therefore has a central role in the new cyber security policy. High-level coordination within the different branches of the government since then is organised by the new Critical Infrastructure Coordination Group (CICG).[66]

The security of the different sectors of the infrastructure is organised by different departments that became "lead agencies" for each of the sectors. For top-level strategic coordination between the government and the private sector, PDD 63 envisaged a National Infrastructure Assurance Council (NIAC), chaired by the National Coordinator. Additionally, new Information Sharing and Analysis Centers (ISAC) in each of the sectors were planned. They should be run by the private companies who would as well determine their institutional forms and working procedures.[67] The close cooperation with the private sector that had begun with the PCCIP thus was continued and even enhanced. The government explicitly emphasised the necessity of these non-hierarchical forms of cooperation:

> *"Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative."*[68]

Not only the state anymore, but as well the private providers of the infrastructures now are responsible for cyber security policy. Different to the realm of the old monopoly of

64 Tritak 1999.
65 PCCIP 1997.
66 White House 1998.
67 White House 1998.
68 National Security Council 1998.

force one here finds a networked self-help system, which in a way could be called post-modern. In some areas the government still plays its traditional role through law enforcement and intelligence, while in other areas it only moderates the activities of the private sector.

3.3. The "National Plan for Information Systems Protection"

The President´s Commission on Critical Infrastructure Protection explicitly had called its 1997 report a "beginning"[69], and the presidential directives of May 1998 as well had acknowledged that there was no masterplan for critical infrastructure protection yet.[70] Since then, a number of government departments, agencies and committees have worked on a comprehensive national strategy. On 7 January 2000, President Clinton presented its first version - under the headline "Defending America´s Cyberspace" - to the public.[71] This "National Plan for Information Systems Protection" still represents the actual state of American policy towards the new cyber risks. The White House published a follow-up report in February 2001 after the inauguration of George W. Bush, but this only documents the state of the single programs and does not include a change in strategy.[72]

The Government Only Protects Itself

The plan emphasises the assumption of cyber security being a shared responibility between the government and the private sector. The government agencies now are only responsible for protecting their own networks agains intruders. Three new institutions together work for the security of the state´s computer systems. The Federal Computer Incident Response Capability (FedCIRC), a part of the General Services Adminstration (GAO), is building a central analysis cell to investigate incidents in all non-military computer networks of the government. For military computers this is done by the Joint Task Force – Computer Network Defense (JTF-CND), which was already set up in 1999. The JTF-CND is located at the Defense Information Systems Agency (DISA) near the Pentagon, but is subordinated to the Space Command in Colorado Springs.[73] The NSA's National Security Incident Response Center (NSIRC) provides support to FedCIRC, JTF-CND, DISA, NIPC und the National Security Council in case of attacks against systems that belong to the national security apparatus.[74] The FBI's NIPC still is responsible for incident warnings, strategic analyses, and law enforcement.[75]

Within the government we now find a decentralised and cooperative risk policy similar to the one intended between the government and the private infrastructure service providers. The FBI still has a fairly strong position compared to the Pentagon and the intelligence community. With FedCIRC one central protective function, though,

---

69 PCCIP 1997:101.
70 White House 1998:3.
71 White House 2000.
72 White House 2001.
73 White House 2000: 39-42.
74 White House 2000: 49.
75 White House 2000: 42.

is now being fulfilled by an agency that itself is an infrastructure service provider of and for the government.

Computer Crime or Cyberwar?

In spite of the FBI's strong position the protection of computer systems is not only a question of domestic security. NIPC is located at and mostly run by the FBI, but it can as well be subordinated to the Department of Defense by presidential order. The National Plan tried to reproduce the classical difference between police and military by making such a decision dependent on an attack coming from abroad. But of course not every simple hacking attempt that does not originate in the U.S. should trigger a respone by the Department of Defense. The decisive criteria for differentiating between war and crime therefore is the scale of the attack.[76] This has an interesting implication: The ability to detect a large-scale attack as such now depends on the sensoric instruments of the NIPC and the willingness of the private sector to share information with the government. The military is almost "blind" here and depends on the judgement of law enforcement agencies and even private infrastructure service providers. In the case of the new cyber risks, it it hard to differentiate between domestic and international security. The de-territorialised cyber-security policy blurs the line between war and crime, and the institutional responsibilities for a government response against an attack have to be set on a case-by-case basis.

