THE CYBERWAR DEBATE: PERCEPTION AND POLITICS IN US CRITICAL INFRASTRUCTURE PROTECTION

Ralf BENDRATH

1. The Information Society as Risk Society

"Cyberwar" has become a growth market in the US. While ten years ago the term would hardly have made sense to any expert, in the meantime attacks on computer networks and their implications for national security have received broad coverage in the 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 US' 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 US government under George W. Bush is likewise trying to address the problem.[1]

As with nuclear energy production, the dangers arising from digital networking are not easily discernible for a non-expert. To detect a virus on your hard drive, you need a virus scanner as a sensory tool; to find out if there is a cracker in your network, you need an intrusion detection system or a competent system administrator with spare time. For the average user, an intentional hacker attack cannot 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 attacks, it is not at all obvious whether the computer that is no longer providing its service has just crashed, whether the cable connecting it to the Internet was physically damaged, or whether it is the victim of a targeted flood of packets and requests.

The so-called "information society" is thus showing significant signs of being a "risk society." The new risks, according to Ulrich Beck, who coined the term in the 1980s, are no longer immediately obvious, 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 is especially true for insecurities related to the infrastructure.

As early as 1990, the US National Academy of Sciences began 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 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 focused especially on the so-called "critical infrastructures" like telecommunications, 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 threat, which consists of the dimensions *actor*, *intention*, and *capabilities*, "cyberwar" threats cannot easily be categorized. First, there is no clearly identifiable *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 globalization. This implies, secondly, that it is very hard to get verifiable information on the *hostile intentions* of the possible attacker: Does he or she want to attack the US at all? Is he planning to use cyber attacks? This leads to the third open question: Does the possible enemy have the *capability* to wage a large-scale cyber attack against the US? 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 personnel 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 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 employed 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 minimizing the possible damage after an attack, or will it aim at preventing an attack in the first place?

The US was 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 have gained some years of experience since. A detailed review of US 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 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 any risk policy: Risk perception, resources, and norms.

2. Factors Influencing the Development of a Risk Policy

2.1. Risk Perception

Capabilities as a Starting Point

The complexity of world society after the end of the Cold War has led security politicians and experts to focus more on the capabilities of possible enemies than on their intentions. This applies just as much to nuclear proliferation or ballistic missiles as to “international terrorism.” Security assessments rely more and more on the technical means that might be available to possible enemies. The new potential for cyber attacks was addressed in similar terms in the debate.

The change in the general perception of insecurity coincided with growing concerns in the Department of Defense over the vulnerability of the networked armed forces. While the debate on the “Revolution in Military Affairs” (RMA) was kicked off with extremely high hopes in the early 1990s, with trendy articles and studies on “network-centric warfare” or the real-time information flow through the global “system of systems” for C^{4}ISR,[7] since the mid-1990s one finds more and more warnings on the risks. Because a great deal of military communication is forwarded through civilian infrastructures, the risks that civil infrastructures are exposed to attacks from hackers and other intruders were also seen as a threat to 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 US military (see 2.2.). As the debate on attacks against the information systems of possible enemies went further, the eventual dangers for the US' own military and civilian data networks became a major issue as well.

What makes the whole debate on the vulnerability of electronic infrastructures typical of current 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 cannot be well compared with reality, 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 of the US military data networks' vulnerability, only unclassified or simulated systems were attacked.[9] Furthermore, one often finds impressive data on the *numbers* of known hacker attacks, but in almost all cases a statement on the *damage* is lacking. A serious risk calculation, however, 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 are still 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] As yet, there are no standard procedures for identifying and assessing the vulnerability of critical infrastructures. These have been under development by the Critical Infrastructure Protection Office's project "Matrix" since June 2000.[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 resulting simplification of this pattern of argumentation can be seen in the simple claim voiced by Deputy Secretary of Defense John Hamre in a Congress hearing in June 1996: "Mr. Chairman, there will be an electronic attack sometime in our future."[13] In this way, the discourse on cyber dangers has been strongly popularized, 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 prevent such events by acting today.[14]

One question is never addressed within this discourse: How plausible are these scenarios? The participants learned to deal with them as external, given realities, and the scenarios established a specific fear-driven cyber mindset in the security policy community, even though many of these assumptions have proven wrong in the long run.[15] This is a good example of how to establish a threat-based discourse in the absence of a clear danger, where there is only the risk of a potential future threat. In other words, like a member of the Syndicate once said to Agent Fox Mulder in the TV show, The X-Files: The best way to predict the future is to invent it.

