INTERNATIONAL TELECOMMUNICATION UNION

WSIS Thematic Meeting on Cybersecurity

Geneva, 28 June – 1 July 2005

Document: CYB/05
10 June 2005

A COMPARATIVE ANALYSIS OF CYBERSECURITY INITIATIVES WORLDWIDE

June 2005

The paper was prepared by Myriam Dunn, Center for Security Studies, Swiss Federal Institute of Technology (ETH Zurich) for the WSIS Thematic Meeting on Cybersecurity.

ABSTRACT

The worst possible consequences of risks created by information and communication technologies manifest themselves in the possible failure of so-called critical infrastructures, which are systems and assets whose incapacity or destruction would have a debilitating impact on the national security and the economic and social well-being of a state. Driven by a growing concern for the potential vulnerability of networked societies together with an increasing number of disruptions in the cyber-domain, many countries have taken steps to better understand the vulnerabilities of and threats to their (information) infrastructure, and have proposed measures for the protection of these assets. This paper investigates national cybersecurity initiatives in order to identify common themes and best practices, but especially problems and pitfalls for a global culture of cybersecurity. In the first chapter, we look at how the topic of cybersecurity has made it onto the security political agenda and what the characteristics of cyber-threats are. Second, we describe how various governments approach the issue and focus on common issues and problems. We aim to explain differences and similarities in national approaches by applying political science theory to the topic. Third, we look at how the topic is approached internationally and uncover two fundamentally opposed paradigms that could pose considerable difficulties for the development of a global culture of cybersecurity. In doing so, we hope to point out the major hazards on the long road to a global culture of cybersecurity.

ABBREVIATIONS

CERT	Computer Emergency Response Team
CI	Critical infrastructures
CII	Critical information infrastructures
CIIP	Critical information infrastructure protection
CIP	Critical infrastructure protection
CNO	Computer Network Operations
CoC	Council of Europe's Cybercrime Convention
DDOS	Distributed Denial of Service
EMP	Electromagnetic Pulse
G8	Group of Eight
GII	Global information infrastructure
HERF	High Energy Radio Frequency
HPM	High Power Microwave
ICT	Information and communications technology
ISAC	Information Sharing and Analysis Center
IT	Information technology
PCCIP	Presidential Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
R&D	Research and Development
WGIG	UN Working Group on Internet Governance
WSIS	World Summit on the Information Society

TABLE OF CONTENTS

1 INTRODUCTION

> Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. A global culture of cybersecurity needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies.[1]

This statement from the 2003 WSIS Declaration of Principles, restated in two succeeding UN resolutions,[2] reflects the strong belief that confidence and security are two of the main pillars of the Information Society.[3] But how are we to get there? How can a global culture of cybersecurity be fostered? The WSIS Plan of Action proposes to reach that goal mainly by promoting cooperation among governments and by getting them, in close cooperation with the private sector, to prevent, detect, and respond to cyber-crime and the misuse of information and communication technologies (ICTs) by developing guidelines and considering legislation, by strengthening institutional support, and by encouraging education and raising awareness.[4]

According to this plan, the onus is on nation-states, even though a strong role of the private sector is acknowledged and called for.[5] And indeed, the security of cyberspace has become an important consideration in most countries, and governments worldwide are already putting a fair amount of effort into cybersecurity. But how does the national become global or, to put it differently, how can we move from these national approaches to a global culture? Is there some common denominator to aim for? Or is there already a global culture of cybersecurity, at least in a rudimentary form? With these questions in mind, this paper investigates national cybersecurity initiatives in order to identify common themes, best practices, but especially problems and pitfalls for a future global culture of cybersecurity.

1.1 Setting the stage: cybersecurity in the past and present

Contrary to widespread belief, concerns about cybersecurity are not a phenomenon of the 1990s. Viruses and worms have been part of the background noise of cyberspace since its earliest days. In the 1986 movie *War Games*, a young teenager hacks his way into the computer that handles command and control for the US nuclear arsenal. The famous Cuckoo's Egg incident in the mid-1980s raised awareness that foreign spies had found new ways to obtain highly classified information.[6] So what is new? On the one hand, the technological environment and substructure is new: Since the early 1990s, information technology has evolved from modest use of mainly stand-alone systems in closed networks to the development of the Internet and other networks connecting businesses, governments, consumers, and any "wired" individual or organization. Access devices have multiplied and diversified to include a variety of portable and wireless accesses. The numbers are telling:[7] According to statistics, there were 21'000 reported virus incidents in 2000. Three years later, the number was more than six times higher.[8] In 2002, the worldwide damage done by worms and viruses was estimated at US$45 billion; August 2003 alone saw costs of almost the same magnitude.[9]

Even if we are highly sceptical about the usefulness and accuracy of statistics, we can also identify a qualitative difference in addition to a quantitative increase in cyber-incidents. This qualitative difference concerns the gravity of the threat: In the mid-1990s, the issue of cybersecurity was catapulted onto the security political agendas when it was persuasively linked to both terrorism and critical infrastructure protection. During that time, it was established that key sectors of modern society, including those vital to national security and to the essential functioning of industrialized economies, rely on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation. This critical information infrastructure (CII) underpins many elements of the critical infrastructure (CI), as many information and communication technologies (ICT) have become all-embracing, connecting other infrastructure systems and making them interrelated and interdependent.

Not only are information systems exposed to failures, they are also potentially attractive targets for malicious attacks. The CI delivers a range of services that individuals, and society as a whole, depend on. Any damage to or interruption of the CI causes ripples across the technical and societal systems ─ a principle that has held true in the past, and even more so today due to much greater interdependencies. Attacking infrastructure therefore has a "force multiplier" effect that allows even a relatively small attack to achieve a much greater impact. For this reason, CI structures and networks have historically proven to be appealing targets for a whole array of actors.[10]

Driven by a growing concern for the potential vulnerability of networked societies and by the increasing number of disruptions in the cyber-domain, many countries have taken steps to better understand the vulnerabilities and threats that their (information) infrastructure is subject to, and have proposed measures for the protection of these assets. For fourteen countries, such protection policies have been compiled in a recent publication constituting a substantive collection of material that can be used as a starting point for more in-depth research.[11] Despite the sometimes substantial differences between these governmental protection policies, they offer a wealth of empirical material from which a variety of lessons can be distilled for the benefit of the international community.

Apart from being interested in common issues across the board, we are also interested in explaining similarities and differences. In addition to the fact that different countries have different ideas about cybersecurity policies, the issue has undergone a change on the agenda of various countries since cybersecurity became an issue in the 1980s. This phenomenon is interesting in our context because by better understanding the mechanisms behind national initiatives, we can derive statements about a framework for a global culture. We claim that countermeasures (cybersecurity initiatives and policies) are the outcome of a process called threat politics ─ a political process by which threats are introduced to and removed from the political agenda, or by which the face of threats on the political agenda is altered.[12] In short, there is no cybersecurity without cyber-threats, or, put differently, we should never look at countermeasures without taking into consideration the threat and especially the perception of the threat by key decision-makers. In this approach, the outcomes of a political process and the nature of countermeasures can be understood by analysing influential actors, their threat perceptions, and institutional settings, namely rules, norms, habits, and resources.[13]

Before we set out to see how the topic of cybersecurity was introduced to the security political agenda in the 1990s and study the particular features of the issue, we believe it is essential to talk about definitions, because we believe that one prerequisite for developing a global culture of cybersecurity is a common understanding of what "cybersecurity" and the related terms actually signify.

1.2 What is cybersecurity? Striving for a definition

The vocabulary of clichés that inhabits the information-age debate, and the overall imprecision in terminology, obstruct meaningful analysis. There are three essential elements in the semantics of the information age: "information", "cyber", and "digital", all three of which are so important that they have become shorthand expressions for the age we live in. The information-age vocabulary is created by simply placing these prefixes before familiar words, thus creating a whole arsenal of new expressions. The nature of these terms is such that their meaning has never been precise – nowadays, however, they have been used so extensively that they can basically mean everything and nothing. To put it mildly, we are bogged down in a "definition quagmire" in terms of information-age vocabulary.[14]

The fuzziness of the terminology could be a problem in the context of developing a global culture of cybersecurity to the extent that it diminishes the ability of different stakeholders to reach agreement on elements of this culture. In particular, there is no generally accepted definition of cybersecurity, and several different terms are in use that have related meanings, such as information assurance, information or data security, or critical information infrastructure protection. Then again, because information technology continues to evolve rapidly, an overly rigid definition would likely lose its usefulness quickly, so that keeping the concept as flexible as possible may be beneficial. In order to at

least clarify some of the basics, we will look at the two semantic elements of cybersecurity separately: "cyber" and "security", both being inherently fuzzy concepts.

Cyber

"Cyber-" is a prefix derived from the word "cybernetics" and has acquired the general meaning of "through the use of a computer". Cybernetics is the theory of communication and control of regulatory feedback that studies communication and control in living beings and in the machines built by humans,[15] and is the precursor of complexity thinking in the investigation of dynamic systems, using feedback and control concepts. The "cyber-" prefix is often used synonymously with "cyberspace".

"Cyberspace", though being one of the most pervasive terms of the information age vocabulary, is just as notoriously fuzzy as the rest of the information-age vocabulary. It is well known that the term was created by W. Gibson in his cyberpunk novel "Neuromancer"[16] and was first used to refer to the Internet in 1991.[17] The term "cyberspace" as it is used today connotes the fusion of all communication networks, databases, and sources of information into a huge, tangled, and diverse blanket of electronic interchange. Thus, a "network ecosystem" is created, a place that is not part of the normal, physical world. It is "virtual", a "bioelectronic environment that is literally universal, that exists wherever there are telephone wires, coaxial cables, fiber-optic lines or electromagnetic waves. This environment is inhabited by knowledge, existing in electronic form".[18] Virtually any element of cyberspace can be at risk, and the degree of interconnection of those elements can make it difficult to determine the extent of the security measures needed.[19]

Security

"Security" is a vast topic that includes the security of countries from military or terrorist attack, the security of computers from crackers, home security from burglars and other intruders, financial security from economic collapse, and many other related situations. In our context, we must be concerned with two different concepts of security: one technical, and one that encompasses the security of entire nations.

The word "security" in general usage is synonymous with "being safe", but as a technical term "security" means not only that something is secure, but that it has been secured. For example, in telecommunication, the term "security" has the following meaning: A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.[20] "National security", on the other hand, can be defined in an objective sense as the absence of threat to a society's core values, and in a subjective sense as the absence of fear that these values will be attacked.[21] It also describes the measures taken by a state to ensure its survival and general well-being.

Therefore, the two notions do not differ in their core: both connote a condition that is free of (real or imagined) danger. However, they differ in scope and they differ in their so-called "referent object", or the thing they aim to protect: While the security of information systems is, in its pure form, concerned with technical measures such as firewalls to ensure that information flows as it should, national security measures include the maintenance of armed forces, the maintenance of intelligence services to detect threats, and civil defence measures and emergency preparedness to ensure safety and freedom.[22] However, with the advent of cybersecurity on the security policy agenda, the two notions merge. National security today is also concerned with attempts to create resilience and redundancy in national infrastructure through cybersecurity measures, or with the protection of classified information.[23] This means that measures that are generally regarded as being within the purview of information security may now also be included among measures to ensure national security.

Cybersecurity

Joining the two words together again, cybersecurity is concerned with making cyberspace safe from threats, namely cyber-threats. The notion of "cyber-threats" is rather vague and implies the malicious use of information and communication technologies (ICT) either as a target or as a tool by a wide range of malevolent actors.[24] As commonly used, the term "cybersecurity" refers to three things:[25]

1. A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to the national security;
2. The degree of protection resulting from the application of these activities and measures;
3. The associated field of professional endeavour, including research and analysis, aimed at implementing and those activities and improving their quality.

Cybersecurity is thus more than just information security or data security, but is nevertheless closely related to those two fields, because information security lies at the heart of the matter. Information security refers to all aspects of protecting information. Most often, these aspects are classified in three categories: confidentiality, integrity, and availability of information.[26] "Confidentiality" refers to the protection of the information from disclosure to unauthorized parties, while "integrity" refers to the protection of information from being changed by unauthorized parties. "Availability" means the information should be available to authorized parties when requested. Sometimes, "accountability", or the requirement that the actions of an entity be uniquely traceable to that entity, is added to the list.[27]

Historically, up to about 1990, confidentiality was the most important element of information security, followed by integrity, and then availability.[28] By 2001, changing usage patterns, the increase of outside attacks, and expectation patterns had moved availability to the top of most versions of this priority list. The first goal of modern information security has, in effect, become to ensure that systems are predictably dependable in the face of all sorts of malice, and particularly in the face of denial-of-service attacks.[29] This again shows us how important it is to take into account the perceptions of threats in connection with countermeasures.

In the first chapter, we will look at how the topic of cybersecurity entered the security political agenda and discuss the characteristics of cyber-threats. Secondly, we will describe how various governments approach the issue, and focus on common issues and problems that will become apparent from a comparison of these initiatives. In particular, we aim to explain differences and similarities in national approaches by applying political science theory to the topic. Third, we look at how the topic is approached in the international arena and uncover two fundamentally opposed paradigms that could pose considerable difficulties for the development of a global culture of cybersecurity.

2 THE TOPIC OF CYBERSECURITY ENTERS THE SECURITY POLICY AGENDA

The cybersecurity debate as we know it today originated in the US in the mid-1990s, from where it subsequently spread to other developed countries and manifested itself on security policy agendas in a variety of forms.[30] The topic is a product of two recent developments: On the one hand, it is inextricably linked to the so-called information revolution, which is about the dynamical evolution and propagation of information and communication technologies into all aspects of life and the integration of these technologies into a multimedia system of communication with global reach.[31] Certain characteristics of this technological development, especially the obvious and inherent insecurity of digital networks, have had a decisive impact on how we perceive and react to cyber-threats.

On the other hand, the rise of cyber-threats can be seen as a child of the major reorientation of security policies that took place after the end of the Cold War. As old security problems declined, governments turned to advisors, specialists, analysts, and researchers not only for advice on policy alternatives, but also to help identify new challenges and problems, which led to the addition of a multitude of "new" issues to the security agendas.[32] This development was driven by concerns in the US defence community that its enormous conventional military dominance would force any kind of adversary – states or sub-state groups – to use asymmetric means, such as weapons of mass destruction, information operations, or terrorism against the US.[33] With the rapid spread of ICT on the global

marketplace, the resulting "free-for-all" access to information weapons, and the increasing dependency of modern societies on ICT, the fear of asymmetrical vulnerabilities was heightened exponentially. It was feared that an enemy who could never win a battle against America's mighty high-tech war machine in any conventional conflict might instead strike at vital points in the US, either at a physical location or in cyberspace.