Privatisation of Cyber Security

The second part of the National Plan deals with the security of privately run infrastructures. It starts with stating, "the Federal Government alone cannot protect U.S. critical infrastructures."[77] The state and local governments are as well called "partners" of the federal government, but the emphasis lies on private companies. The goal is a close private-public partnership. To ease concers of the infrastructure service providers, the plan goes at great lenghts emphasising fundamental principles like "voluntary" or "trust" and the companies' own interests in protective measures.[78] The government tries to make them accept its offers for checking their defenses, for sharing information, and for further developing technical standards. Existing institutions like the North American Electric Reliability Council (NERC) are named as good examples.[79]

The private sector, though, still is hestitating strongly. The Information Sharing and Analysis Centers (ISACs) that were already planned in the 1998 Presidential Decision Directive have been set up very late, in some sectors they do not exist at all until today. The Financial Services ISAC (FS/ISAC), the first of these centers, was only set up on 1 October 1999, almost one and a half year after the Presidential directives, and the IT-ISAC only started operations in March of 2001. Other sectors do not have

76 White House 2000: 42.
77 White House 2000: 104.
78 White House 2000: 106.
79 White House 2000: Chapter 5.

coordination centers like these until today. Besides the old NERC there only is the National Coordinating Center for Telecommunications, run jointly by the state and the industry.[80]

This hesitation is remarkable, because the government has put much effort into reaching more.[81] President Clinton in summer 1999 even signed an executive order to accelerate the founding process of the *National Infrastructure Assurance Council* (NIAC). The NIAC had already been planned since 1998 as a forum for strategic debates among government officials and representatives of the big IT companies.[82] It was finally set up in January 2001, one day before Bill Clinton left his office in the White House.[83]

Many companies do not see any necessity of working together with the government, and they are especially reluctant to let law enforcement or intelligence agencies know too much about their information systems. And they do not see government institutions as a real help against the new risks related with computer security. Especially the NIPC received heavy criticism after it failed to quickly respond to some email worm infections in 2000 and 2001.[84] A lot of companies therefore prefer contracting private IT security service providers, as these work faster and less bureaucratic than government agencies. These specialised IT security companies more and more take the role of traditional risk management consultants.[85]

As long as the "electronic Pearl Harbor" does not occur, we can not expect the private sector to develop an original interest in a more prominent role of the government in IT security. Instead of a centralised coordination by the state, almost all the companies need are the private, local security instruments provided by the market.

4. Conclusion

Since the early nineties the debate about hacker attacks against the U.S. has made its way from specialised expert circles to the agenda of "high politics" and national security. This alone is remarkable because of the lack of a classical "threat triangle" consisting of actor, intention, and capabilities. There was no clear enemy and therefore no hostile intention around which such a discourse could have cristallised. The risk communication instead started at the last corner of the triangle, the capabilities. Here as well we can note something special: The possibility of a damage to critical infrastructures was not induced by the existence of weapons or other dangerous tools, but by the socio-technical structure of the United States itself.

Until the mid-nineties three different risk strategies were available: Repression and military strength (intervention), technical solutions for securing the systems (preparation) and awareness-building (information). These strategies were linked to

80 For an overview see Bendrath 2001a.
81 White House 2000: Chapter 5.
82 iPartnership 1999.
83 Frank 2001.
84 Wolf 2001.
85 Ceniceros 2000.

different actors in different institutions and cultures, who promoted them using different ressources and calling upon different norms.

According to the standard assumptions of risk sociology the perception of risks plays an important role in deciding how to deal with them. The "risk communication" therefore should be an indicator for the selected security strategies. In the case presented here the dramatisation of the risk with terms like "information warfare", "cyberwar" or "electronic Pearl Harbor" was necessary to get the problem onto the political agenda. The political strategies developed should therefore have been more interventionist, using military-like means and approaches. Other case studies on the "war on drugs" or "counter-terrorism" show these results. Here the dangers and situations as well were framed in terms taken from military language.[86]

The risk policy selected in the case of cyber security differs significantly from these assumptions. In spite of high public interest the militant discourse could not be transformed into a like-minded strategy. The outcome of ten years of discussion and almost five years of reforms, presented by Bill Clinton in the National Plan for Information Systems Protection in January 2000, consists of three approaches: Law enforcement, private-public partnership, and private and public self-help. At its core we find the strategy of preparation, the preventive protection of critical infrastructures by technical means.