However, this approach has placed cyber-risk on the political agenda. The main remaining question was: How to deal with it? Or, maybe more important in the fragmented political landscape of Washington: Who should be in charge? Should it be the classical institutions responsible for national security, like the Pentagon or the intelligence agencies? Or 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 way potential enemies or damages were cast.

Military Rivals

In the summer of 1995, the National Intelligence Council reported on the information warfare capabilities of other international actors for the first time. The document is classified, but its conclusions were presented to the public. According to the report, 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 Bill 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 is thin, though; it consists mostly 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 specialized "infowar" units of the People's Liberation Army, but cannot provide information on their capabilities. The Russian concept of information warfare, on the other hand, differs significantly from the US view, aiming more at psychological manipulation and less on computer network attacks.[20]

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

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

Yet, this military-like discourse had much influence on Washington's security policy establishment; CIA director John Deutch, for example, has regularly warned of threats to national security from cyber attacks since the mid-1990s. 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 arise from states. Jaques Gansler, then Assistant Secretary of Defense for Acquisition 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 American society to the new risks, thus forcing the political elite to respond somehow. The mass media gratefully took up the term and featured it prominently in almost every report on the issue.[29] The concept of an "electronic Pearl Harbor" had a great impact on the US debate, because it constructed both 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 US. This picture of a dangerous "other" reinforces the idea of the nation as a collective self. Common 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 is, of course, the state—not the single computer user or network provider. The logical and political implication of this is that defense against cyber attacks is a task for national security policy.

In the other dimension, the "electronic Pearl Harbor"-analogy implies a structure for security policy. Because the image is taken from military history, it implies a strategy based on analogies to physical warfare. The terms "cyberwar" or "information warfare," which became popular in the mid-1990s, 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 was to be responsible for the security of the other departments' and even of the private sector's infrastructure.[32] Deputy Secretary of Defense John Hamre made this strategy more than clear on several occasions: "Cyberspace ain't for geeks, it's for warriors."[33] In his last annual report to Congress, President Clinton's Defense Secretary William Cohen described a role for the DoD in fighting cyber-terrorism as well.[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. For example, his national security advisor, Condoleezza Rice, called cyberwar "a classic deterrence mission"[35] in March 2001.

Computer Crime

The risk perception of the law enforcement agencies is structured differently. Many critics of a military involvement argued that the "electronic Pearl Harbor"—should it ever happen—would take place inside the US. Thus the Federal Emergency Management Agency (FEMA) or the FBI would be better suited for preventing such an attack or hunting down the perpetrators. Additionally, the FBI was already involved in investigating computer crime and had set up a special Computer Crime Squad in the early 1990s. On the basis of the *Computer Fraud and Abuse Act* of

1986, this unit investigated more than 200 cases until the mid-1990s and had picked up a great deal of information along the way about the practical problems of the risk. Dealing with hacker intrusions, data theft and similar things had led to a more differentiated, but also less dramatic view of the risk. One point that FBI officials frequently emphasize 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, the director of the FBI's National Infrastructure Protection Center up to March 2001.[36]

One key experience, later 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 US military, the nuclear weapons laboratories, the Department of Energy and NASA. At precisely the same time, the US forces in the Middle East were being built up because of tensions with Iraq over 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 Iraqi government had to 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 cannot respond militarily to a cyber attack as long as the attacker is not clearly identified. Then FBI director Louis Freeh 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 Attorney General Janet Reno at the Cybercrime Summit 2000.[38]

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

Economic Loss

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

Just as important as the top management's risk perception is that of the group of persons often working "in the basement," namely the system administrators and IT experts. They have to deal with hacking attempts almost daily, and for them, the problem breaks down into single, concrete challenges. They install new virus scanners on the company's network, make sure the users change their passwords on a regular basis, try to reduce the server workload during denial-of-service attacks, or restore deleted files from the backup tapes after a hacker break-in. For this technical expert community, the problem currently discussed as a "national security threat" has existed since computers first became networked. Here it is mainly seen as a technical and practical problem, less as a political issue and much less as a question of national security policy. The operative ideas are "computer security" or "IT security," not "national security." Because these experts often are the only ones in an organization who can really assess the details and challenges, their perception also influences the way the management deals with IT security.