In a nutshell, the perception of cyber-threats therefore has two main aspects: A new kind of vulnerability due to modern society's dependency on inherently insecure information systems on the one hand, and the expansion of the threat spectrum, especially in terms of malicious actors and their capabilities, on the other. In this chapter, we want to explore these issues in some more detail: In a first subchapter, we will address the technological subsystem and its apparent and inherent insecurity, and then discuss how the issue is linked to the critical infrastructure protection debate. Third, we will examine the threat side of the equation before we characterize the cyber-threat.

2.1 The apparent insecurity of the networked global information infrastructure

Some argue that the beginnings of the current information revolution go back to the invention of the telegraph,[34] but it was only in the early 1990s that a confluence of events brought about what can be described as a "techno-crescendo" of information revolution dreams, when computers became popular with the masses, and knowledge workers began to outnumber factory workers.[35] One of the most noteworthy features of this more recent technological environment is the tendency towards "connecting everything to everything", thus creating vast open networks of different sizes and shapes.

From their modest beginnings some twenty years ago, computer networks have become a pivotal element of modern society,[36] and in a more abstract sense, the "network" has become a metaphor for many aspects of modern life.[37] The marriage of computers and telecommunications, and the worldwide linkage of systems such as advanced computer systems, databases, and telecommunications networks that make electronic information widely available and accessible – sometimes called global information infrastructure (GII) – is, in fact, what made the current revolution into a mass phenomenon of such grand proportions.

However, it is not that easy to understand what the information infrastructure is exactly, even on a small scale. This is due to the fact that it not only has a physical component that is fairly easily grasped – such as high-speed, interactive, narrow-band, and broadband networks; satellite, terrestrial, and wireless communications systems; and the computers, televisions, telephones, radios, and other products that people employ to access the infrastructure – but also an equally important immaterial, sometimes very elusive (cyber-) component, namely the information and content that flows through the infrastructure, the knowledge that is created from it, and the services that are provided on that basis.[38] In addition, the tools of the information revolution are rapidly advancing and changing, even though the burst of the dot-com-bubble has considerably dampened the hyper-tech-euphoria of the late 1990s. Experts tend to agree that the major technological trends of the future are automation; mobility; miniaturization, global networking, and increasing ubiquity of computing and networking,[39] which will reinforce existing trends, but also create new ones. In our context, the security implications of this are of special interest. As mentioned above, since cyber-threats are about the malicious use of the (global) information infrastructure, the (current and future) characteristics of the technological environment have a considerable impact on the perception of the threat. In particular, the increasing disruptive occurrences in the cyber-domain, together with the Microsoft monoculture on operating systems that show persistent security flaws, have led to the impression that the IT world has a severe security problem.

The best-known and also most influential network today is "the Internet". It has been called the pulse, the bloodstream, and the essence of the information revolution, vibrantly radiating the "suggestive power of virtual technologies",[40] and its unprecedented boom and phenomenal growth rate have made it the most popular and most amazing manifestation of ICT. As the key component of the networked global information infrastructure, the Internet can serve as a showcase for the inherent insecurity of the technological environment. As every computer that is connected to a larger part of the global

information infrastructure becomes part of the Internet, this insecurity weighs particularly heavy, as every such machine becomes, in theory, susceptible to attack and intrusion. It was also due to the extensive and widespread dependence on the Internet, or at least the perception thereof, that new attention has been given to the importance of information to national security in the first place.[41]

In order to understand the inherent insecurity of the Internet, a historical detour is most enlightening. As is well known, the Internet began in the 1960s as the ARPANET (Advanced Research Projects Agency Network), a US Department of Defense project to create a nationwide computer network that would continue to function even if a large portion of it were destroyed in a nuclear war or natural disaster. During the next two decades, the network that evolved was used primarily by academic institutions, scientists, and the government for research and communications. Nevertheless, all the early network protocols that now form part of the Internet infrastructure were designed for openness and flexibility, not with security in mind, even though recognition of the inherent vulnerabilities date back at least to 1988, when a student called Morris created a worm that invaded ARPANET computers and disabled roughly 6'000 computers by flooding their memory banks with copies of itself.[42]

In the early 1990s, the nature of the Internet changed significantly when the US government pulled out of network management and commercial entities began to offer Internet access to the general public for the first time, in a development that coincided with the advent of increasingly powerful, yet reasonably-priced personal computers with easy-to-use graphical operating systems. The commercialization of the Internet contributed to a considerable degree towards making the network inherently insecure, because there are significant market-driven obstacles to IT-security: There is no direct return on investment, time-to-market impedes extensive security measures, and security mechanisms often have a negative impact on usability,[43] so that security is often sacrificed for functionality.

Beyond the various governing boards that work to establish policies and standards, the Internet is bound by few rules and answers to no single organization. The Internet is therefore a primary example of an unbounded system, and as such is characterized by distributed administrative control without central authority, limited visibility beyond the boundaries of local administration, and a lack of complete information about the network.[44] While certain conventions exist that allow the parts of the Internet to work together, there is no global administrative control to assure that these parts behave according to these conventions.[45]

Another factor that contributes to the vulnerability of the Internet is the rapid growth and use of the network, accompanied by rapid deployment of network services involving complex applications. Often, as seen above, these services are not designed, configured, or maintained securely. In addition, it is believed that the security problems of the technical subsystems of today will be further aggravated in the future. It is clear already that the characteristics of the emerging information infrastructure will differ considerably from those of contemporary structures. We are facing an ongoing dynamic globalization of information services, which in connection with technological innovation, as described shortly above, will bring about a dramatic increase of connectivity and complexity of systems, leading to ill-understood behaviour of systems, as well as barely understood vulnerabilities.[46] Not only will the GII likely provide constant connection through multiple devices embedded in all aspects of business, public, and personal life – and thus become not only inter-dependent, but rather super-dependent[47] – but the mutual interaction between systems and networks will also continue to increase, thus creating ever more complex structures. The more complex an IT system is, however, the more bugs it contains – and the more complex an IT system is, the more difficult it becomes to control or manage its security.[48]

2.2 … and the link to the critical infrastructure protection debate in the 1990s

Technological insecurity in isolation would most likely not cause the same degree of concern across such a variety of actors in a variety of policy fields, were it not for our dependency, or more precisely, the complete dependency of our society on these technologies, which makes technological insecurity a

potential threat to the functioning of highly-developed societies. This is why the cyber-threat debate needs to be seen in the larger context of critical infrastructure protection (CIP).

CIP as a policy issue has risen to the top of the security agendas of many countries in the last couple of years. It is clear that protection concepts for strategically important infrastructures and objects have been part of national defence planning for decades, though at varying levels of importance. Towards the end of the Cold War and for a couple of years thereafter, however, the possibility of infrastructure discontinuity caused by attacks or other disruptions played a relatively minor role in the security debate – only to gain new impetus around the mid-1990s,[49] mainly due to the information revolution. The US, due to, among other factors, its leading role as an IT-nation, was the first state to address the problem of CIP in earnest. This new interest in infrastructure protection was augmented by the enhanced threat perception after the Oklahoma City bombing of 1995.

After the attack on the Alfred P. Murrah Federal Building in Oklahoma City, government officials realized that the loss of a seemingly insignificant federal building, outside the "nerve centre" of Washington, was able to set off a chain reaction that impacted an area of the economy that would not have normally been linked to the functions of that federal building. The idea was that, beyond the loss of human lives and physical infrastructure, a set of processes controlled from that building was lost as well (i.e., a local bureau of the FBI, a payroll department, etc.), with a hitherto unimaginable impact on other agencies, employees, and/or the private sector down the supply chain and far away from the physical destruction of the building. This made clear that interdependency between infrastructures and their vulnerability were major issues.

One direct outcome of the Oklahoma City bombing was Presidential Decision Directive 39 (PDD-39), which directed the Attorney-General to lead a government-wide effort to re-examine the adequacy of the available infrastructure protection. As a result, Attorney-General Janet Reno convened a working group to investigate the issue and report back to the cabinet with policy options. The review, which was completed in early February 1996, particularly highlighted the lack of attention that had been given to protecting the cyber-infrastructure of critical information systems and computer networks. Thus, the topic of cyber-threats was linked to the topics of critical infrastructure protection and terrorism. Subsequently, President Bill Clinton started to develop a national protection strategy with his Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996, and the issue has stayed on a high priority ever since. In a clear case of policy diffusion by imitation,[50] numerous countries have drafted protection policies of their own.

In this debate, certain forms of infrastructure are deemed more essential than others. It is believed that if any of these elements ceases to function for a prolonged period, society will be hard pressed to keep functioning as a whole. Therefore, these are called "critical" structure elements. For an infrastructure to be judged critical, it must be vital to one or more broad national functions. That set of functions has expanded over time, beginning with national defence and economic security, to include public health and safety, and more recently, national morale.[51] Some experts even argue that the debate should be enlarged to the whole of the "built environment", which encompasses all human-made physical elements of society and in which the average person spends 95% of their lives.[52]

The information infrastructure plays a very special role in the CIP debate. Over the years, infrastructure operators have taken measures to guard against, and to quickly respond to, many possible disruptions of physical infrastructures that may be due to poor design, operator error, or physical destruction due to natural causes such as earthquakes or floods, as well as physical destruction due to intentional human actions.[53] However, the growing dependency of these systems on information technologies and computer networks introduces a new vector by which problems can be brought in. Since the distinguishing characteristic of the information infrastructure is that it underpins the larger infrastructure, many of the critical services that are essential to the well-being of developed societies are now dependent, to a greater or lesser extent, on IT. Again, some of these IT systems or parts of the information infrastructure are considered more essential than others and are therefore called critical information infrastructures (CII). Insecurity at the technical level therefore has the potential to create a new set of problems on higher levels.

Potentially damaging events that could happen to the information infrastructure can be categorized as "failures", "accidents", and "attacks", even though these categories do not partition these events into mutually exclusive or easily distinguishable sets.[54] These events are only considered to be potentially damaging, because not all events actually produce harmful results – system failure will not occur as long as the error does not reach the service interface of the system, and might go unobserved.[55]

- Failures are potentially damaging events caused by deficiencies in the system or in an external element on which the system depends. Failures may be due to software design errors, hardware degradation, human errors, or corrupted data;
- Accidents include the entire range of randomly occurring and potentially damaging events such as natural disasters. Usually, accidents are externally generated events (i.e., from outside the system), whereas failures are internally generated events;
- Attacks are potentially damaging events orchestrated by an adversary. This category is of prime importance in the cyber-threats debate. There are various tools for attack.

In practice, it is often difficult to determine whether a particular detrimental event is the result of a malicious attack, a failure of a component, or an accident,[56] which means that from the practitioner's point of view, the distinction between a failure, an accident, or attack an is often considered less important than the impact of the event, at least in a short-term perspective. Technically speaking, information is a string of bits and bytes travelling from a sender to a receiver. If this string arrives in the intended order, the transfer has been successful. If the information is altered, intercepted, or deviated, however, problems are likely to arise. In practice, this means that the first and most important question is not what exactly caused the loss of information integrity, but rather what the possible result and complications may be. A power grid might fail because of a simple operating error without any kind of external influences, or because of a sophisticated hacker attack. In both cases, the result is the same: A possible blackout and the accompanying domino effect of successive failures in systems that are linked through interdependencies. Analysing whether a failure was caused by a terrorist, a criminal, a simple human error, or a spontaneous collapse will not help to stop or reduce the domino effect.

In the context of security studies, however, the possibility of human agency is of special interest. Even though the immediate response has to be tailored to the actual event on the technical level, mid- or long-term strategies work on a different level. As we will see in more detail in chapter 3.6, an appropriate reaction does depend on an awareness of the perpetrator.

2.3 The threat spectrum: cyber-perpetrators and their tools

Statistically, some of the biggest threats are from attacks committed by "insiders" – individuals who are, or previously had been, authorized to use the information systems they eventually employ to spread harm.[57] However, most stakeholders are far more concerned with external attacks. In fact, long before 11 September 2001, it was understood that there are more and more state actors as well as non-state actors who are willing to contravene national legal frameworks and hide in the relative anonymity of cyberspace.[58] If these actors carry out their attack using "cyber-" weapons and strategies, one label often bestowed upon them is "hacker", another catchphrase in the information age vocabulary with a variety of meanings and a long record of misuse. It is used in two main ways, one positive and one pejorative: In the computing community, it describes a member of a distinct social group, a particularly brilliant programmer or technical expert who knows a set of programming interfaces well enough to write novel and useful software. In popular usage and in the media, however, it generally describes computer intruders or criminals. In fact, different types of hackers must be distinguished[59], mainly by their motivation and skill level:

- Script kiddies: Script kiddies are considered to be on the lowest rung of the hackers' social ladder. They download readily-available code from the Internet rather than writing their own. The driving force of script kiddies has been shown to be boredom, curiosity, or teenage bravado.

- Hacktivists: Hacktivism is generally considered to involve the use of computer attacks for political, social, or religious purposes. Hacktivists are motivated by a wide range of social and political causes and use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage.[60] Web "sit-ins" and virtual blockades, automated email bombs, web hacks and defacements of websites, computer break-ins, and computer viruses and worms
- Cracker, "Black Hat Hacker": Someone who (usually illegally) attempts to break into or otherwise subvert the security of a program, system, or network, often with malicious intent. Hackers themselves like to distinguish between this type of hacker and
- Sneakers, or "White Hat Hackers", which is someone who attempts to break into systems or networks in order to help the owners of the system by making them aware of security flaws in it.

In the debate over cyber-threats, hacking is considered a method used not only by technologically apt individuals, but also by malicious actors with truly bad intent, such as terrorists or actors operating on behalf of hostile foreign states. Members of the last two hacker groups in particular have the knowledge, skills, and tools to attack the information infrastructure. Even though they generally lack the motivation to cause violence or severe economic or social harm,[61] it is feared that a human actor with the capability to cause serious damage but lacking motivation could be swayed to employ their knowledge by sufficiently large sums of money provided by a "malicious" group of actors.

Basically, there are two threat scenarios ─ one from hackers and individuals, and the other from foreign nation states. The first is sometimes described as an "unstructured" threat, while the latter is considered a "structured" threat.[62]

- The unstructured threat is random and relatively limited. It consists of adversaries with limited funds and organization and short-term goals. These actors have limited resources, tools, skills, and funding to accomplish a sophisticated attack. The unstructured threat is not a danger to national security. However, such attacks might cause considerable damage if they are sufficiently foolish or lucky.
- The structured threat is considerably more methodical and better supported. These adversaries have all-source intelligence support, extensive funding, organized professional support, and long-term goals. Foreign intelligence services, criminal elements, and professional hackers involved in information warfare, criminal activities, or industrial espionage fall into this threat category. Even though the unstructured threat is not of direct concern, it is feared that a structured threat actor could masquerade as an unstructured threat actor.[63]

Means to exploit, distort, disrupt, and destroy information resources range from hacker tools to devices such as magnetic weapons; directed energy weapons; HPM (High Power Microwave) or HERF (High Energy Radio Frequency) guns; and electromagnetic pulse (EMP) cannons.[64] The attack against an information infrastructure can therefore be carried out with both physical implements (hammer, backhoe, bomb, HERF, HPM) and cyber-based hacking tools. The same is true for the target: It can be immaterial, consisting for example of information or applications on a network, or physical, such as computers or a telecommunications cable. The so called "infrastructure threat matrix" (Table 1) distinguishes four types of information attack, all four of which involve the malicious use of the information infrastructure either as a target or as a tool. However, as we have seen above, it is becoming increasingly difficult to distinguish between purely physical and cyber components of the information infrastructure.