The study has shown the overdetermination of this rather civilian and cooperative outcome. Strong restrictions against a military-interventionist strategy existed in the dimension of perception as well as of ressources and norms.

In the realm of risk *perception* two discourses were influential besides the military metaphors widely used in the mass media. On the one hand, law enforcement agencies emphasised their view of the risk as "computer crime", on the other hand and more importantly, the private sector running the infrastructures perceived the risk as a local, technical problem or as economic costs. Therefore, the debate about cyber risks is an example for a failed "securitisation"[87]. The security policy institutions only partly managed to widen the concept of security in this case, because it was impossible to achieve a consensus between the different groups about the reference object of security. Similar to the regulation of cryptography[88], at the core of the debate was the question: Does "security" mean the security of the American society as a whole - "national security" - , or is it the security of the single users or technical systems? Implicitly, this security policy discourse dealt with the relation between the state and its citizens.

The distribution of *resources*, the technical and social means for countering the risk, was important as well and also had an impact on the discourse. Because the technical foundations of the risk make it very difficult to fight possible attackers in advance, in practice the measures taken focused on preparative strategies, trying to minimise the impact of an attack when it occurs. Here, the infrastructure providers with their preference for decentalised and private approaches had a strong position, because in the end only they are able to install the technical instruments for IT security at the single infrastructures.

---

86 Daase/Feske/Peters 2001.

87 Wæver 1996:47-53.

88 Saco 1999.

Norms as well were important in selecting the strategies. Cultural norms like the new economy's anti-etatistic "Californian ideology" as well as legal restrictions prohibited a bigger role of the state, especially of the armed forces. The interventionist mind-set of the security policy community almost gained no acceptance. On the contrary, within the armed services there even was much hesitation against new, non-traditional military tasks. Most importantly, the general "no government regulations" approach towards the new economy which had wide support across all political factions strongly limited the strategy selection. This as well reflects the policy of the Clinton administration that normally preferred economic over security policy ideas - prominently featured in the famous President's quote: "It's the economy, stupid!" Besides these cultural strategy differences legal norms as well set limits for a more military-like strategy. The difficulties to decide if cyber attacks constitute an act of war, the fear of committing war crimes by conducting electronic counter strikes, and the prohibition of using the armed forces domestically made the Pentagon hesitate with building up its own infowar units. On the contrary, the cybercrime laws that had already existed since the eighties enabled the FBI to start building up operative units very early.

Altogether, this study has shown that the public perception, which until today is full of military metaphors, only had a limited influence on the risk policy strategy. When there are concurrent discourses and viewpoints, the policy selection obviously depends upon two factors: One is the different ressources available to the different groups which become the more important the closer they are connected to the real (here: technical) structure of the risk. The other factor is the cultural and legal norms, because they limit the set of answers available to the fundamental question: What kind of strategy can be selected at all?

For the newer debates in other countries about the risks of the information society, this study leads to a conclusion that can shortly be described as "don't panic". The militarisation of cyber security policy will be very difficult in a liberal society with private infrastructure providers. From the American experience we should rather learn that "cyberwar" is a fundamentally inadequate term that more disturbs than enables a useful risk policy.

Bibliography

ABC Nightline 1997: Cyber Terror - A Consequence of the Revolution, 12/07/1997, transcript available at http://www.infowar.com/CLASS_3/class3_011298a.html-ssi.

Aldrich, Richard W. 1996: The International Legal Implications of Information Warfare, in: Airpower Journal, 10: 3, 99-110.

Anderson, Robert H./Hearn, Anthony C. 1996: An Exploration of Cyberspace Security R&D Investment Strategies for DARPA. "The Day After ... in Cyberspace II", Santa Monica/Ca.: RAND

Arquilla, John/Ronfeldt, David/Zanini, Michele 1998: Networks, Netwar, and Information-Age Terrorism, in: Lesser, Ian O./Hoffmann, Bruce/Arquilla, John/ Ronfeldt, David/Zanini, Michele (Hrsg.): Countering the New Terrorism, Santa Monica/Ca.: RAND, 39-84.

Associated Press 1999: Pentagon Ponders Legality of Cyber Weapons, 11/09/1999.