2.2. Resources

The Military

The US armed forces are the most advanced in the world when it comes to offensive information warfare capabilities. They are intended to serve as "another arrow in the quiver"[42] in conventional military operations, but also to give the government deterrence and strike capabilities for countering a 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 US military networks.[43]

The US military has already been active in digital electronic warfare since the 1980s, when the armed services started their own research in computer viruses.[44] In the early 1990s, when the Gulf war showed the importance of information systems and communications lines for fighting a short, effective war, the development of these capabilities gained more momentum. A special School for Information Warfare and Strategy was set up at the National Defense University in 1994. The US military has had its own Joint Doctrine for Information Operations (Joint Pub. 3-13), which also covers computer network attacks on civilian infrastructures, since 1998.[45] The central coordination point for these activities, the Joint Task Force - Computer Network Attack, was set up and subordinated to US Space Command in October 2000. More units are located at the Air Intelligence Agency in San Antonio, Texas, among them the Air Force Information Warfare Center with more than 1,000 personnel and the Joint Information Operations Center.[46]

In spite of the growing interest and the great efforts made in this field, the US military has not yet acquired the capability to successfully wage a large-scale cyberwar. The few cyber-missions during the Kosovo war showed this quite clearly. The Air Force waged some cyber attacks on the Serb air defense system,[47] but afterwards came under heavy criticism for the inefficiency of these measures.[48] Cascading effects of information attacks in particular are complicated to estimate, because one not only needs the know-how and technology to get into the enemy’s computer systems, but also needs to know how they are embedded in his social organization and strategy.

Law Enforcement

The law enforcement agencies have been dealing with computers for some years now, because normal criminals tend to make more and more use of modern technologies as well. This led to the establishment of the National Computer Crimes Squad at the FBI as early as February 1992. In the same year, the Computer Analysis and Response Team (CART), a specialized unit for computer forensics, was set up. Each of the 56 FBI field offices has had its own Computer Crimes Squad since 1998.[49] The various 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 out 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 federal agents are not really prepared for their task.[50]

In spite of these difficulties, the FBI’s build-up of specialized computer units has shown some results. During the last year, some spectacular cases of hacking or computer fraud were solved within a very short time. These successes led to greater self-confidence on the part of the 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 attorney 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 local or private entities, the latter had an important role within the cyber security debate from the beginning. Only here can the technical expertise that one needs to successfully defend against an attack be found. The companies that run the systems can much more easily focus on reinforcing them than on striking back. They install firewalls, redundant emergency systems, backup facilities, and other defensive systems. With these features, they are already helping to protect the US from a large-scale cyber attack, often without viewing this as part of a national security policy strategy at all.

More importantly, the strategic resources available to the infrastructure providers include not only their staff and their firewalls, but also the virtual landscape in which a cyber attack would occur. Unlike the territorial border or the national coastline, this landscape consists of private infrastructures providing public services through the market. In a significant departure from classical territorial defense, attacks in cyberspace can only be warded off by controlling the systems of which it consists. Delegating this task to the state is difficult, if not practically impossible.

2.3. Norms

Neo-Liberalism and the ‘Californian Ideology‘

A number of strong norms have limited the efforts of the traditional security policy institutions to expand their activities into cyberspace. These norms have 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 has gained much acceptance among the elites of western societies in the 1990s, calls for minimal involvement of the state, especially in economic affairs. In the field of new technologies, two additional elements added to this approach: First, a large majority in Washington was strictly 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 invested in the digital communications media. Many expected that they would help the development of decentralized and self-organized social structures. This so-called “Californian ideology”[53] that also became popular in Washington in the mid-1990s promised an era of free and non-hierarchical association of electronically networked citizens. Within this technology-deterministic and anti-statist framework of norms, 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 centered on the question of 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 individual computer systems and their users. Here, the civil rights organizations played an important role in warning of the unintended consequences of a risk policy based on military strength or repression—mainly the resulting threat to privacy.