Table 1: The infrastructure threat matrix

		Target	
		Physical	Cyber
Means / Tool	Physical	1) - Severing a telecommunications cable with a backhoe - Smashing a server with a hammer - Bombing the electric grid	2) -Use of electromagnetic pulse and radio-frequency weapons to destabilize electronic components
	Cyber	3) - Hacking into a SCADA system that controls municipal sewage - "Spoofing" an air traffic control system to bring down a plane	4) -Hacking into a critical government network - Trojan horse in public switched network

Note: SPU_note.

Source: SPU_source (Devost et al., 1997:78; OCIPEP, 2003).

The most frequently discussed topic in connection with cyberspace today is cyber-crime. Unlike traditional crimes, cyber-crimes are global crimes committed by perpetrators with coordination from two or more countries. Most of these crimes are becoming more sophisticated by the day. Incidents of "phishing", which involves the sending of false emails purportedly from banks or other institutions to their customers to trick them into giving out their account details, have increased significantly during the past couple of years. Issues of identity theft and authentication on the Internet are impeding e-commerce across the globe. Regular attempts of DDOS attacks are causing enough losses to business establishments to be more than a mere nuisance.[65]

But is this a national security threat? It cannot be disputed that cyber-attacks and cyber-incidents are a costly problem for the business community and cause major inconvenience. In the last couple of years, they have cost billions of US dollars in the form of lost intellectual property, maintenance and repair, lost revenue, and increased security costs.[66] Beyond the direct impact, cyber-attacks can also reduce public confidence in the security of Internet transactions and e-commerce, damaging corporate reputations and reducing the efficiency of the economy.[67] It is, however, highly controversial whether risks linked to the Internet and other information infrastructure constitute a real national security threat, since the menacing scenarios of major disruptive occurrences in the cyber-domain triggered by malicious actors have remained just that – scenarios, even when one takes into account that there have been some few incidents with the potential for grave consequences.[68]

2.4 The unsubstantiated nature of cyber-threats and the implications for countermeasures

The ability of governments to gauge threats to critical infrastructures has traditionally been contingent upon their ability to evaluate a malicious actor's intent and that actor's ability to carry out a deliberate action. This was significantly easier during the Cold War, when the authorities were merely concerned with the security of physical structures. Due to the global nature of information networks, attacks can be launched from anywhere in the world, and discovering the origin of attacks remains a major difficulty, if, indeed, they are detected at all. Compared to traditional security threat analysis, which consists of analyses of actors, their intentions, and their capabilities, cyber-threats have various features that make such attacks difficult to monitor, analyse, and counteract:[69]

- Anonymity of actors: The problem of identifying actors is particularly difficult in a domain where maintaining anonymity is easy and where there are time lapses between the action that an intruder takes, the intrusion itself, and the effects of the intrusion. In addition, the continuing proliferation of sophisticated computer technologies among the mainstream population makes the identification of actors increasingly difficult.
- Lack of boundaries: Malicious computer-based attacks are not restricted by political or geographical boundaries. Attacks can originate from anywhere in the world and from multiple locations simultaneously. Investigations that follow a string of deliberately constructed false leads can be time-consuming and resource-intensive.
- Speed of development: Technology develops extremely quickly. The time between the discovery of a new vulnerability and the emergence of a new tool or technique that exploits that vulnerability is getting shorter.
- Low cost of tools: The technology employed in such attacks is simple to use, inexpensive, and widely available. Tools and techniques for invading computers are available on computer bulletin boards and various websites, as are encryption and anonymity tools.
- Automated methods: Increasingly, the methods of attack have become automated and more sophisticated, resulting in greater damage from a single attack.

These characteristics considerably hamper the ability to predict certain adverse future scenarios. Various types of uncertainties make it difficult for the intelligence community to effectively analyse the changing nature of the threat and the degree of risk involved. And these uncertainties are linked to inherent characteristics of cyber-threats ─ characteristics that they share with a whole set of "new" threats to security.

The end of the Cold War meant not only the end of a relatively stable bipolar world order, but also the end of the boundedness of threats. Following the disintegration of the Soviet Union, a variety of "new", and often non-military threats, such as migration, terrorism, proliferation, etc., were moved onto the security policy agendas.[70] Even though the label "new" is not justified in most cases, many of these threats are distinctly different from Cold War security threats. The main difference is an unprecedented quality of uncertainty about them.[71] The reason for this uncertainty is that chief among the new threats are those emanating from non-state actors using non-military means. Any combination of threat involving either non-military – or asymmetric – means and/or non-state actors poses significant difficulties for traditional approaches to intelligence collection: Linking capability to intent only works well when malefactors are clearly discernible and intelligence agencies can focus collection efforts to determine what capabilities they possess or are trying to acquire.[72]

While an attack by another state with unconventional means and a clearly assignable agency at least makes military options feasible, non-state actors completely play outside the "box" of the Westphalian state-order. Uncertainty surrounds the identity and goals of these potential adversaries, the timeframe within which threats are likely to arise, and the contingencies that might be imposed on the state by others.[73] Furthermore, there is uncertainty concerning the capabilities against which one must prepare, and also about what type of conflict to prepare for. In conclusion, experts are unable to predict how likely a cyber-attack really is.[74]

On the other hand, even though cyber-threats have not (yet) materialized as "real", the ongoing debate creates considerable pressure for decision-makers. For many governments, the decision has indeed been straightforward: they consider the threat to national security to be real, and have consequently drafted or even implemented a number of steps to counter it. The unsubstantiated nature of cyber-threats means, however, that the debate is not only about predicting the future, but also about how to prepare for possible contingencies in the present. As there have been no major destructive attacks on the cyber-level, decisions must be made on the basis of various scenarios. The different actors involved – ranging from government agencies to the technology community to insurance companies – have divergent interests and are competing with each other by means of constructed versions of the future.[75]

The selection of policies then largely depends upon two factors: One is the varying degree to which resources are available to the different groups. The other factor is the result of cultural and legal norms, because they restrict the number of potential strategies available for selection. A focus on the perception of the threat can show us why certain countermeasures are considered more suitable than others. For example, we see that the types of institutional solutions vary according to whether a state believes that other states or rather various non-state actors represent the threat subject: If the threat subject is perceived to consist of state actors, a state will tend to focus on strategic questions and military responses; when the threat is perceived to originate mainly from sub-state actors, a state will tend to focus primarily on law-enforcement responses. We will turn to these countermeasures in the next chapter.

3 A COMPARISON OF NATIONAL CYBERSECURITY INITIATIVES WORLDWIDE

For a number of years, policy-makers at the highest levels have been expressing their concerns that insecure information systems threaten economic growth and national security. As a result of these concerns, a complex and overlapping web of national, regional, and multilateral initiatives has emerged. A recent publication offers a compilation and analysis of cybersecurity efforts in fourteen countries.[76] The International CIIP Handbook provides an overview of issues of high importance in the field of critical information infrastructure protection (CIIP), serves as a reference work for the interested community, and provides a basis for further research by compiling relevant material. In this chapter, the main findings of this volume are presented. We are focusing mainly on five focal points of high importance that emerged from a cross-comparison of country surveys:

1. Critical Sectors: This section compares critical infrastructure sectors as identified by the respective countries. To look at the concept of critical infrastructures is important, because cybersecurity has emerged in parallel to CIP in all countries.
2. Organizational Overview: The second part of this chapter provides an overview of important public actors in the national cybersecurity organizational framework. It only characterizes the specific responsibilities or public actors at the state (federal) level (such as ministries, national offices, agencies, coordination groups, etc.). Public actors at the lower state level and private actors (companies, industry, etc.) are not taken into account.
3. Early Warning Approaches: The third section describes national organizations responsible for cyber-early warning, namely cybersecurity-related information-sharing organizations such as CERTs (Computer Emergency Response Teams), ISACs (Information Sharing and Analysis Centers), etc.
4. Current Topics in Law and Legislation: The development of effective regulations, laws, and criminal justice mechanisms is essential in deterring virtual abuse and other offences against the information infrastructure. Moreover, a strict regulation may create trust in the new ICT and encourage the private sector and individuals to make better use of e-Commerce or e-Government services.
5. Research and Development: The last section gives an overview of recent efforts in Research and Development (R&D) concerning cybersecurity.

3.1 Critical sectors

The classification of what is “critical” lies mainly in the eye of the beholder. Having said that, the concept of criticality itself is also undergoing constant change. A look at policy documents and at the many definitions and lists of critical infrastructures shows us great variety of conceptions. The main reason is that the criteria for determining which infrastructures qualify as critical have expanded over time; the PCCIP, for example, defined assets whose prolonged disruptions could cause significant

military and economic dislocation as critical.[77] Today, critical infrastructures in the US also include national monuments (e.g., the Washington Monument), where an attack might cause a large loss of life or adversely affect the nation's morale.[78] This development shows two differing, but interrelated perceptions of criticality:[79]

- Criticality as systemic concept: This approach assumes that an infrastructure or an infrastructure component is critical due to its structural position in the whole system of infrastructures, especially when it constitutes an important link between other infrastructures or sectors, and thus reinforces interdependencies.
- Criticality as a symbolic concept: This approach assumes that an infrastructure or an infrastructure component is inherently critical because of its role or function in society; the issue of interdependencies is secondary – the inherent symbolic meaning of certain infrastructures is enough to make them interesting targets.[80]

The symbolic understanding of criticality allows the integration of non-interdependent infrastructures as well as objects that are not man-made into the concept of critical infrastructures, including significant personalities or natural and historical sights with a strong symbolic character. Additionally, the symbolic approach allows us to define essential assets more easily than the systemic one, because it is not the interdependencies as such that are defining in a socio-political context, but the role, relevance, and symbolic value of specific infrastructures.[81]

Moreover, the question of criticality in the socio-political context is always inextricably linked to the question of how damage or disruption of an infrastructure would be perceived and exploited politically. Actual loss, be it monetary loss or loss of lives, would be compounded by political damage or the loss of basic public trust in the mechanisms of government, and by erosion of confidence in the government's inherent stability.[82] From this perspective, the criticality of an infrastructure can never be identified preventively based on empirical data alone, but only ex post facto, after a crisis has occurred, and as the result of a normative process.

In most countries, the definition of critical sectors is subject to ongoing discussions. Accordingly, the available lists of critical sectors are not conclusive. In comparing definitions over time, it also becomes obvious that these definitions are not static. It is indeed likely that the definition of criticality will continue to change, for example due to events such as the 11 September 2001 attacks or general changes in the conceptualization of cybersecurity.

Variations between countries can be seen not only in the definition of critical sectors, but also in the definition of CIP or cybersecurity. Some countries, such as Australia, Canada, the Netherlands, the UK, or the US, provide clear definitions, while other countries offer none at all. While superficially, it is always the sectors that are defined and listed as critical, in reality, the products, services, and functions provided by these sectors are the actual focus of protection efforts. This is clearly the case with recent additions such as "National Icons and Monuments", listed by Australia, Canada, and the US. These are deemed critical because of their inherent symbolic value.

Table 2 shows which country defines which sectors as critical. One must be careful, however, to avoid misleading comparisons: While Australia, Canada, the Netherlands, the UK, and the US are very precise in identifying critical sectors and sub-sectors as well as products and services that these sectors provide, others, such as Austria, Italy, or Sweden, have no official list of CI sectors. Often, identified critical sectors lack clear definitions, and it remains unclear which sub-sectors are included. Furthermore, the fact that similar or even identical assets can be labelled differently in different countries may hamper straightforward comparison.

Table 2: Overview of Critical Sectors and Sub-sectors

Country / Sector	AUS	A	CAN	CH	DE	F	FIN	I	NL	NO	NZ	SE	UK	USA	Total
Air Control Systems												✓			1
Banking and Finance	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	14
Central Government / Government Services	✓		✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	11
Civil Defense				✓				✓							2
(Tele)Communications / ICT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	14
Dams														✓	1
(Higher) Education														✓	1
Energy / Electricity	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	14
Emergency / Rescue Services	✓	✓	✓	✓	✓		✓			✓	✓		✓	✓	10
Food / Agriculture	✓		✓		✓		✓		✓				✓	✓	7
Hazardous Materials / CBRN			✓										✓	✓	3
Health Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	12
(Defense) Industry / Manufacturing	✓		✓	✓		✓	✓							✓	6
Information Services / Media /Broadcasting	✓	✓	✓	✓			✓		✓			✓	✓		8
Insurance	✓				✓									✓	3
Justice / Law Enforce-ment					✓				✓		✓		✓	✓	5
Military Defense / Army / Defense Facilities	✓	✓			✓				✓	✓					5
National Icons and Monuments	✓		✓											✓	3
Nuclear Power Plants						✓								✓	2
Oil and Gas Supply	✓		✓		✓			✓	✓	✓	✓		✓	✓	9
Police Services	✓	✓	✓				✓			✓			✓		6
Post Systems		✓												✓	2
Public Administration		✓		✓	✓		✓	✓	✓				✓	✓	8
Public Order / Public Safety						✓			✓				✓		3
Sewerage / Waste Man-agement	✓		✓							✓			✓		4
Social Securtiy / Welfare		✓					✓			✓	✓				4
Transportation / Logistics / Distribution	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	13
Utilities	✓	✓								✓					3

Source: Dunn and Wigert 2004: p. 345.

However, it is possible to make a rough comparison of CI sectors across the selected countries without over-interpreting the collected information. The most frequently mentioned critical sectors in all countries are listed below. These are the core sectors of modern societies, and possibly the ones where large-scale interruption would be most devastating:

- Banking and Finance,
- Central Government/Government Services,
- (Tele-) Communication/Information and Communication Technologies (ICT),
- Emergency/Rescue Services,
- Energy/Electricity,
- Health Services,
- Transportation/Logistics/Distribution, and
- Water (Supply).