Barbrook, Richard/Cameron, Andy 1997: Die kalifornische Ideologie, in: telepolis, 02/05/1997, http://www.heise.de/tp/deutsch/inhalt/te/1007/1.html.

Beck Ulrich 1986: Risikogesellschaft. Auf dem Weg in eine andere Moderne, Frankfurt/M.: Suhrkamp Verlag.

Becker, Elizabeth 1999: Pentagon Sets Up New Center for Waging Cyberwarfare, in: New York Times, 10/08/1999.

Bendrath, Ralf 2001a: Homeland Defense, virtuelle Raketenabwehr - und das schnöde Ende einer Medienhysterie, in: telepolis, 03/28/2001, http://www.telepolis.de/deutsch/special/info/7234/1.html.

Bendrath, Ralf 2001b: Krieger in den Datennetzen. Die US-Streitkräfte erobern den Cyberspace, in: Armin Medosch (Hrsg.): Viren, Warez und Hoaxes – Die Kultur des gesetzlosen Internet, Hannover: Heise Verlag, forthcoming.

Carlin, John 1997: A Farewell to Arms, in: Wired, 5: 5, May.

Ceniceros, Roberto 2000: More Consultants Offering Technical Help to Ensure Security, in: Business Insurance, 04/03/2000.

Clarke, Richard A. 2000: Memorandum. Implementation of PDD 63 through Project Matrix, Critical Infrastrucutre Assurance Office, 07/19/2000, Washington D.C.

CNN 1996: Cyberspace Attacks Threaten National Security, CIA chief says, 06/25/1996.

Cohen, William S. 2000: Annual Report of the Secretary of Defense to the President and the Congress, Washington D.C., Chapter 1: The Defense Strategy.

Commission on National Security in the 21st Century 2001: Road Map for National Security: Imperative for Change. The Phase III Report of the U.S. Commission on National Security/ 21st Century, Washington D.C., 02/15/2001.

Daase, Christopher/Feske, Susanne/Peters, Ingo (eds.) 2001: Internationale Risikopolitik, Baden-Baden: Nomos Verlagsgesellschaft, forthcoming.

Deutch, John 1996: Foreign Information Warfare Programs and Capabilities, Testimony to the U.S. Senate Committee on Governmental Affairs; Permanent Subcommittee on Investigations, 06/25/1996.

DoD 1998: Department of Defense: News Briefing, 04/16/1998.

Frank, Diane 2001: IT Firms Unite to Share Security Info, in: Federal Computer Week, 01/17/2001.

Freeh, Louis J. 2000: Statement of the Director Federal Bureau of Investigation before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies, 02/16/2000.

Garamone, Jim 1999: Hamre “Cuts” Op Center Ribbon, Thanks Cyberwarriors, in: American Forces Press Service, 08/11/1999.

Graham, Bradley 1998: In Cyberwar, A Quandary Over Rules And Strategy, in: International Herald Tribune, 07/09/1998.

Hamre, John J./Campbell, John H. 1998: Statement of the Honorable Hamre (Deputy Direcor of Defense) and Brigadier General John H. Campbell (Deputy Director for Information Operations) at the Joint Military Procurement and Research and Development Subcommittee Hearing on Critical Infrastructure Protection - Information Assurance, 06/11/1998.

Ingles-le Nobel, Johan J. 1999: Cyberterrorism Hype, in: Jane´s Intelligence Review, 10/21/1999.

iPartnership 1999: President Forms Infrastructure Assurance Council, 07/15/1999.

Joint Chiefs of Staff 1998: Joint Pub. 3-13, Joint Doctrine for Information Operations, Washington D.C., 10/9/1998.

Klischewski, Ralf/Ruhmann, Ingo 1995: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie. Studie für das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Bonn.

Madsen, Wayne 1998: Teens a Threat, Pentagon Says, in: Wired News, 06/02/1998.

Marauhn, Thilo/Stein, Torsten 2000: Völkerrechtliche Aspekte von Informationsoperationen, in: Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, 60: 1, 1-40.

McKay, Niall 1998: Cyber Terror Arsenal Grows, in: Wired News, 10/16/1998.

Mendoza, Martha 2000: Valley Cool to Reno Cybercrime Plan, in: L.A. Times, 04/06/2000.

Minihan, Kenneth A. 1998: Prepared statement by Lt. Gen. Kenneth A. Minihan, Director, National Security Agency, before the Senate Governmental Affairs Committee, 06/24/1998.