Military Identity and Professionalism

The idea of waging war in cyberspace seemed odd for many military officers in the first place. The term "cyberspace" implies a completely different concept of space and body, because the space in question consists only of symbols and their links. Because there are no linear distances like in the Cartesian physical expanse, there is no frontline anymore. The actors in cyberspace are not physically present, but are instead represented by symbols. In this ethereal cyberspace, there is no room for physical violence. The application and organization of physical violence, however, is still part of the professional military identity. "Any time things start to smell like something other than killing people and breaking things, people in the military start pointing in other directions" a Pentagon advisor described this.[54]

Only recently have the armed forces seemed able 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 are still debating if cyber attacks can be considered acts of war at all.[56] But if this is the case, a strategy based on electronic 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 be at odds with more important norms codified in the Hague and Geneva conventions. These international treaties, for example, prohibit perfidious or unnecessary attacks, the use of the territory of neutral states, attacks on civilian populations or weapons that do not distinguish between combatants and non-combatants.[57] The fact that the US armed forces only reluctantly made use of their cyber arsenal was partly due to these concerns. In the Kosovo war of 1999, some planned cyber attacks against Serbia did not take place because the Pentagon's own lawyers vetoed them after having studied the international legal difficulties of cyber war.[58]

US domestic law also gave the armed forces' lawyers a few headaches, because an attack on American infrastructures could originate in Iraq as well as in the US. A military counter-strike through cyberspace might therefore unwittingly lead to an operation of US 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 1980s. The most important of these is the Computer Fraud and Abuse Act of 1984, which has been amended three times since.[60] Electronic break-ins into computer systems have been treated as crimes on the basis of this Act, and the FBI quickly used this piece of legislation for building up structures able to deal with them. The domestic laws thus gave the law enforcement agencies a strong hand in fighting cyber attacks.

One of the oldest laws governing computer security, the *Computer Security Act* of 1987,[61] points in another direction. Under this provision, 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 decentralized, preparative manner.

The legal norms, in sum, prevented a more important role for the armed forces in the protection of critical infrastructures, while giving the law enforcement community new tasks. Moreover, decentralized preventive measures were already taken in the 1980s. This is reflected today in the cooperation efforts with the private sector.

3. Policy

3.1. First Studies

President Bill Clinton set up a special study group in June 1995, the Presidential Commission on Critical Infrastructure Protection (PCCIP), whose task was to deliver a comprehensive report on the security of all infrastructure systems in the US. While this brief included not only information and telecommunications networks, but the financial sector, energy supply, transportation and the emergency services as well, the main focus was on cyber risks. There were two reasons for this decision. First, these were the least known because they were so new, and secondly, many of the other infrastructures depend on data and communications 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 involvement was based on the assumption that security policy in the IT field was 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. The members of the IPTF were drawn from the state's classical security policy institutions exclusively—the FBI, the Department of Defense and the NSA.[63] Insofar the IPTF can be understood as a compromise between a completely cooperative approach—including the private sector and other departments—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 Department of Justice to make use of the Computer Investigations and Infrastructure Threat Assessment Center (CITAC), which had been set up shortly before at the FBI.[64] Obviously, the institutional resources of the FBI were a decisive factor here. A more militant approach was still an option then, as can be seen, 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 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 assembled 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 coordinates the various governmental and private sector activities. The NIPC, therefore, has a central role in the new cyber-security policy. Coordination within different high-level branches of the government has been effected by the new Critical Infrastructure Coordination Group (CICG).[66]

A number of departments act as "lead agencies", each of which is charged with the security of one sector of the infrastructure. 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 were to be run by private companies who would also determine their institutional and working procedures.[67] The close cooperation with the private sector that had begun with the PCCIP was thus continued and even enhanced. The government explicitly stressed 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]

Responsibility for cyber security policy no longer rests exclusively with the state, but also extends to private infrastructure providers. In a marked departure from the old monopoly of force, a networked self-help system has been established here that might be called post-modern. In some areas, the government still plays its traditional role through law enforcement and intelligence services, 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 had explicitly described its 1997 report as a "beginning,"[69] and the presidential directives of May 1998 also acknowledged that there was no master plan 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 current US policy with regard to the new cyber risks. The White House published a follow-up report in February 2001 after the inauguration of George W. Bush, but this document only attests to the state of the respective programs and does not include a change in strategy.[72]