Variations in terminology can be explained not only in terms of different threat perceptions or conceptualization of what is critical, but also by country-specific peculiarities and traditions. Individual sectors, for example "Social Security/Welfare", "Insurance", or "Civil Defense", are influenced by socio-political factors and traditions, while others, for example "Water/Flood Management" in the case of the Netherlands, are determined by specific geographical and historical preconditions. Some sectors have been added after high-profile incidents. This is the case for the categories of "National Icons and Monuments" or the "Post Systems", introduced after 11 September 2001, or the "Meteorological Services", identified as a specific critical sub-sector in Canada after an

ice storm that severely affected Eastern Canada and Quebec in 1998. As mentioned above, these lists can be expected to change slightly over the years, especially due to incidents and events.

A different question arises in connection with terminology. Is it really the infrastructures that we want to protect? Infrastructures are defined by the Presidential Commission on Critical Infrastructure Protection (PCCIP) as "network[s] of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services".[83]

In Presidential Decision Directive (PDD) 63, infrastructures are described as "the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defence and economic security […]."[84]

If we compare the two concepts, the most striking similarity is the focus on "essential goods/products and services". That means that the actual objects of protection interests are not static infrastructures as such, but rather the services, the physical and electronic (information-) flows, their role and function for society, and especially the core values that are delivered by the infrastructures. This is a far more abstract level of understanding essential assets.
While infrastructures are constructed, maintained, and operated by humans and can be relatively easily illustrated in terms of organizational and institutional hierarchies, it is a much more complex and difficult task to understand intangibles like services, flows, and values.[85]

This also shifts attention away from man-made assets, which makes perfect sense in the age of media saturation where the symbolic value of things has become over-proportionally important. To conclude this short excursion into terminology, it makes more sense ─ from the point of view of both system dynamics and actual protection interest ─ to speak of "critical services robustness" or "critical services sustainability".[86]

3.2 Organizational overview

In most countries, responsibility for cybersecurity and/or critical infrastructure protection rests with more than one authority and with organizations from different departments, and thus involves many different players from different communities. This factor, together with events such as those of 11 September 2001, increases the urgency of reorganizing the existing structures by establishing new organizations with a distinct cybersecurity focus and coordination roles. The following are examples of organizations with at least a partial focus on cybersecurity:

- The former Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) in Canada, now Public Safety and Emergency Preparedness Canada (PSEPC);
- The Federal Office for Information Security (BSI) in Germany;
- The Centre for Critical Infrastructure Protection (CCIP) in New Zealand;
- The National Infrastructure Security Co-ordination Centre (NISCC) in the UK;
- The Department of Homeland Security (DHS) in the US.

The establishment and location of these key organizations within the government structures is influenced by various factors such as civil defence tradition, the allocation of resources, historical experience, and the general threat perception of key actors in the policy domain.

The following is a short overview of country-specific findings with regard to organizational structure in cybersecurity:

- In Australia, several organizations are responsible for CIP/CIIP. Since terrorism was identified as the most likely threat to arise against Australia's critical infrastructure (considering attacks against both virtual and physical structures), cybersecurity has been perceived as part of the country's overall counter-terrorism effort. Therefore, the members of the Critical Infrastructure Protection Group also include the Defence Signals Directorate, the Australian

Security Intelligence Organisation, and the Australian Federal Police, all of which are operational military, security, and policing intelligence services.

- In Austria, there is no single authority responsible for CIP/CIIP – all ministries have their own specific security measures to defend against outside attacks and to prevent the unauthorized usage of data. Cybersecurity is mainly perceived as an issue of data protection, as the Austrian E-Government Program, the Official Austrian Data Security Website, or the Pilot Project Citizen Card indicate.
- Canada's former Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), now Public Safety and Emergency Preparedness Canada (PSEPC), is the key organization responsible for both CIP/CIIP as well as Civil Emergency Planning. Hence, Canada has a centralized organizational model for CIP/CIIP.
- In Finland, cybersecurity is seen as a data security issue and as a matter of economic importance that is closely related to the development of the Finnish information society. Several organizations deal with cybersecurity, including the Communications Regulatory Authority, the Emergency Supply Agency, the Board of Economic Defense, and the Committee for Data Security.
- In France, cybersecurity is seen both as a high-tech crime issue and as an issue affecting the development of the information society. Overall responsibility for cybersecurity lies with the Secretary-General of National Defense.
- In Germany, the Federal Office of Information Security (BSI), which is part of the Ministry of the Interior, is the lead authority for cybersecurity matters within the organizational structure.
- In Italy, cybersecurity is regarded as part of the advancement of the information society. There is no single authority dealing with cybersecurity. A working group on cybersecurity was recently set up at the Ministry for Innovation and Technologies. It includes representatives of all ministries involved in the management of critical infrastructures, and many Italian infrastructure operators and owners as well as some research institutes.
- In the Netherlands, responsibility for CII lies with a number of authorities, but the Ministry for Interior and Kingdom Relations coordinates CIP/CIIP policy across all sectors and responsible ministries.
- In New Zealand, the Centre for Critical Infrastructure Protection (CCIP), located at the Government Communications Security Bureau, is the central institution dealing with cybersecurity. The main actor in charge of formulating New Zealand's security policy, including cybersecurity, is the Domestic and External Secretariat, DESS (which is the support secretariat for the Officials Committee for Domestic and External Security Co-ordination, ODESC).
- In Norway, the national key player in civil emergency planning, the Directorate for Civil Defense and Emergency Planning (DSB) is also a key player for CIP/CIIP-related issues. It is subordinated to the Ministry of Justice and Police.
- In Sweden, a number of organizations are involved in CIP/CIIP. The Swedish Emergency Management Agency (SEMA) at the Ministry of Defense has a key role.
- In Switzerland, there are a number of different organizational units dealing with CIP/CIIP. The Reporting and Analysis Centre for Information Assurance (Melde- und Analysestelle Informationssicherung, MELANI) has a key role. Public-private partnerships are among the central pillars of Switzerland's CIIP policy.
- In the UK, the key interdepartmental organization dealing with CIP/CIIP is the National Infrastructure Security Co-ordination Centre (NISCC). The NISCC has strong ties with the private sector and the intelligence community.
- In the US, the Department of Homeland Security (DHS) has the leading role in CIP and cybersecurity. However, several other organizational units are also involved in CIP/CIIP.

Public-private partnerships, e.g., Information Sharing and Analysis Centers (ISACs), are given a considerable role.

In their efforts to secure the information age, governments are challenged to operate in unfamiliar ways and to share influence with experts in the IT community, with businesses, and with non-profit organizations, because the ownership, operation, and supply of the critical systems are in the hands of a largely private industry, which is diverse, intermixed, and relatively unregulated.[87] Collectively, this industry has far more technical resources and operational access to the infrastructures than the government does, so that ultimately, the private sector will have to do most of the work and must bear most of the burden to make infrastructures more secure.[88]

Therefore, public-private partnerships are becoming a strong pillar of cybersecurity policy. Different types of such partnerships are emerging, including government-led partnerships, business-led partnerships, and joint public-private initiatives. Due to the importance of public-private partnerships, the location of new organizations is often constrained by the need to assure private-sector companies that their sensitive commercial and security information will be adequately safeguarded, and by the need to provide a secure environment that can adequately protect intelligence information to which the organization must have access.[89]

One of the future challenges in many countries will be to achieve a balance between security requirements and business efficiency imperatives. Satisfying shareholders by maximizing company profits has often led to minimal security measures. This is because like many political leaders, business leaders tend to view cyberattacks on infrastructures as a tolerable risk. Additionally, public-private partnerships are mainly based on trust, so that information-sharing is arguably one of the most significant issues in cybersecurity.

3.3 Early-warning approaches

The general trend in early warning points towards establishing central contact points for the security of information systems and networks. Among the existing early-warning organizations are various forms of Computer Emergency Response Teams (CERTs), e.g., special CERTs for government departments, CERTs for small and medium-sized businesses, CERTs for specific sectors, and others. CERT functions include handling of computer security incidents and vulnerabilities or reducing the probability of successful attacks by publishing security alerts.

In some countries, permanent analysis and intelligence centres have been developed in order to make tactical or strategic information available to the decision-makers within the public and private sectors more efficiently. Tasks of early-warning system structures include analysing and monitoring the situation as well as the assessment of technological developments. Examples can be found in Canada (Integrated Government of Canada Response Systems), in Switzerland (Reporting and Analysis Center for Information Assurance, MELANI), and in the US (Directorate for Information Analysis and Infrastructure Protection, IAIP). Furthermore, there is cross-border cooperation in early warning between Australia and New Zealand. Such international cooperation is sensible when one considers the inherently cross-boundary nature of cyber-threats.

Similar CERTs have been set up mainly at national and governmental levels, and these organizations are involved in incident response management and advisories at higher levels. Most of the CERTs are in communication with each other and could therefore be considered to represent the simplest form of a global incident response entity. The notion of addressing network security by legal and technological means is gaining major currency globally.

3.4 Legal issues

Although many developed countries have been concerned with the protection and security of information (infrastructures) and related legislation for some years, they have begun to review and adapt their cybersecurity legislation after 9/11. Because national laws are developed autonomously,

some countries have preferred to amend their penal or criminal code, whereas others have passed specific laws on cybercrime.

The following is an overview of important common issues currently discussed in the context of legislation procedures in the countries covered in the handbook:[90]

- Data protection and security in electronic communications (including data transmission, safe data storage, etc.);
- IT security and information security requirements;
- Fraudulent use of computer and computer systems, damage to or forgery of data, and similar offences;
- Protection of personal data and privacy;
- Identification and digital signatures;
- Responsibilities in e-Commerce and e-Business;
- International harmonization of cybercrime law;
- Minimum standards of information security for (e-)governments, service providers, and operators, including the implementation of security standards such as BS7799, the code of practice for information security management ISO/IEC 17799, the Common Criteria for Information Technology Security Evaluation ISO/IEC 15408, and others;
- Public key infrastructure and its regulation.

Due to the inherently transnational character of the information infrastructure, the need to harmonize national legal provisions and to enhance judicial and police cooperation has been a key issue for a number of years. However, so far, the international legal framework has remained rather confused and is actually an obstacle to joint action by the actors involved. At the European level, the Council of Europe Convention on Cybercrime and the European Framework Decision on Attacks Against Information Systems are currently among the most important pillars of transnational cybersecurity legislation efforts. We will address international cyberlaw issues in more detail below.

3.5 Research & development

There are also a large number of R&D topics in this area, ranging from technical aspects to social themes. At the moment, the US and the EU are the major players in the field of cybersecurity R&D. The US has a leading role in identifying and promoting relevant research topics. The EU plays a crucial role in supporting cross-national R&D and information exchange in the field of cybersecurity in Europe. There is no doubt that cybersecurity will be a major R&D challenge in the future. Recent publications and overviews show that R&D in the field of cybersecurity is undertaken by a large variety of actors in each country: Research institutes at universities, private sector research institutes and laboratories, networks of excellence, national research councils, etc.[91]

The inherently transnational nature of the information infrastructure and the growing international dependency on these systems, as well as the cross-boundary threats and vulnerabilities to the national CI/CII (a good example is the big blackout in Italy's electric power system in October 2003) make the topic of cybersecurity R&D an obvious issue for international cooperation. The rationale for strategic coordination of R&D at the international level was outlined at a December 2001 EU-US workshop on R&D in the field of CIIP.[92] On that occasion, a list of important drivers for international collaboration on R&D was outlined. Among these drivers are:[93]

- Increasingly networked and more complex embedded systems;
- Growing interdependencies between essential infrastructures;
- A shared understanding that global problems require global solutions;
- Improved cost-effectiveness through greater efficiency and faster results;

- Improved access to relevant data that is not available nationally.

The need for more research into methodologies for the analysis of critical information infrastructures and other issues is acknowledged. However, puzzles persist – such as the functioning of interdependencies; identifying what is critical to whom, when, and why; vulnerabilities and dispersions of disturbances; the influence of threat perceptions; or even the consequences of specific risks to the information infrastructure.[94] Solving them requires an integrated set of methods and tools for analysis, assessment, protective measures, and decision-making. Research on interdependencies and cascading effects in case of failures is especially essential. Moreover, more research into the nature of criticality is necessary, with a strong focus on the socio-political dimension, including terrorism research. There is a clear need for computer models for all protection phases – such as state-of-the-art-evaluation, the definition of potential improvements, assessment, and to some extent implementation and control.[95]

This points to one fundamental issue and major challenge in terms of research: Only interdisciplinary approaches do justice to an issue that is inherently interdisciplinary due to its multifaceted nature. However, the question of cybersecurity and related topics has received little attention from large parts of academia up to now. Research is generally focused on aspects of IT-security, on the technical level, and on local or closed subsystems. These aspects are important – but they often miss crucial key features of the complex systems at hand and are inadequate for problem solution.

It is true that the putative new societal risks and vulnerabilities are directly or indirectly related to the development and utilization of new technologies. However, it is likely that critical vulnerabilities, and even the worst consequences of infrastructure disruptions, will not be traceable in any useful way to single technical subsystems – as a consequence of an already overwhelming complexity of open socio-political systems.[96] Also, in view of the rapid technological developments that are constantly taking place, and of the particular nature of their implementations, even if one carefully examines a relatively localized subsystem from the point of view of risks and threats, thereby identifying certain of its vulnerabilities, these insights can hardly be generalized or established in order to utilize them "beyond" the subsystem itself and on a higher system level.

Effective protection for critical infrastructures, therefore, demands holistic and strategic threat and risk assessment at the physical, virtual, and psychological levels as the basis for a comprehensive protection and survival strategy, and will thus require a comprehensive and truly interdisciplinary R&D agenda encompassing fields ranging from engineering and complexity sciences to policy research, political science, and sociology.

3.6 Explaining similarities and differences in cybersecurity policies

What can we learn from this in conclusion? It is obvious that governmental cybersecurity policies are at various stages of implementation – some are enforced, while others are just a set of suggestions – and come in various shapes and forms, ranging from a regulatory policy focus concerned with the smooth and routine operation of infrastructures and questions such as privacy or standards, to the inclusion of cybersecurity into more general counter-terrorism efforts.

One feature common to all initiatives is that cybersecurity has become an issue of high relevance to many different, very diverse, and overlapping communities. These different groups, whether they be private, public, or a mixture of both, do not usually agree on the exact nature of the problem or on what assets need to be protected with which measures. Depending on their influence or on the resources at hand, various key players shape the issue in accordance with their view of the problem.

Within governments, turf battles are just as frequent. Only in a few countries have central governmental organizations been created to deal specifically with cybersecurity issues. Mostly, responsibility lies with multiple authorities and organizations in different governmental departments. Very often, responsibility for the issue is given to well-established organizations or agencies that appear suitable for the task. Depending on their key assignment, these agencies bring their own

perspective to bear on the problem and shape the policy accordingly. In the next chapter, we want to introduce four simplified viewpoints and explore their meaning when it comes to countermeasures.