Molander, Roger C./Riddile, Andrew S./Wilson, Peter A. 1996: Strategic Information Warfare: A New Face of War, Santa Monica/Ca.: RAND.

National Security Council 1998: White Paper. The Clinton Administration´s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, Washington D.C.

Office of the Under Secretary of Defense for Aquisition & Technology 1996: Report of the Defense Science Board on Information Warfare-Defense, Washington D.C.

Owens, Charles L. 1997: Testimony of Charles L. Owens, Chief, Financial Crimes Section, Federal Bureau of Investigation, on Computer Crimes and Computer Related or Facilitated Crimes before the Subcommittee on Technology, Terrorism, and Government Information, Senate Committee on the Judiciary, 03/19/1997.

PCCIP 1997: President´s Commission on Critical Infrastructure Protection: Critical Foundations. Protecting America´s Infrastructures, Washington D.C.

PC World 2000: Feds To Net Criminals: You Can't Hide, in: PC World, 09/06/2000.

Poulsen, Kevin 2001: Hack Attacks Called the New Cold War, in: The Register, 03/23/2001.

Power, Richard 2000: 2000 CSI/FBI Computer Crime and Security Survey, in: Computer Security Issues&Trends, 6:1, 1-15.

Reno, Janet 2000: A Law Enforcement/Information Technology Industry Dialogue on Prevention, Detection, Investigation and Cooperation, Speech at the Cybercrime Summit, Stanford/Ca., 04/05/2000.

Rötzer, Florian 2000: Die Infektionsgefahr eines Liebesbriefs, in: Telepolis, 05/05/2000, http://www.heise.de/tp/deutsch/inhalt/glosse/8110/1.html.

Saco, Diana 1999: Colonizing Cyberspace: “National Security” and the Internet, in: Weldes, Jutta/Laffey, Mark/Gusterson, Hugh/Duvall, Raymond (eds.): Cultures of Insecurity. States, Communities, and the Production of Danger, Minneapolis/Minn.: University of Minnesota Press, 261-291.

Serabian, John A. Jr. 2000: Statement for the Record before the Joint Economic Committee on Cyber Threats and the U.S. Economy, 02/23/2000.

Smith, George 2001a: “Electronic Pearl Harbour”, in: Crypt Newsletters´s Guide to Tech Terminology, http://sun.soci.niu.edu/~crypt/other/ harbor.htm.

Smith, George 2001b: “Eligible Receiver”, in: Crypt Newsletter´s Guide To Tech Terminology, http://www.soci.niu.edu/~crypt/other/eligib.htm.

Suro, Roberto 1999: FBI Cyber Squad Termed Too Small for Hacker Threat, in: Washington Post, 10/07/1999.

Thomas, Timothy L.: Russian and Chinese Views of Information Warfare, Workshop at the InfowarCon in Washington D.C., 09/07/2001.

Tritak, John S. 1999: Statement before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information, 10/06/1999.

UPI 2000: Space Command Readies For Infowar, United Press International, 01/05/2000.

U.S. Space Command 2000: U.S. Space Command Takes Charge of Computer Network Attack, Press Release No. 15-00, 09/29/2000.

United States Congress 1988: Computer Security Act of 1987, Public Law 100-235 (H.R. 145), 01/08/1988.

United States Congress 1996: Report of the Senate Committee on the Judiciary on the National Information Infrastructure Protection Act, Washington D.C.

United States Internet Council 2000: State of the Internet 2000, Washington D.C.

Verton, Dan 2000: DoD Redefining Info Ops, in: Federal Computer Week, 05/29/2000.

Wæver, Ole 1996: Sicherheit und Frieden: Erweiterte Begriffe, engere Freiräume für Politik?, in: antimilitarismus information, 25: 11, 45-57.

White House 1996: Executive Order 13010: Critical Infrastructure Protection, 07/15/1996.

White House 1998: Presidential Decision Directive/NSC-63, Critical Infrastructure Protection.

White House 2000: Defending America´s Cyberspace. National Plan for Information Systems Protection Version 1.0. An Invitation to a Dialogue, 01/07/2000.

White House 2001: Federal Critical Infrastructure Protection Activities, 02/22/2001.

Wolf, Jim 2001: US cyber security center lags on threat warnings - GAO, in: Reuters, 05/22/2001.