The Government Only Protects Itself

The plan reinforces the perception of cyber security as a responsibility shared between the government and the private sector. The government agencies now are only responsible for protecting their own networks against intruders. Three new institutions work together for the security of the state's computer systems. The Federal Computer Incident Response Capability (FedCIRC), a part of the General Services Administration (GSA), is building a central analysis cell to investigate incidents in all of the government's non-military computer networks. For military computers, this is done by the Joint Task Force – Computer Network Defense (JTF-CND), 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 and the National Security Council in case of attacks against systems that belong to the national security apparatus.[74] The FBI's NIPC is still responsible for incident warnings, strategic analyses, and law enforcement.[75]

Within the government, we now find a decentralized and cooperative risk policy similar to the one pursued 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, however, one central protective function 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 also be subordinated to the Department of Defense by presidential order. The National Plan tried to maintain the traditional distinction between police and military by making such a decision dependent on an attack coming from abroad. But naturally, not every simple hacking attempt that does not originate in the US should trigger a response by the Department of Defense. The decisive criterion for differentiating between war and crime is therefore 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 sensory 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 judgment of law enforcement agencies and even private infrastructure service providers. In the case of the new cyber risks, it is hard to differentiate between domestic and international security. The de-territorialized cyber-security policy blurs the line between war and crime, and the institutional responsibilities for a government response against an attack have to be established on a case-by-case basis.

Privatization of Cyber Security

The second part of the National Plan deals with the security of privately run infrastructures. It starts by stating that "the Federal Government alone cannot protect US critical infrastructures."[77] The state and local governments are also called "partners" of the federal government, but the emphasis is placed on private companies. The goal is a close private-public partnership. To ease concerns of the infrastructure service providers, the plan goes at great lengths to emphasize fundamental principles like "voluntary" cooperation or "trust" and safeguarding the companies' own interests through protective measures.[78] The government tries to make them accept its offers to check their defenses, to share information, and to further develop technical standards. Existing institutions like the North American Electric Reliability Council (NERC) are cited as good examples of this sort of cooperation.[79]

The private sector, though, is still very hesitant. The Information Sharing and Analysis Centers (ISACs) that were already planned in the 1998 Presidential Decision Directive were set up with considerable delay, and in some sectors do not exist at all to this day. The Financial Services ISAC (FS/ISAC), the first of these centers, was only set up on 1 October 1999, almost one and a half years after the presidential directives, and the IT-ISAC only started operations in March of 2001. Other sectors do not have this kind of coordination centers to this day. Besides the old NERC, there is only 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 achieving more.[81] President Clinton even signed an executive order in the summer of 1999 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 major IT companies.[82] It was finally set up in January 2001, one day before Bill Clinton left office.[83]

Many companies do not see any necessity for working 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 aid in tackling the new risks related to computer security. The NIPC in particular was subjected to heavy criticism after it failed to respond quickly to some E-mail worm infections in 2000 and 2001.[84] A lot of companies prefer contracting private IT security service providers, as they work faster and less bureaucratically than government agencies. These specialized IT security companies are increasingly taking on the role of traditional risk management consultants.[85]

Until an “electronic Pearl Harbor” occurs, we cannot expect the private sector to develop a keen interest in a more prominent role of the government in IT security. Instead of centralized coordination by the state, almost all the companies require private, local security instruments provided by the market.

4. Conclusions

Since the early 1990s, the debate about hacker attacks against the US has made its way from specialized expert circles to the agenda of “high politics” and national security. This in itself 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 crystallized. Instead, the risk communication started at the last corner of the triangle, the capabilities. Here we can note something special: The potential for damage to critical infrastructures was not created by the introduction of weapons or other dangerous tools, but by the socio-technical structure of the US itself.

Until the mid-1990s, 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 different actors in different institutions and cultures, who promoted them using different resources and calling upon different norms.

According to the basic tenets 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 dramatization 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 means and approaches. The political treatment of issues such as the "war on drugs" or "counter-terrorism" is a case in point where the threat assessment was given 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 military diction chosen in the early stages of the discourse could not be transformed into a similarly militant strategy. The outcome of ten years of discussion and almost five years of reforms, presented by 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, meaning the preventive protection of critical infrastructures by technical means.