3.6.1 Different viewpoints and protection typologies

We can roughly distinguish between the following perspectives. While all typologies can be found in all countries, the emphasis given to one or more of them varies to a considerable degree. The dominance of one or several typologies has implications for the shape of the protection policies and, subsequently, in determining appropriate protection efforts, goals, strategies, and instruments for problem solution:

- Cybersecurity is an IT security issue: cybersecurity can be approached as an IT security or information assurance issue, with strong focus on Internet security. Policies are thus aimed at countering threats to the information infrastructure by technical means such as firewalls, anti-virus software, or intrusion detection software. The main actors are IT security professionals. The main threats perceived range from accidents, system failures, bad programming, and human failures to hacker attacks.
- Cybersecurity is as an economic issue: cybersecurity is seen as relevant to business continuity, and especially to e-business, which requires permanent access to ICT infrastructures and permanently available business processes to ensure satisfactory business performance. The main actors are representatives of the private sector. The main threats are viruses and worms, human failures, but also hacker attacks of all sorts, and acts of cyber-crime.
- Cybersecurity is a law enforcement issue: cybersecurity is seen as relevant to (cyber-) crime. "Cyber-crime" is a very broad term with various meanings, and definitions can include everything from technology-enabled crimes to crimes committed against individual computers. The main actors are law enforcers. The main threats are acts of computer criminality, but also "cyber-terrorism".
- Cybersecurity is as a national security issue: Society as a whole and its core values are seen as endangered, due to their dependence on ICT. Action against the threat is aimed at several levels (the technical, legislative, organizational, or international levels). The main actors are security specialists. The main threats are terrorists, but also information warfare threats from other states.

More specifically, in accordance with the perspectives outlined above, information infrastructures are seen variously as tools for maintaining a competitive edge over business adversaries, as technical-operational systems, as facilitators of criminal activities, as defence-relevant strategic assets, or, more generally, as objects of national and international security policy. Depending on the perspective taken, cybersecurity may be perceived either as the responsibility of the private/corporate sector, or as the responsibility of specific governmental agencies, ranging from law enforcement to the defence establishment, or a mixture of the above.[97] In this light, the protection of a nation's critical information infrastructure must first and foremost answer the question of which partner is providing which service in what case. This automatically brings together different stakeholders: state institutions like prosecution, intelligence and law enforcement, as well as the technological community and the private sector as the main proprietor and operator of the critical information infrastructure.

How does this observation link to policy and in our case, national cybersecurity initiatives? To explain this connection, we need to introduce some aspects of social-science theory. In the introduction, we have already introduced the idea of threat politics and the study of how threats are included on the agenda. As pointed out above, the elusive and unsubstantiated nature of cyber-threats means that the perceptions of risks and threats can be contested between different social groups, as stated in chapter 2.4. The different actors involved – ranging from government agencies to the technology community to insurance companies – have divergent interests and are competing with each other by means of future scenarios, which represent their version of how they believe the threat will manifest itself.[98] This view shifts the focus of analysis from an objective, positivistic, and materialistic understanding of threats or risks towards a subjective, constructivist perception and a focus on political discourse and

processes. Instead of conceiving of threats as given factors that can be measured objectively, such an approach focuses on the process by which key actors subjectively arrive at a shared understanding of what is to be considered and collectively responded to as a security threat.[99]

There are in fact various positions of authority within the state from which security issues can be voiced.[100] In accordance with the tenets of discourse theory, which understand the interactions and processes that form reality as conflicts and struggles between antagonistic and competitive forces over "the structuring of social meaning",[101] this multiplicity of positions leads to struggles over legitimacy and primacy between competing discourses. However, the threat politics process is not reduced to simple rhetoric, but implies extensive mobilization of resources to support the discourse.[102] At some point, one professional or group of professionals of security will emerge as the "winner" of the subsequent turf battles. The most crucial question for the study of threat politics is therefore: Who wins the discursive struggle when for what reasons, or, in short: Who wins when, and why?

3.6.2 And the winner is: law enforcement and Cybercrime

We will illustrate this with a short example. Until the mid-1990s, there were three different risk strategies for the protection of critical information infrastructures in the US: Repression and military strength (intervention), technical solutions for securing the systems (preparation), and awareness-building (information). Two discourses were influential besides the military metaphors widely used in the mass media ("electronic Pearl Harbor", "information warfare", "cyber warfare"): On the one hand, law enforcement agencies emphasized their view of the risk as "computer crime," while on the other hand, the private sector running the infrastructures perceived the risk as consisting primarily of a local, technical problem or of economic costs.[103]

In the end, the distribution of resources and the technical and social means for countering the risk were important for the outcome. Because the technology generating the risk makes it very difficult to fight potential attackers in advance, 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 "Californian ideology", as well as legal restrictions, prohibited a bigger role of the state, especially of the armed forces. Most importantly, the general aversion to government regulation of the new economy, which had wide support across all political factions, strictly limited the choice of strategies. And in addition, there was considerable hesitation within the armed services concerning the adoption of new, non-traditional military tasks.[104] Besides these cultural differences with regard to strategy, legal norms also obviated a strategy based more on a military response: 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.[105] 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.

This example from the US also has validity for other countries. Even though the military usually plays a lesser role in the beginning, the cyber-crime/law enforcement paradigm is emerging as the strongest viewpoint in most countries. Across all boundaries, there are two main factors that influence and sometimes even hinder efficient law enforcement ─ one with a national, the other with an international dimension:

- Lack of know-how or of functioning legal institutions: Even if a country has strict laws and prohibits many practices, the enforcement of such laws is often difficult. Frequently, the necessary means to effectively prosecute misdemeanours are lacking, due to resource problems, inexistent or emerging cyber-crime units, or a lack of supportive legislation, such as the storing of rendition data.[106]

- Lack or disparity of legal codes: While most crimes, such as theft, burglary, and the like are punishable offences in almost every country of the world, some rather grave disparities still remain. For example, in most European countries, it is illegal to publish right-wing extremist or anti-Semitic statements on the Internet. However, the US does not prosecute such offences if committed within its borders, as they are usually protected by the First Amendment to the Constitution, which guarantees freedom of speech.[107]

It has, in fact, been clear for years that the existing state-centric policing and legislative structures are inadequate for regulating international networks. The WSIS declaration of principles and the policy action plan, as well as countless policy papers, repeatedly stress the need for increased international cooperation.[108] Why are international approaches crucial to the successful protection of cyberspace? The answer is rather simple and originates in the fact that like other security issues, the vulnerability of modern societies ─ caused by dependency on a broad spectrum of highly interdependent information systems ─ has global origins and implications. Specifically,

- Information infrastructures transcend territorial boundaries, so that information assets vital to the national security and the essential functioning of the economy of one state may reside outside of its sphere of influence, on the territory of other nation-states.
- Malicious actors are willing to contravene national legal frameworks and hide in the relative anonymity of cyberspace.

As a result, any adequate protection policy extending to strategically important information infrastructures will ultimately require transnational solutions. Such a solution may take the form of an international regulatory regime for the protection of cyberspace.

4 TOWARDS MULTILATERAL SOLUTIONS? – PROBLEMS AND PROSPECTS FOR AN INTERNATIONAL REGIME FOR THE PROTECTION OF CYBERSPACE

Regimes are usually defined as "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations".[109] Such regimes emerge from the mediation of disparate interests of various stakeholders within arenas of political interaction. The outcome of these interactions usually takes the form of new rules, which are created by constraining actors' choices and prescribing who can act when, and affect behaviour both directly and indirectly.[110]

In the past two decades, a variety of initiatives have been undertaken on the international floor to improve the security and dependability of systems, of management practices, and of international policing efforts. However, an underlying tension with regard to the use of cyberspace prevents the coherent establishment and implementation of rules and norms. We can distinguish broadly between two different paradigms as to what kind of threat is actually posed and by whom:[111]

Cyberthreats as a threat to the economic prosperity of all nations

This approach defines the threat as originating mainly from organized crime, electronic vandalism, and corporate espionage and is, as we have pointed out, currently the predominant one. The threat is defined as a menace to the economic prosperity and social stability of all nations that are plugged into the global information infrastructure. In this paradigm, all nations have an interest in working together to devise international regimes that will ensure the reliability and survivability of information networks.

From this perspective, a range of mechanisms can be used to mitigate the risks. It is a non-zero sum game, meaning that one actor's gain is not necessarily to the detriment of other actors. Indeed, in extreme cases of non-zero-sum games, the players' interests overlap entirely. International organizations can promulgate information security standards and industry can be encouraged to make

its information systems more secure and dependable. International law enforcement institutions and mechanisms, e.g. Interpol, can be used for information exchange and investigations, while multilateral conventions on computer crime, such as the Council of Europe convention, can be negotiated in analogy to those that deal with hijacking and other forms of crime. While transnational investigations and traceback will always be a problem, at least the appropriate mechanisms exist through which such problems can be addressed.[112]

Cyberthreats as a threat to national security

The other view sees the attempt to counter malicious use of cyberspace as a zero-sum game. A zero-sum game describes a situation in which one participant's gain (or loss) is exactly balanced by the losses (or gains) of the other participant(s). As the term suggests, when the total gains and losses of all participants are added up, the resulting value should be zero.[113] In this view, attacks against the information infrastructure of another state or rival actor in general are perceived as tools of strategic coercion. Attacks that do breach the confidentiality, integrity, or availability of information systems could in theory be treated as acts of war and be brought within the scope of arms control or the laws of armed conflict. In this approach, existing mechanisms and methods such as the Laws of Armed Conflict and arms control/verification regimes could be applied to this new "weapon system." The main threat is perceived as stemming from other state actors and terrorist groups.

This basically means that the discussion on security implications in the information age runs on two interwoven tracks: the military track concerns the development of, among other things, offensive information warfare capabilities, while the civil track aims at protecting the whole of society from threats against critical infrastructures and, most importantly, threats against the crucial information infrastructure. The main problem with these two perspectives is the underlying tension between the desire of military establishments to exploit cyberspace for military advantages and to develop doctrines and capabilities within the broad rubric of "Information Operations", and concerns about the dependency of militaries, governments, economies, and societies on the networked information systems that are emerging as the backbone of post-industrialized societies. This paradox needs to be addressed carefully before any conclusive international regime can be developed or a policy approach can be adopted.

4.1 Non-zero sum game: cybercrime convention and other legal instruments

In the past two decades, a variety of initiatives have been undertaken on the international floor to improve the security and dependability of systems, of management practices, and of international policing efforts. As a result, a complex and overlapping web of national, regional, and multilateral initiatives has emerged. In the following, we will look more closely at four possible categories of initiatives launched by multilateral actors: deterrence, prevention, detection, and reaction.

- Deterrence – or the focus on the use of multilateral cyber-crime legislation: Multilateral initiatives to deter the malicious use of cyberspace include initiatives to a) harmonize cyber-crime legislation and to promote tougher criminal penalties (e.g. the Council of Europe Convention on Cybercrime),[114] and b) improve e-commerce legislation (e.g., the efforts of the United Nations Commission on International Trade Law (UNCITRAL) for electronic commerce).[115]
- Prevention – or the design and use of more secure systems, better security management and the promotion of more security mechanisms: Multilateral initiatives to prevent the malicious use of cyberspace centre around a) promoting the design and use of more secure information systems (e.g., the Common Criteria Project);[116] b) improving information security management in both public and private sectors (e.g., the ISO and OECD standards and guidelines initiatives);[117] c) legal and technological initiatives such as the promotion of security mechanisms (e.g., electronic signature legislation in Europe).
- Detection – or cooperative policing mechanisms and early warning of attacks: Multilateral initiatives to detect the malicious use of cyberspace include a) the creation of enhanced

cooperative policing mechanisms (e.g., the G-8 national points of contact for cyber-crime); and b) early warning through information exchange with the aim of providing early warning of cyber-attack by exchanging information between the public and private sectors (e.g., US Information Sharing & Analysis Centers, the European Early Warning & Information System, and the European Network and Information Security Agency (ENISA)).

- Reaction – or the design of stronger information infrastructures, crisis management programs, and policing and justice efforts: Multilateral initiatives to react to the malicious use of cyberspace include a) efforts to design robust and survivable information infrastructures; b) the development of crisis management systems; and c) improvement in the coordination of policing and criminal justice efforts.

The most important legislative instrument in this area is the Council of Europe Cybercrime Convention (CoC), which was signed on 23 November 2001 by 26 members and four non-members of the Council. The Convention is the first international treaty on crimes committed via the Internet and other computer networks. Its main objective is to pursue a common law enforcement policy aimed at the protection of society against cyber-crime, especially by adopting appropriate legislation and fostering international cooperation.[118] An additional protocol to the Convention outlaws racist and xenophobic acts committed through computer systems. The criminal offences concerned are:

- Crimes against the confidentiality, integrity, and availability of computer data or systems, such as spreading of viruses;
- Computer-related offences such as virtual fraud and forgery;
- Content-related offences, such as child pornography;
- Offences related to infringements of intellectual property and related rights;
- Another objective of the convention is to facilitate the conduct of criminal investigations in cyberspace.[119]

While other politically powerful entities like the G8 also try to foster collaboration and a more efficient exchange of information when it comes to cyber-crime and terrorism, the CoC goes one step further. It lays out a framework for future collaboration between the signature state's prosecution services. It achieves this mainly by harmonizing the penal codes of the CoC signees. As a result, such crimes as hacking, data theft, and distribution of paedophile and xenophobic material etc. will be regarded as illegal actions per se, thus resolving the problem of legal disparities between nations that was mentioned above. This also allows the authorities to speed up the process of international prosecution. Since certain activities are defined as illegal by all CoC member-states, the sometimes long and painful task of crosschecking supposed criminal charges committed in a foreign country becomes obsolete with the adoption of that offence to the own national penal code. Consequently, reaction times will be shortened and the CoC-signees will establish a round-the-clock network within their countries to handle aid requests that demand swift intervention.[120] While the implementation of the CoC will most likely be a slow and sometimes thorny process, the idea of finding a common denominator and harmonizing at least some of the most crucial problems is certainly a step in the right direction.