The study has shown the over-determination of this predominantly civilian and cooperative outcome. Strong restrictions against a military-interventionist strategy existed in the dimensions of perception as well as of resources 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 emphasized their view of the risk as "computer crime," while on the other hand, and more importantly, the private sector running the infrastructures perceived the risk as consisting primarily of a local, technical problem or as economic costs. Therefore, the debate on cyber risks is an example of a failed "securitization."[87] The security policy institutions only partly managed to extend the concept of "security" in this case, because it was impossible to achieve a consensus between the different groups on what the word should refer to. Similar to the regulation of cryptography,[88] the debate centered on the question: Does "security" mean the security of the American society as a whole—"national security"—or the security of individual users or technical systems? Implicitly, this security policy discourse dealt with the relationship between the state and its citizens.

The distribution of *resources*, the technical and social means for countering the risk, was also important and had an impact on the discourse. Because the technology generating the risk makes it very difficult to fight potential attackers in advance, in practice, the measures taken focused on preventive strategies and on trying to minimize the impact of an attack when it occurs. Here, the infrastructure providers with their preference for decentralized and private approaches were in a strong position, because at the end of the day, only they are able to install the technical safeguards for IT security at the level of individual infrastructures.

Norms were also important in selecting the strategies. Cultural norms like the new economy's anti-statist "Californian ideology," as well as legal restrictions, prohibited a bigger role of the state, especially of the armed forces. The interventionist mindset of the security policy community gained hardly any acceptance. On the contrary, there was even much hesitation within the armed services concerning 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 choice of strategies. This also reflects the Clinton administration's policy of preferring economic ideas over security policy—prominently featured in the president's famous quote: "It's the economy, stupid!" Besides these cultural differences with regard to strategy, legal norms also obviated a more military strategy. The difficulties in determining whether cyber attacks constitute an act of war, the fear of committing war crimes by conducting electronic counter strikes, and the injunction against using the armed forces domestically made the Pentagon hesitate to build up its own information warfare units. On the other hand, the cyber-crime laws that had already existed since the 1980s 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 varying degree to which resources are 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 result of cultural and legal norms, because they restrict the number of potential strategies available for selection.

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 militarization of cyber security policy will be very difficult in a liberal society with private infrastructure providers. From the American experience, we should rather conclude that “cyberwar” is a fundamentally inadequate term that disrupts the discussion on useful risk policy more than it contributes.

Notes:

[1] Ralf Bendrath, “Homeland Defense, virtuelle Raketenabwehr - und das schnöde Ende einer Medienhysterie,” *telepolis* (28 March 2001). Available @ http://www.telepolis.de/deutsch/special/info/7234/1.html.

[2] Ulrich Beck, *Risikogesellschaft. Auf dem Weg in eine andere Moderne* (Frankfurt/M.: Suhrkamp Verlag, 1986), 73, translation by R.B.

[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 Acquisition & Technology 1996, *Report of the Defense Science Board on Information Warfare-Defense* (Washington, D.C., 1996), A-1.

[4] For the origins of this term, see George Smith, “Electronic Pearl Harbor,” *Crypt Newsletters´s Guide to Tech Terminology* (2001). Available @ http://sun.soci.niu.edu/~crypt/other/harbor.htm with many references.

[5] President’s Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations. Protecting America’s Infrastructures* (Washington, D.C., 1997), 14.

[6] Christopher Daase, Susanne Feske and Ingo Peters, eds., *Internationale Risikopolitik* (Baden-Baden: Nomos Verlagsgesellschaft, forthcoming 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.

[9] Department of Defense: News Briefing, 04/16/1998.

[10] Niall McKay, “Cyber Terror Arsenal Grows,” *Wired News* (16 October 1998). Richard Aldrich, Staff Judge Advocate of the Air Force Office of Special Investigations (AFOSI), in his presentation at the InfowarCon in Washington on September 6, 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] Richard A. Clarke, *Memorandum. Implementation of PDD 63 through Project Matrix*, Critical Infrastrucutre Assurance Office (Washington, D.C., 19 July 2000)

[12] The President's Commission on Critical Infrastructure Protection (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, … [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," 5.

[13] John J. Hamre and John H. Campbell, *Statement of the Honorable John J. Hamre (Deputy Director 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* (11 June 1998).

[14] Robert H. Anderson and Anthony Hearn, *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After ... in Cyberspace II"* (Santa Monica: RAND, 1996); Roger C. Molander, Andrew Riddile and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica: RAND, 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.

[16] John Deutch, *Foreign Information Warfare Programs and Capabilities, Testimony to the U.S. Senate Committee on Governmental Affairs; Permanent Subcommittee on Investigations* (25 June 1996).

[17] White House, Presidential Decision Directive/NSC-63, *Critical Infrastructure Protection*, 1998.

[18] Kenneth A. Minihan, *Prepared statement by Lt. Gen. Kenneth A. Minihan, Director, National Security Agency, before the Senate Governmental Affairs Committee* (24 June 1998), my emphasis.

[19] John A. Serabian, Jr., *Statement for the Record before the Joint Economic Committee on Cyber Threats and the U.S. Economy* (23 February 2000).

[20] Timothy L. Thomas, *Russian and Chinese Views of Information Warfare*, Workshop at the InfowarCon in Washington, D.C. (7 September 2001).

[21] John Arquilla, David Ronfeldt and Michele Zanini, "Networks, Netwar, and Information-Age Terrorism," in Lesser, Ian O., Bruce Hoffmann, John Arquilla, David Ronfeldt and Michele Zanini, eds., *Countering the New Terrorism* (Santa Monica: RAND, 1998), 39-84.

[22] George Smith, "Electronic Pearl Harbor."

[23] Serabian, *Statement for the Record*.

[24] Louis J. Freeh, *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* (16 February 2000).

[25] Johan J. Ingles-le Nobel, "Cyberterrorism Hype," *Jane's Intelligence Review* (21 October 1999).

[26] CNN, "Cyberspace Attacks Threaten National Security, CIA chief says" (25 June 1996).

[27] Madsen, Wayne, "Teens a Threat, Pentagon Says," *Wired News* (02 June 1998).

[28] George Smith, "Electronic Pearl Harbor."

[29] Infowar enthusiast Winn Schwartau, who coined the term more than ten years ago, recently even wrote a novel titled *Pearl Harbor.Com.*

[30] Then Deputy Secretary of Justice Jamie Gorelick, in ABC Nightline 199, "Cyber Terror - A Consequence of the Revolution," 12/07/1997, transcript available @ http://www.infowar.com/CLASS_3/class3_011298a.html-ssi.

[31] President's Commission on Critical Infrastructure Protection 1997, passim.

[32] Office of the Under Secretary of Defense for Acquisition & Technology, 1996, 6-7.

[33] Inside the Army, 22.4.1999, quoted in George Smith, "Eligible Receiver," *Crypt Newsletter´s Guide To Tech Terminology*, http://www.soci.niu.edu/~crypt/other/eligib.htm.

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

[35] Quoted in Kevin Poulsen, "Hack Attacks Called the New Cold War," *The Register* (23 March 2001).

[36] Quoted in McKay, "Cyber Terror Arsenal Grows."

[37] Freeh, *Statement of the Director Federal Bureau of Investigation*.

[38] Janet Reno, *A Law Enforcement/Information Technology Industry Dialogue on Prevention, Detection, Investigation and Cooperation*, Speech at the Cybercrime Summit, Stanford, CA (05 April 2000).

[39] Richard Power, "2000 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues & Trends* 1 (2000).

[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, Computer Crime and Security Survey, 13.

[41] Martha Mendoza, "Valley Cool to Reno Cybercrime Plan," *L.A. Times* (06 April 2000).

[42] Then Commander of U.S. Space Command and now Chairman of the Joint Chiefs of Staff, General Richard B. Myers, quoted in "Space Command Readies For Infowar," *United Press International* (05 January 2000).

[43] Jim Garamone, "Hamre "Cuts" Op Center Ribbon, Thanks Cyberwarriors," *American Forces Press Service* (11 August 1999).

[44] Bradley Graham, "In Cyberwar, A Quandary Over Rules And Strategy," *International Herald Tribune* (09 July 1998).