4.2 Zero-sum game: discussing the need for arms control in cyberspace

However, when dealing with the issue of cyberspace protection, it is important to be aware of an underlying tension that has a great impact on this topic. To date, various states are developing doctrines and even capabilities to exploit cyberspace for military advantage. Their military establishments invest in military technologies and doctrines designed to disrupt the (information) infrastructures of rival nations.[121] Those states see these capabilities as a comparative strategic advantage, and they will be loath to give them up. As a consequence, we witness a parallel development in the use of information and communications technology: On the one hand, there is the development of Information Operation ideas and doctrines by the military and the push for an

offensive and aggressive use of cyberspace. On the other hand, we observe calls and initiatives that aim to protect cyberspace from being exploited by both enemy nations and terrorist groups.[122]

This is why some voices have called for efforts to control the military use of computer exploitation through arms control or multilateral behavioural norms. Such agreements might pertain to the development, distribution, and deployment of cyber-weapons, or they might apply only to their use. They might relate primarily to criminal law, or might govern the conduct of nation states in the domain of international law.[123] However, it will be impossible to establish meaningful cyber arms controls if nation-states are opposed. Governments might oppose any treaty that restricts their ability to develop offensive cyber-weapons on the grounds that such restrictions would hamper their ability to prepare an adequate cyber-defence in the event of an attack. The position of the US has been that it would be premature to consider negotiating an international agreement on information warfare, and that the energies of the international community would be better spent on cooperating to secure information systems against criminals and terrorists.[124]

In addition, it is hard to envisage traditional capability-based arms control being of much use, mainly due to the impossibility of verifying limitations on the technical capabilities of a state. The avenues so far available for "arms control" in this arena are primarily information exchange and norm-building, whereas structural approaches and attempts to prohibit the means of information warfare altogether or restricting their availability are largely impossible due to the ubiquity and dual-use nature of information technology.[125]

While it is true that the creation of organized military Information Operation units could be monitored with the assistance of Western intelligence services, the proliferation of information infrastructure attack capabilities in themselves could not really be monitored, since the technology required is globally available. The fact that existing multilateral and national arms control regimes are only beginning to grapple with the export of intangibles such as software and know-how indicates how difficult any controls would be in an era when cyber-attack scripts reside on Internet hosts computers around the world.

Accordingly, an effective cyber-arms control treaty would have to overcome obstacles in several areas. For example, as stated, it has been extremely difficult to enforce existing criminal laws that pertain to computer network attacks. Many attacks are never detected in the first place. When they are, finding the perpetrator is seldom easy, especially when the person has looped through numerous computers in different countries. An attack against computers in one country, for example, might appear to originate from government computers in another, although it may have been perpetrated by teenage hackers in a third country who gained control over the computers.[126]

To enforce general prohibitions against cyber-weapons would also be very difficult, as they can be manufactured without any special physical materials or laboratory facilities. All that is required is a computer and standard software, both of which are readily available. Moreover, once produced, cyber-weapons are easily copied and distributed on the Internet through electronic mail, websites, instant messaging, peer-to-peer sharing systems, and other mechanisms. Another issue is that even if the presence of a controlled cyber weapon were detected, it would be impossible to find and eliminate all copies, which might be stored on thousands of computers all over the world. Monitoring for treaty compliance would also be hard given the rapid changes in technology and in methods and tools of attack.[127]

Mainly because the obstacles for arms control in cyberspace seem almost incredibly high, we must hope for self-restraint of national actors. However, existing state-led approaches to attack through cyberspace or computer network operations (CNO) have so far failed to recognize the nature of the globally interdependent network environment and the leading role of the private sector in this domain. Andrew Rathmall has argued, for example, that the notion of interdependencies is not appreciated by current military thinking. Constrained by a focus on delivering "effect" to a particular geographic conflict zone, armed forces are trying to exploit electronic attacks for precise targeting of enemy infrastructures. However, there is a disjunction between the emerging military doctrine on Information

Operations and computer attacks on the one hand, and the technological and market realities of a globalized, interdependent, and networked world on the other.

The features of the emerging information environment make it extremely unlikely that any but the most limited and tactically-oriented instances of computer attack could be contained, as current military doctrine would demand. More likely, computer attacks by the military could "blow back" on Western societies through the interdependencies that will characterize the new environment. Even in today's environment, relatively harmless viruses and worms cause considerable disruption to businesses, governments, and consumers randomly. In addition, the routine use of CNO would most likely undermine the already brittle trust in cyberspace. The knowledge that global information networks are routinely exploited by Western militaries would lead users to question whether data and systems were trustworthy, and to wonder whether information was being polluted. The damage to consumer and business confidence could well undermine efforts to promote a reliable Information Society.

5 CONCLUSION

A Canadian once said about cybersecurity that it was "a Gordian knot around which many stakeholders circle, pulling on the strands that seem most promising and causing the entire thing to tighten even more snugly rather than loosen to reveal its internal structure".[128] Even though this quote dates back to 1999, it still rings true today. Cybersecurity poses a great puzzle to many actors from a variety of communities, and its inner secrets are far from being revealed. In this paper, we have aimed to shed some light on the issue by investigating what can be learned from national cybersecurity initiatives that might bring us closer to a global culture of cybersecurity. On the one hand, we have found a great many approaches at national level and a great degree of diversity. On the other hand, we have identified common themes that are of central importance in all countries. The most important ones are early-warning approaches, legal issues, public-private partnerships, and the need for more research. We have also identified different perspectives of the problem as they become apparent in a cross-country comparison, ranging from the purely technical to the more complex national security focus.

In the majority of countries, the law-enforcement/cyber-crime perspective has emerged as the most prominent one, due to the nature of the threat, the resources that were available to the law enforcement community, and cultural and legal norms, because they restrict the number of potential strategies available for selection. Thus, one key issue for all countries is the harmonization of the law to facilitate the prosecution of cyber-perpetrators. The most important legislative instrument in this area is the Council of Europe Cybercrime Convention. Even though the implementation of this convention will likely make us aware of the practical difficulties behind such an endeavour, the development of lowest common denominators in this field indicates a global understanding of issues.

In this domain, the basis for a global culture of cybersecurity has naturally emerged from a common need on the part of the nation-states: There can be no question that the world-wide scope of the Internet demands an international approach, even though any cyber-perpetrator is a physical entity in a physical location with an Internet connection. In other domains, such a culture might be a lot further away. The dilemma we have identified in the last chapter may also carry the seed of destruction: due to the nature of the technological environment, military plans to engage in computer network operations and to attack and harm an adversary mean that the chances for a global culture of cybersecurity are considerably diminished. There is a need for a common understanding of threats and needs, an understanding that can only be fostered if all relevant stakeholders find a common language to address these issues. Equipped with such a common understanding, the many stakeholders will no longer have to pull on the strands that seem most promising, but will be able to systematically untangle those strands that have hitherto kept the community from developing a global culture of cybersecurity.

6 REFERENCES

1 World Summit on the Information Society (2003a): Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium. Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003. URL: http://www.itu.int/wsis/docs/geneva/official/dop.html [last accessed on 10 June 2005].

2 In UN resolution 57/239 of December 2002, the UN General Assembly outlined elements for creating a global culture of cybersecurity, inviting member states and all relevant international organizations to take account of them in their preparations for the Summit. In December 2003, UN resolution 58/199 further emphasized the promotion of a global culture of cybersecurity and the protection of critical information infrastructures.

3 World Summit on the Information Society (2003b): Plan of Action. Document WSIS-03/GENEVA/DOC/5-E, 12 December 2003. URL: http://www.itu.int/wsis/docs/geneva/official/poa.html [last accessed on 10 June 2005].

4 World Summit on the Information Society, 2003b.

5 See: Porter, Charlene (2003): U.S. Outlines Priorities for World Summit on the Information Society: Commitment to Private Sector, Rule of Law Critical for Infrastructure Development, US State Department, December 2003. URL: http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2003&m=December&x=20031203163730retropc0.0570032&t=usinfo/wf-latest.html [last accessed on 10 June 2005].

6 Stoll, Cliff (1990): The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage (New York: Pocket Books).

7 Clarke, Richard and Lee Zeichner (2004): Beyond the Moat: New Strategies for Cybersecurity, in: Bank Systems & Technology, January 27. URL: http://www.banktech.com/showArticle.jhtml?articleID=17501355 [last accessed on 10 June 2005].

8 Security Statistics – Virus Statistics. URL: http://www.securitystats.com/virusstats.html [last accessed on 10 June 2005].

9 ICSA Labs 2003 Virus Prevalence Survey. URL: http://www.icsalabs.com/2003avpsurvey/index.shtml; ICSA Labs 2002 Virus Prevalence Survey. URL: http://www.icsalabs.com/2002avpsurvey/index.shtml [last accessed on 10 June 2005].

10 Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2003): Threat Analysis, no. TA03-001. URL: http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf [last accessed on 10 June 2005].

11 Myriam Dunn and Isabelle Wigert (2004): The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies). The following countries are included in the 2004 edition: Australia, Austria, Canada, Finland, France, Germany, Italy, Netherlands, New Zealand, Norway, Sweden, Switzerland, United Kingdom, and the United States. The third edition is forthcoming in 2006 and will have two volumes: The first volume will feature 20 country surveys, and the second volume offers in-depth analysis of key issues.

12 Dunn, Myriam (forthcoming 2006): Cyber-threats and Countermeasures. Explaining the Threat Politics behind Efforts to Secure the Information Age.

13 Dunn, Myriam (2004): Cyber-Threats and Countermeasures: Towards an Analytical Framework for Explaining Threat Politics in the Information Age. Conference paper, SGIR Fifth Pan-European IR Conference, The Hague, 10 September. URL http://www.sgir.org/conference2004/papers/Dunn%20-%20Cyber-Threats%20and%20countermeasures.pdf [last accessed on 10 June 2005].

14 French, Geoffrey S. (2000): Shunning the Frumious Bandersnatch: Current Literature on Information Warfare and Deterrence. The Terrorism Research Center.

15 Wiener, Norbert (1948): Cybernetics, or Control and Communication in the Animal and Machine (Cambridge: MIT Press); Ashby, W. Ross (1956): Introduction to Cybernetics (Methuen, London).

16 Gibson, William (1984): Neuromancer (New York: Ace Books).

17 Lynch, Keith (2003): Keith Lynch's timeline of net related terms and concepts. URL: http://keithlynch.net/timeline.html. Last updated July 8th, 2003 [last accessed on 10 June 2005].

18 Dyson, Esther, George Gilder, George Keyworth, and Alvin Toffler (1994): Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Progress & Freedom Foundation).

19 Fischer, Eric A. (2005): Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, February 22, CRS Report for Congress, Order Code RL32777.

20 Wikipedia: http://en.wikipedia.org/wiki/Security [last accessed on 10 June 2005].

21 Wolfers, Arnold (1962): National Security as an Ambiguous Symbol, in: Idem: Discord And Collaboration: Essays on International Politics (Baltimore: Johns Hopkins): pp. 147-165; Baldwin, D.A. (1997): The Concept of Security, in: Review of International Studies, l 3,13; Goldman, Emily O. (2001): New Threats, New Identities and New Ways of War: The Sources of Change in National Security Doctrine, in: Journal of Strategic Studies, 24, 3: pp. 12-42.

22 Wikipedia: http://en.wikipedia.org/wiki/Security [last accessed on 10 June 2005].

23 Wikipedia: http://en.wikipedia.org/wiki/National_security [last accessed on 10 June 2005].

24 Dunn, forthcoming 2006.

25 Fischer, 2005.

26 Stoneburner, Gary (2001): Computer Security. Underlying Technical Models for Information Technology Security. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-33. (Washington, D.C.: U.S. Government Printing Office). URL: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf [last accessed on 10 June 2005].

27 Ibid.

28 Wikipedia: http://en.wikipedia.org/wiki/Information_security [last accessed on 10 June 2005].

[29] Ibid.

[30] Dunn and Wigert, 2004.

[31] Alberts, David S. and Daniel S. Papp (1997) (eds.): The Information Age: An Anthology of Its Impacts and Consequences (Washington D.C., National Defense University); Dunn, Myriam (2002): Information Age Conflicts: A Study on the Information Revolution and a Changing Operating Environment. Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 64 (Zurich: Center for Security Studies): pp. 59-64.

[32] Eriksson, Johan (2001) (ed.): Threat Politics: New Perspectives on Security, Risk and Crisis Management. (Ashgate: Aldershot); Eriksson, Johan (1999): Agendas, Threats, and Politics. Securitization in Sweden, paper presented at the ECPR Joint Sesssions, workshop 'Redefining Security', Mannheim (26-31 March 1999).

[33] Kolet, Kristin S. (2001): Asymmetric Threats to the United States, in: Comparative Strategy, 20: pp. 277-292.

[34] Alberts, David S., Daniel S. Papp, and W. Thomas Kemp III (1997): The Technologies of the Information Revolution, in: Alberts, David S. and Daniel S. Papp (eds.): The Information Age: An Anthology of Its Impacts and Consequences. (Washington D.C., National Defense University).

[35] Kushnick, Bruce (1999): The Unauthorized Biography of the Baby Bells & Info-Scandal (New Networks Institute): p. 22.

[36] Ellison, R. J., D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead (1997): Survivable Network Systems: An Emerging Discipline. November 1997: Technical Report. CMU/SEI-97-TR-013. ESC-TR-97-013. URL: http://www.cert.org/research/97tr013.pdf [last accessed on 10 June 2005].

[37] Arquilla, John and David F. Ronfeldt (1996): The Advent of Netwar (Santa Monica: RAND); Arquilla, John and David Ronfeldt (eds.) (2001): Networks and Netwars: The Future of Terror, Crime, and Militancy (Santa Monica: RAND); Castells, Manuel (1996): The Rise of the Network Society (Oxford: Blackwell).

[38] Dunn and Wigert, 2004; OCIPEP, 2003.

[39] Batelle (2004): Technology Forecast - Strategic Technologies for 2020. URL: http://www.battelle.org/forecasts/technology2020.stm [last accessed on 10 June 2005].

[40] Virilio, Paul (1995): Speed and Information: Cyberspace Alarm!, in: Ctheory, 18 March 1995.

[41] Hundley, Richard O. and Robert H. Anderson (1997): Emerging Challenge: Security and Safety in Cyberspace, in: Arquilla, John and David Ronfeldt (eds.): In Athena's Camp: Preparing for Conflict in the Information Age (Santa Monica: RAND, 1997): pp. 231-252; Chapman, Gary (1998): National Security and the Internet, paper presented at the Annual Convention of the Internet Society (Geneva, July 1998); Halperin, David (2000): The Internet and National Security: Emerging Issues, in: Alberts, David S., Daniel S. Papp (eds.): The Information Age: An Anthology of Its Impacts and Consequences, Volume II (Washington: National Defense University Press): pp. 137-73; Campen, Alan (1992): The First Information Warfare (Fairfax, AFCEA International Press); Campen, Alan D. and Douglas H. Dearth (eds.) (1998): Cyberwar 2.0: Myths, Mysteries and Reality (Fairfax, AFCEA International Press).

[42] Dekker, Marcel (1997): Security of the Internet, in: The Froehlich/Kent Encyclopedia of Telecommunications, vol. 15 (New York): pp. 231-55. URL: http://www.cert.org/encyc_article/tocencyc.html [last accessed on 10 June 2005]; Papp, Daniel S. (2003): Cyberterrorism: Threat(?) And Response, paper given at the CEEISA/ISA International Convention, Budapest, Hungary, June 26 -28, 2003.

[43] Näf, Michael (2001): Ubiquitous Insecurity? How to "Hack" IT Systems, in: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Volume 7: pp. 104-18.

[44] Ellison et al., 1997.

[45] Akdeniz, Yaman (1999): The Regulation of Internet Content in Europe: Governance Control versus Self-Responsibility, in: Swiss Political Science Review, 5, 2: pp. 123-31; Cukier, Kenneth Neil (1999): Internet Governance and the Ancien Regime, in: Swiss Political Science Review, 5, 1: pp. 127-33; Baird, Zoë (2002): Governing the Internet: Engaging Government, Business, and Nonprofits, in: Foreign Affairs, 81, 6, pp. 15-20; Giacomello, Giampiero (1999): Taming the Net? The Issue of Government Control on the Internet, in: Swiss Political Science Review, 5, 2: pp. 116-22.

[46] Strogatz, Steven H. (2001): Exploring Complex Networks, in: Nature, 410 (8 March 2001): pp. 268-276.

[47] Rathmell, Andrew (2001): Controlling Computer Network Operations, in: Wenger, Andreas (ed): The Internet and the Changing Face of International Relations and Security, Information & Security An International Journal, Volume 7: pp. 121-44.

[48] Näf, 2001.

[49] Luiijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver (2003): Critical Infrastructure Protection in the Netherlands: A Quick-scan, in: Gattiker, Urs E., Pia Pedersen and Karsten Petersen (eds.): EICAR Conference Best Paper Proceedings. URL: http://www.tno.nl/instit/fel/refs/pub2003/BPP-13-CIP-Luiijf&Burger&Klaver.pdf [last accessed on 10 June 2005].

[50] Eriksson, 2001a.

[51] Moteff, John, Claudia Copeland, and John Fischer (2002): Critical Infrastructures: What Makes an Infrastructure Critical? CRS (Congressional Research Service) Report for Congress RL31556. (30 August 2002); Metzger, Jan (2004): The Concept of Critical Infrastructure Protection (CIP), in: Bailes, A. J. K. and Isabelle Frommelt (eds.): Business and Security: Public-Private Sector Relationships in a New Security Environment (Oxford University Press: Oxford): pp. 197-209.

[52] Yates, Athol (2003): Engineering a Safer Australia: Securing Critical Infrastructure and the Built Environment. (Institution of Engineers, Australia). URL: http://www.ieaust.org.au/SafeAustralia/Engineering%20a%20Safer%20Aust.pdf) [last accessed on 10 June 2005].

[53] Moteff, John D. (2003): Critical Infrastructures: Background, Policy, and Implementation. CRS (Congressional Research Service) Report for Congress. (Updated 10 February, 2003).URL: http://www.fas.org/irp/crs/RL30153.pdf [last accessed on 10 June 2005].

[54] Ellison et al., 1997.

[55] Avizienis et al., 2000; OCIPEP, 2003.

[56] Ellison et al., 1997:3.

[57] U.S. Secret Service and Carnegie Mellon University Software Engineering Institute (2005): Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. URL: http://www.secretservice.gov/ntac_its.shtml [last accessed on 10 June 2005].

[58] President's Commission on Critical Infrastructure Protection (1997) (PCCIP): Critical Foundations: Protecting America's Infrastructures. (Washington, D.C., October 1997); National Academy of Sciences, Computer Science and Telecommunications Board (1991): Computers at Risk: Safe Computing in the Information Age (Washington D.C.: National Academy Press).

[59] Levy, Steven (1984): Hackers Heroes of the Computer Revolution (New York: Anchor Press); Erickson, Jon (2003): Hacking: The Art of Exploitation (San Francisco: No Starch Press); OCIPEP, 2003.

[60] Denning, Dorothy E (1999): Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, presented at Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop, 10 December).

[61] Denning, Dorothy (2001): Is Cyber-terror Next? Essay for the Social Science Research Council, after September 11. URL: http://www.ssrc.org/sept11/essays/denning.htm [last accessed on 10 June 2005].

[62] National Academy of Sciences, 1991.

[63] Minihan, Kenneth A. (1998): Prepared statement before the Senate Governmental Affairs Committee, 24 June 1998.

[64] Krutskikh, Andrei (1999): Information Challenges to Security, in: International Affairs, 45, 2: pp. 29-37; Sibilia, Riccardo (1997): Informationskriegsführung: eine schweizerische Sicht (Zürich: Institut für militärische Sicherheitstechnik, ETH Zürich).

[65] CSO Magazine, United States Secret Service and CERT® Coordination Center. (2004): 2004 E-Crime Watch Survey (Framingham, MA: CXO Media).

[66] Cashell, Brian, William D. Jackson, Mark Jickling, and Baird Webel (2004): The Economic Impact of Cyber-Attacks, Congressional Research Service Documents, CRS RL32331 (Washington).

[67] Westrin, Peter (2001): Critical Information Infrastructure Protection, in: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Volume 7: pp. 67-79.

[68] Examples: 1) In 1998, a 12-year old hacked the system running the Roosevelt Dam (AZ), which retains up to 489 trillion gallons. Mesa and Tempe are downstream, with a combined population of 1 million; 2) In early 2000, a 48-year old disgruntled worker hacked into Queensland's wastewater system, managing to create pumping station failures causing approximately 1 million litres of sewage to spill into parks, waterways, and the grounds of a tourist resort; 3) The SoBig virus affected the CSX transportation system, halting train service for 4-6 hours along the Northeast corridor of the U.S. in August 2003; 4) The Sasser worm took out several oil platforms in the Gulf of Mexico in the Spring of 2004.

[69] Dunn, forthcoming 2006; Dunn, Myriam (2004): Threat Frames in the US Cyber-Terror Discourse, paper presentation at the 2004 British International Studies Association (BISA) Conference, Warwick, 21 December 2004.

[70] Buzan, Barry, Ole Wæver and Jaap de Wilde (1998): Security: A New Framework for Analysis (Boulder: Rienner).

[71] Huysmans, Jef (1998): Security! What do you mean? From Concept to Thick Signifier, in: European Journal of International Relations, 4, 2: pp. 226-55.

[72] PCCIP, 1997: 14.

[73] Goldman, 2001:45

[74] Dunn, Myriam (2005): The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP), in: International Journal for Critical Infrastructure Protection, 1, 2/3: pp. 58-68; Ingles-le Nobel, Johan J. (1999): Cyberterrorism Hype, in: Jane's Intelligence Review, 10/21/1999; Center for the Study of Terrorism and Irregular Warfare (1999): Cyberterror: Prospects and Implications. White Paper; Green, Joshua (2002): The Myth of Cyberterrorism, in: Washington Monthly, November 2002; Shea, Dana A. (2003): Critical Infrastructure: Control Systems and the Terrorist Threat. CRS Report for Congress, February 21, 2003. URL: http://www.fas.org/irp/crs/RL31534.pdf [last accessed on 10 June 2005]; Denning, 2001; Technical Analysis Group, Institute for Security Technology Studies, Darthmouth College (2003). Examining the Cyber Capabilities of Islamic Terrorist Groups. URL: https://www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf [last accessed on 10 June 2005].

[75] Bendrath, Ralf (2003): The American Cyber-Angst and the Real World – Any Link? in: Robert Latham (ed.): Bombs and Bandwidth: The Emerging Relationship between IT and Security (New York: The New Press), pp. 49-73.

[76] Dunn and Wigert 2004.

[77] PCCIP, 1997: Appendix B, Glossary, B-2.

[78] Moteff, John, Claudia Copeland, and John Fischer (2003): Critical Infrastructures: What Makes an Infrastructure Critical? CRS (Congressional Research Service) Report for Congress RL31556, 30 August 2002. URL: http://www.fas.org/irp/crs/RL31556.pdf [last accessed on 10 June 2005].

[79] Metzger, 2004.

[80] For an example (critical assessment without interdependencies), see: United States General Accounting Office. Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations; House Committee on Government Reform, Homeland Security: Key Elements of a Risk Management, Statement of Raymond J. Decker, Director Defense Capabilities and Management, 12 October 2001, p. 6. http://www.house.gov/reform/ns/statements_witness/GAO-02-150T.pdf [last accessed on 10 June 2005].

[81] Metzger, 2004.

[82] Westrin, 2001.

[83] PCCIP, 1997: Appendix B, Glossary, B-2.

[84] Clinton, William J. (1998): Protecting America's Critical Infrastructures: Presidential Decision Directive 63 (The White House, Washington D.C., 22 May 1998). URL: http://www.fas.org/irp/offdocs/pdd-63.htm [last accessed on 10 June 2005].

[85] Metzger, 2004.

[86] Cf. CRN Workshop on "Critical Infrastructure Protection in Europe – Lessons Learned and Steps Ahead", Zurich 9-10 November 2001), proceedings available online at: www.isn.ethz.ch/crn.

[87] Baird, 2002.

[88] Goodman, Seymour E., Pamala B. Hassebroek, Daving Kind, and Andy Azment (2002): International Coordination to Increase the Security of Critical Network Infrastructures, Document CNI/04, paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures, Seoul (20-22 May 2002); Bosch, Olivia (2002): Cyber Terrorism and Private Sector Efforts for Information Infrastructure Protection, paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures (Seoul, 20-22 May 2002).

[89] Goodman et al., 2002.

[90] Finnish Communications Regulatory Authority (2202): Information Security Review Related to the National Information Security Strategy (24 May 2002). URL http://www.ficora.fi/englanti/document/review.pdf [last accessed on 10 June 2005].

[91] Schmitz, Walter (2003): ACIP D6.4 Comprehensive Roadmap - Analysis and Assessment for CIP. Work Package 6, Deliverable D6.4, Version 1 (European Commission Information Society Technology Programme, May).

[92] EU-US Workshop Report, R&D Strategy for a dependable information society: EU-US collaboration, 1-2 December 2001 (Düsseldorf, Germany), available from www.ddsi.org.

[93] DDSI (2002), R&D Strategy Roadmap for Information Infrastructure Dependability, November 2002, p. 17.

[94] Dunn, 2005

[95] Dunn, Myriam and Isabelle Wigert (2003): The International CIIP Handbook 2004: Findings and Prospects, in: The CIP Report, 2, 6, December: p 7, 13-14.

[96] Westrin, 2001.

[97] Dunn, 2005.

[98] Ibid.; Bendrath, 2003.

[99] Dunn, forthcoming 2006.

[100] Buzan et al. 1998; Bourdieu, Pierre (1991): Language and Symbolic Power (Cambridge: Harvard University Press).

[101] Howarth, David (1995): Discourse Theory, in: March D. and G. Stoker (eds.): Theory and Methods of Political Science (London: Macmillan): p 132.

[102] Bigo, Didier (2000): When Two Becomes One: Internal and External Securitisation in Europe, in: Kelstrup, Morten and Michael C. Williams (eds.): International Relations Theory and the Politics of European Integration: Power, Security and Community (London: Routledge).

[103] Bendrath 2003; Dunn, forthcoming 2006.

[104] Bendrath, Ralf (2001): The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection, in: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Volume 7: pp. 80-103.

[105] Eriksson, Anders E. (1999): Information Warfare: Hype Or Reality? in: The Non-Proliferation Review, 6, 3.

[106] Goodman et al., 2002.

[107] Gelbstein, Eduardo and Ahmad Kamal (2002): Information Insecurity. A Survival Guide to the Uncharted Territories of Cyberthreats and Cybersecurity. United Nations ICT Task Force and United Nations Institute for Training and Research (New York, November 2002). URL: http://www.un.int/unitar/patit/dev/old%20site/curriculum/Information_Insecurity_Second_Edition_PDF.pdf [last accessed on 10 June 2005].

[108] World Summit on the Information Society, 2003a.

[109] Krasner, Stephen D. (ed.) (1984): International Regimes (Ithaca: Cornell University Press): p. 2.

[110] Giacomello, Giampiero and Fernando Mendez (2001): Cuius Regio, Eius Religio, Omnium Spatium? State Sovereignty in the Age of the Internet, in: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, 7: pp. 15-27.

[111] Rathmell, 2001.

[112] Ibid.

[113] Wikipedia: http://en.wikipedia.org/wiki/Game_theory [last accessed on 10 June 2005].

[114] Council of Europe Convention on Cybercrime. URL: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [last accessed on 10 June 2005].

[115] http://www.uncitral.org/english/workinggroups/wg_ec/index.htm [last accessed on 10 June 2005].

[116] http://www.commoncriteriaportal.org/ [last accessed on 10 June 2005].

[117] The International Organization for Standardization ISO has developed a code of practice for information security management (ISO/IEC 17799:2000). URL: http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html [last accessed on 10 June 2005]; The Organisation for Economic Co-operation and Development (OECD) promotes a "culture of security" for information systems and networks. URL: http://www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html [last accessed on 10 June 2005].

[118] Council of Europe Convention on Cybercrime. URL: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [last accessed on 10 June 2005].

[119] Press Statement (2001): The Convention on Cybercrime, a Unique Instrument for International Co-operation. URL: http://press.coe.int/cp/2001/893a(2001).htm [last accessed on 10 June 2005].

[120] Taylor, Greg (no date): The Council of Europe Cybercrime Convention. A civil liberties perspective. URL: http://www.crime-research.org/library/CoE_Cybercrime.html [last accessed on 10 June 2005].

[121] World Summit on the Information Society, 2003a.

[122] Rathmell, 2001.

[123] Heinrich Böll Stiftung (2001): Perspectives for Peace Policy in the Age of Computer Network Attacks, Conference Proceedings. URL: http://www.boell.de/downloads/medien/DokuNr20.pdf [last accessed on 10 June 2005].

[124] Dorothy E. Denning (2001): Obstacles and Options for Cyber Arms Controls, paper presented at Arms Control in Cyberspace Conference, Heinrich Böll Foundation, Berlin, Germany, June 29-30. URL: http://www.cs.georgetown.edu/~denning/infosec/berlin.doc [last accessed on 10 June 2005].

[125] Ibid.

[126] Ibid.

[127] Ibid.

[128] Porteous, Holly (1999): Some Thoughts on Critical Information Infrastructure Protection, in: Canadian IO Bulletin, 2, 4, October. URL: http://www.ewa-canada.com/Papers/IOV2N4.htm [last accessed on 10 June 2005].

7 BIBLIOGRAPHY

Akdeniz, Yaman (1999): The Regulation of Internet Content in Europe: Governance Control versus Self-Responsibility, in: Swiss Political Science Review, 5, 2: pp. 123-31.

Alberts, David S. and Daniel S. Papp (1997) (eds.): The Information Age: An Anthology of Its Impacts and Consequences (Washington D.C., National Defense University).

Alberts, David S., Daniel S. Papp, and W. Thomas Kemp III (1997): The Technologies of the Information Revolution, in: Alberts, David S. and Daniel S. Papp (eds.): The Information Age: An Anthology of Its Impacts and Consequences. (Washington D.C., National Defense University).

Arquilla, John and David F. Ronfeldt (1996): The Advent of Netwar (Santa Monica: RAND).