[45] Joint Chiefs of Staff, Joint Pub. 3-13, *Joint Doctrine for Information Operations* (Washington, D.C., 9 October 1998).

[46] For an overview see Ralf Bendrath, "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).

[47] Elizabeth Becker, "Pentagon Sets Up New Center for Waging Cyberwarfare," *New York Times* (8 October 1999).

[48] Dan Verton, "DoD Redefining Info Ops," *Federal Computer Week* (29 May 2000).

[49] Charles L. Owens, *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 (19 March 1997).

[50] Suro, Roberto, "FBI Cyber Squad Termed Too Small for Hacker Threat," *Washington Post* (7 October 1999).

[51] Quoted in PC World, "Feds To Net Criminals: You Can't Hide," *PC World* (6 September 2000).

[52] United States Internet Council, *State of the Internet 2000* (Washington, D.C.: 2000).

[53] Barbrook, Richard and Andy Cameron, "Die kalifornische Ideologie," *telepolis* (5 February 1997), http://www.heise.de/tp/deutsch/inhalt/te/1007/1.html.

[54] Quoted in John Carlin, "A Farewell to Arms," *Wired* 5, 5 (1997).

[55] U.S. Space Command, *U.S. Space Command Takes Charge of Computer Network Attack*, Press Release No. 15-00 (29 September 2000).

[56] For a skeptical position, see Richard W. Aldrich, "The International Legal Implications of Information Warfare," *Airpower Journal* 10, 3 (1996): 99-110; for the opposite interpretation see Thilo Marauhn and Torsten Stein, "Völkerrechtliche Aspekte von Informationsoperationen," *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht,* 60: 1, 1-40 (2000: 3-6).

[57] Aldrich, "The International Legal Implications of Information Warfare," 104-109.

[58] Associated Press, *Pentagon Ponders Legality of Cyber Weapons* (9 November 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.

[60] 18 U.S. Code § 1030, amended 1986, 1994 and 1996, see United States Congress, *Report of the Senate Committee on the Judiciary on the National Information Infrastructure Protection Act* (Washington, D.C.: 1996).

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

[62] White House, Executive Order 13010: Critical Infrastructure Protection (15 July 1996).

[63] Ibid.

[64] John S. Tritak, *Statement before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information* (6 October 1999).

[65] PCCIP 1997.

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

[67] Ibid.

[68] National Security Council, White Paper. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (Washington, D.C., 1998).

[69] PCCIP 1997, 101.

[70] White House 1998, 3.

[71] White House, *Defending America´s Cyberspace. National Plan for Information Systems Protection Version 1.0. An Invitation to a Dialogue* (7 January 2000).

[72] White House, *Federal Critical Infrastructure Protection Activities* (22 February 2001).

[73] White House 2000, 39-42.

[74] Ibid., 49.

[75] Ibid., 42.

[76] Ibid.

[77] Ibid., 104.

[78] Ibid., 106.

[79] Ibid., Chapter 5.

[80] For an overview see Bendrath, Homeland Defense.

[81] White House 2000: Chapter 5.

[82] IPartnership, *President Forms Infrastructure Assurance Council* (15 July 1999).

[83] Diane Frank, "IT Firms Unite to Share Security Info," *Federal Computer Week* (17 January 2001).

[84] Jim Wolf, "US cyber security center lags on threat warnings – GAO," *Reuters* (22 May 2001).

[85] Roberto Ceniceros, "More Consultants Offering Technical Help to Ensure Security," *Business Insurance* (3 April 2000).

[86] Daase, Internationale Risikopolitik.

[87] Ole Wæver, "Sicherheit und Frieden: Erweiterte Begriffe, engere Freiräume für Politik?," *antimilitarismus information* 25, 11, pp. 47-53.

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

RALF BENDRATH has studied physics and political science in Bremen and Berlin and currently is working on his doctoral dissertation about "Information Warfare in the USA." Since 1999, he maintains the German E-mail discussion list "Infowar.de." He is a founding member of the German-Austrian Research Group Information Society and Security Policy (Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik, FoG:IS) and a frequent contributor to the online magazine "telepolis." In 2000-2001 he was a visiting scholar at the Center for International Science and Technology Policy at George Washington University in Washington D.C. *E-mail*: bendrath@zedat.fu-berlin.de.