Arquilla, John and David Ronfeldt (eds.) (2001): Networks and Netwars: The Future of Terror, Crime, and Militancy (Santa Monica: RAND).

Ashby, W. Ross (1956): Introduction to Cybernetics (Methuen, London).

Baird, Zoë (2002): Governing the Internet: Engaging Government, Business, and Nonprofits, in: Foreign Affairs, 81, 6, pp. 15-20.

Baldwin, D.A. (1997): The Concept of Security, in: Review of International Studies, l 3,13: pp. 5-26.

Bendrath, Ralf (2001): The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection, in: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Volume 7: pp. 80-103.

Bendrath, Ralf (2003): The American Cyber-Angst and the Real World – Any Link?, in: Robert Latham (ed.): Bombs and Bandwidth: The Emerging Relationship between IT and Security (New York: The New Press), pp. 49-73.

Bigo, Didier (2000): When Two Becomes One: Internal and External Securitisation in Europe, in: Kelstrup, Morten and Michael C. Williams (eds.): International Relations Theory and the Politics of European Integration: Power, Security and Community (London: Routledge).

Bosch, Olivia (2002): Cyber Terrorism and Private Sector Efforts for Information Infrastructure Protection, paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures (Seoul, 20-22 May 2002).

Bourdieu, Pierre (1991): Language and Symbolic Power (Cambridge: Harvard University Press).

Buzan, Barry, Ole Wæver, and Jaap de Wilde (1998): Security: A New Framework for Analysis (Boulder: Rienner).

Campen, Alan (1992): The First Information Warfare (Fairfax, AFCEA International Press).

Campen, Alan D. and Douglas H. Dearth (eds.) (1998): Cyberwar 2.0: Myths, Mysteries and Reality (Fairfax, AFCEA International Press).

Cashell, Brian, William D. Jackson, Mark Jickling, and Baird Webel (2004): The Economic Impact of Cyber-Attacks, Congressional Research Service Documents, CRS RL32331 (Washington DC).

Castells, Manuel (1996): The Rise of the Network Society (Oxford: Blackwell).

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

Chapman, Gary (1998): National Security and the Internet, paper presented at the Annual Convention of the Internet Society (Geneva, July 1998).

Clarke, Richard and Lee Zeichner (2004): Beyond the Moat: New Strategies for Cybersecurity, in: Bank Systems & Technology, January 27. URL: http://www.banktech.com/showArticle.jhtml?articleID=17501355 [last accessed on 10 June 2005].

CSO Magazine, United States Secret Service and CERT® Coordination Center. (2004): 2004 E-Crime Watch Survey (Framingham, MA: CXO Media).

Cukier, Kenneth Neil (1999): Internet Governance and the Ancien Regime, in: Swiss Political Science Review, 5, 1: pp. 127-33.

Dekker, Marcel (1997): Security of the Internet, in: The Froehlich/Kent Encyclopedia of Telecommunications, vol. 15 (New York: Marcel Dekker): pp. 231-55. URL: http://www.cert.org/encyc_article/tocencyc.html [last accessed on 10 June 2005.

Denning, Dorothy (2001): Is Cyber-terror Next? Essay for the Social Science Research Council, after September 11. URL: http://www.ssrc.org/sept11/essays/denning.htm [last accessed on 10 June 2005].

Denning, Dorothy E (1999): Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, presented at Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop, 10 December).

Dorothy E. Denning (2001): Obstacles and Options for Cyber Arms Controls, paper presented at Arms Control in Cyberspace Conference, Heinrich Böll Foundation, Berlin, Germany, June 29-30. URL: http://www.cs.georgetown.edu/~denning/infosec/berlin.doc [last accessed on 10 June 2005].

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

Dunn, Myriam (2004): Cyber-Threats and Countermeasures: Towards an Analytical Framework for Explaining Threat Politics in the Information Age. Conference paper, SGIR Fifth Pan-European IR Conference, the Hague, 10 September. URL http://www.sgir.org/conference2004/papers/Dunn%20-%20Cyber-Threats%20and%20countermeasures.pdf [last accessed on 10 June 2005].

Dunn, Myriam (2004): Threat Frames in the US Cyber-Terror Discourse, paper presentation at the 2004 British International Studies Association (BISA) Conference, Warwick, 21 December 2004.

Dunn, Myriam (2005): The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP), in: International Journal for Critical Infrastructure Protection, 1, 2/3: pp. 58-68.

Dunn, Myriam (forthcoming 2006): Cyber-threats and Countermeasures. Explaining the Threat Politics behind Efforts to Secure the Information Age.

Dunn, Myriam and Isabelle Wigert (2003): The International CIIP Handbook 2004: Findings and Prospects, in: The CIP Report, 2, 6, December: p 7, 13-14.

Dyson, Esther, George Gilder, George Keyworth, and Alvin Toffler (1994): Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Washington: Progress & Freedom Foundation).

Ellison, R. J., D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead (1997): Survivable Network Systems: An Emerging Discipline. November 1997: Technical Report. CMU/SEI-97-TR-013. ESC-TR-97-013. URL: http://www.cert.org/research/97tr013.pdf [last accessed on 10 June 2005].

Eriksson, Anders E. (1999): Information Warfare: Hype Or Reality?, in: The Non-Proliferation Review, 6, 3: pp. 57-64.

Eriksson, Johan (1999): Agendas, Threats, and Politics. Securitization in Sweden, paper presented at the ECPR Joint Sesssions, workshop 'Redefining Security', Mannheim (26-31 March 1999).

Eriksson, Johan (2001) (ed.): Threat Politics: New Perspectives on Security, Risk and Crisis Management. (Aldershot : Ashgate).

Fischer, Eric A. (2005): Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, February 22, CRS Report for Congress, Order Code RL32777. URL: http://www.usembassy.it/pdf/other/RL32777.pdf [last accessed on 10 June 2005].

French, Geoffrey S. (2000): Shunning the Frumious Bandersnatch: Current Literature on Information Warfare and Deterrence (Washington DC: Information Warfare Research Center).

Gelbstein, Eduardo and Ahmad Kamal (2002): Information Insecurity. A Survival Guide to the Uncharted Territories of Cyber-Threats and Cybersecurity. United Nations ICT Task Force and United Nations Institute for Training and Research (New York, November 2002). URL: http://www.un.int/unitar/patit/dev/old%20site/curriculum/Information_Insecurity_Second_Edition_PDF.pdf [last accessed on 10 June 2005].

Giacomello, Giampiero (1999): Taming the Net? The Issue of Government Control on the Internet, in: Swiss Political Science Review, 5, 2: pp. 116-22.

Giacomello, Giampiero and Fernando Mendez (2001): Cuius Regio, Eius Religio, Omnium Spatium? State Sovereignty in the Age of the Internet, in: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, 7: pp. 15-27.

Gibson, William (1984): Neuromancer (New York: Ace Books).

Goldman, Emily O. (2001): New Threats, New Identities and New Ways of War: The Sources of Change in National Security Doctrine, in: Journal of Strategic Studies, 24, 3: pp. 12-42.

Goodman, Seymour E., Pamala B. Hassebroek, Daving Kind, and Andy Azment (2002): International Coordination to Increase the Security of Critical Network Infrastructures, Document CNI/04, paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures, Seoul (20-22 May 2002).

Green, Joshua (2002): The Myth of Cyberterrorism, in: Washington Monthly, November 2002.

Halperin, David (2000): The Internet and National Security: Emerging Issues, in: Alberts, David S., Daniel S. Papp (eds.): The Information Age: An Anthology of Its Impacts and Consequences, Volume II (Washington: National Defense University Press): pp. 137-73.

Heinrich Böll Stiftung (2001): Perspectives for Peace Policy in the Age of Computer Network Attacks, Conference Proceedings. URL: http://www.boell.de/downloads/medien/DokuNr20.pdf [last accessed on 10 June 2005].

Howarth, David (1995): Discourse Theory, in: March, D. and G. Stoker (eds.): Theory and Methods of Political Science (London: Macmillan): pp. 115-33.

Hundley, Richard O. and Robert H. Anderson (1997): Emerging Challenge: Security and Safety in Cyberspace, in: Arquilla, John and David Ronfeldt (eds.): In Athena's Camp: Preparing for Conflict in the Information Age (Santa Monica: RAND, 1997): pp. 231-252.

Huysmans, Jef (1998): Security! What do you mean? From Concept to Thick Signifier, in: European Journal of International Relations, 4, 2: pp. 226-55.

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

Kolet, Kristin S. (2001): Asymmetric Threats to the United States, in: Comparative Strategy, 20, 3: pp. 277-292.

Krasner, Stephen D. (ed.) (1984): International Regimes (Ithaca: Cornell University Press).

Kushnick, Bruce (1999): The Unauthorized Biography of the Baby Bells & Info-Scandal (New York: New Networks Institute).

Levy, Steven (1984): Hackers Heroes of the Computer Revolution (New York: Anchor Press); Erickson, Jon (2003): Hacking: The Art of Exploitation (San Francisco: No Starch Press).

Luiijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver (2003): Critical Infrastructure Protection in the Netherlands: A Quick-scan, in: Gattiker, Urs E., Pia Pedersen and Karsten Petersen (eds.): EICAR Conference Best Paper Proceedings. URL: http://www.tno.nl/instit/fel/refs/pub2003/BPP-13-CIP-Luiijf&Burger&Klaver.pdf [last accessed on 10 June 2005].

Lynch, Keith (2003): Keith Lynch's timeline of net related terms and concepts. URL: http://keithlynch.net/timeline.html. Last updated July 8th, 2003 [last accessed on 10 June 2005].

Metzger, Jan (2004): The Concept of Critical Infrastructure Protection (CIP), in: Bailes, A. J. K. and Isabelle Frommelt (eds.): Business and Security: Public-Private Sector Relationships in a New Security Environment (Oxford University Press: Oxford): pp. 197-209.

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

Moteff, John D. (2003): Critical Infrastructures: Background, Policy, and Implementation. CRS (Congressional Research Service) Report for Congress (Updated 10 February, 2003).URL: http://www.fas.org/irp/crs/RL30153.pdf [last accessed on 10 June 2005].

Moteff, John, Claudia Copeland, and John Fischer (2002): Critical Infrastructures: What Makes an Infrastructure Critical? CRS (Congressional Research Service) Report for Congress RL31556 (30 August 2002).

Moteff, John, Claudia Copeland, and John Fischer (2003): Critical Infrastructures: What Makes an Infrastructure Critical? CRS (Congressional Research Service) Report for Congress RL31556 (30 August 2002). URL: http://www.fas.org/irp/crs/RL31556.pdf [last accessed on 10 June 2005].

Myriam Dunn and Isabelle Wigert (2004): The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies). The following countries are included in the 2004 edition: Australia, Austria, Canada, Finland, France, Germany, Italy, Netherlands, New Zealand, Norway, Sweden, Switzerland, United Kingdom, and the United States.

Näf, Michael (2001): Ubiquitous Insecurity? How to "Hack" IT Systems, in: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Volume 7: pp. 104-18.

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

Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2003): Threat Analysis, no. TA03-001. URL: http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf [last accessed on 10 June 2005].

Papp, Daniel S. (2003): Cyberterrorism: Threat (?) And Response, paper given at the CEEISA/ISA International Convention, Budapest, Hungary, June 26 -28, 2003.

Porteous, Holly (1999): Some Thoughts on Critical Information Infrastructure Protection, in: Canadian IO Bulletin, 2, 4, October. URL: http://www.ewa-canada.com/Papers/IOV2N4.htm [last accessed on 10 June 2005].

Porter, Charlene (2003): U.S. Outlines Priorities for World Summit on the Information Society; Commitment to private sector, rule of law critical for infrastructure development, US State Department, December 2003. URL: http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2003&m=December&x=20031203163730retropc0.0570032&t=usinfo/wf-latest.html [last accessed on 10 June 2005].

President's Commission on Critical Infrastructure Protection (1997) (PCCIP): Critical Foundations: Protecting America's Infrastructures. (Washington, D.C.: White House).

Rathmell, Andrew (2001): Controlling Computer Network Operations, in: Wenger, Andreas (ed): The Internet and the Changing Face of International Relations and Security, Information & Security An International Journal, Volume 7: pp. 121-44.

Schmitz, Walter (2003): ACIP D6.4 Comprehensive Roadmap - Analysis and Assessment for CIP. Work Package 6, Deliverable D6.4, Version 1 (European Commission Information Society Technology Programme, May).

Shea, Dana A. (2003): Critical Infrastructure: Control Systems and the Terrorist Threat. CRS Report for Congress (February 21, 2003). URL: http://www.fas.org/irp/crs/RL31534.pdf [last accessed on 10 June 2005].

Stoll, Cliff (1990): The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage (New York: Pocket Books).

Stoneburner, Gary (2001): Computer Security. Underlying Technical Models for Information Technology Security. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-33. (Washington, D.C.: U.S. Government Printing Office). URL: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf [last accessed on 10 June 2005].

Strogatz, Steven H. (2001): Exploring Complex Networks, in: Nature, 410 (8 March 2001): pp. 268-76.

Taylor, Greg (no date): The Council of Europe Cybercrime Convention. A Civil Liberties Perspective. URL: http://www.crime-research.org/library/CoE_Cybercrime.html [last accessed on 10 June 2005].

Technical Analysis Group, Institute for Security Technology Studies, Darthmouth College (2003). Examining the Cyber Capabilities of Islamic Terrorist Groups. URL: https://www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf [last accessed on 10 June 2005].

U.S. Secret Service and Carnegie Mellon University Software Engineering Institute (2005): Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. URL: http://www.secretservice.gov/ntac_its.shtml [last accessed on 10 June 2005].

Virilio, Paul (1995): Speed and Information: Cyberspace Alarm!, in: Ctheory, 18 March 1995.

Westrin, Peter (2001): Critical Information Infrastructure Protection, in: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Volume 7: pp. 67-79.

Wiener, Norbert (1948): Cybernetics, or Control and Communication in the Animal and Machine (Cambridge: MIT Press).

Wolfers, Arnold (1962): National Security as an Ambiguous Symbol, in: Idem: Discord And Collaboration: Essays on International Politics (Baltimore: Johns Hopkins): pp. 147-65.

World Summit on the Information Society (2003a): Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium. Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003. URL: http://www.itu.int/wsis/docs/geneva/official/dop.html [last accessed on 10 June 2005].

World Summit on the Information Society (2003b): Plan of Action. Document WSIS-03/GENEVA/DOC/5-E, 12 December 2003. URL: http://www.itu.int/wsis/docs/geneva/official/poa.html [last accessed on 10 June 2005].

Yates, Athol (2003): Engineering a Safer Australia: Securing Critical Infrastructure and the Built Environment. (Institution of Engineers, Australia). URL: http://www.ieaust.org.au/SafeAustralia/Engineering%20a%20Safer%20Aust.pdf) [last accessed on 10 June 2005].