CRN REPORT

Focal Report 3

Critical Infrastructure Protection

Cybersecurity – Recent Strategies and Policies: An Analysis

Zurich, August 2009

Crisis and Risk Network (CRN)
Center for Security Studies (CSS), ETH Zürich

Commissioned by the Federal Office for Civil Protection (FOCP)

CRN
Supported by ISN

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Purpose: As part of a larger mandate, the Swiss Federal Office for Civil Protection (FOCP) has tasked the Center for Security Studies (CSS) at ETH Zurich with compiling "focal reports" (Fokusberichte) on critical infrastructure protection and on risk analysis to promote discussion and provide information about new trends and insights.

Authors and Contributors: Elgin Brunner, Anna Michalkova, Manuel Suter, Myriam Dunn Cavelty

Contact:
Center for Security Studies
Seilergraben 45-49
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25

crn@sipo.gess.ethz.ch
www.crn.ethz.ch

Contracting entity: Federal Office for Civil Protection (FOCP)
Project lead FOCP: Stefan Brem, Head Risk Analysis and Research Coordination
Contractor: Center for Security Studies (CSS), ETH Zurich
Project supervision ETH-CSS: Myriam Dunn, Head New Risks Research Unit,
Andreas Wenger, Director CSS; Victor Mauer, Deputy Director CSS

TABLE OF CONTENTS

1 INTRODUCTION

In support of Switzerland's CIP efforts and CIP strategy development, the Swiss Federal Office for Civil Protection (FOCP) has tasked the Center for Security Studies (CSS) at ETH Zurich with producing focal reports (*Fokusberichte*) on critical infrastructure protection.

These focal reports are compiled using the following method: First, a "scan" of the environment is performed with the aim of searching actively for information that helps to expand and deepen the knowledge and understanding of the issue under scrutiny. This is a continuous process based on the following sources:

- *Internet Monitoring*: New publications and documents with a) a general CIP focus and b) a focus on scenarios with specific importance for the FOCP are identified and collected.
- *Science Monitoring*: Relevant journals are identified and regularly evaluated (with the same two focal points as specified above).
- *Government Monitoring*: The focus is on policy developments in the United States, Canada, Sweden, Norway, Denmark, Germany, the Netherlands, and the United Kingdom as well as other states in the European vicinity that are relevant to Switzerland.

Second, the material collected is filtered, analyzed, and summarized in the focal reports.[1]

This focal report concentrates on cybersecurity. *First*, cybersecurity is regarded as a key element of CIP since the mid 1990s. *Second*, in both previous reports, the growing and continued attention on the cyberspace dimension of CIP was identified as a trend. *Third*, many countries have recently launched new cybersecurity strategies or noteworthy policy papers on this topic:

- Most prominently, in May 2009, the administration of US President Barack Obama published the results of a 60-day review on cybersecurity, which was the starting point for a broad discussion on cybersecurity policy in the United States;[2]
- The United Kingdom released its cybersecurity strategy in June 2009;[3]
- Estonia published its strategy in October 2008;[4]
- The EU Commission issued a communication on Critical Information Infrastructure Protection in March 2009;[5]
- The NATO Parliamentary Assembly published a commission report entitled "NATO and Cyber Defence" in spring 2009;[6]
- In 2008, several other countries such as Sweden,[7] Japan,[8] or Belgium[9] published policy papers with regard to this topic.

1 Previous focal reports can be downloaded from the website of the Crisis and Risk Network CRN (*http://www.crn.ethz.ch*).

2 US Government. 2009. Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communication Inftrastructure. Available at: *http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*.

3 Cabinet Office of the United Kingdom. 2009. Cyber Security Strategy of the United Kingdom. Safety, Security and Resilience in Cyber Space. Available at: *http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf*.

4 Ministry of Defence of Estonia. 2008. Cyber Security Strategy. Available at: *http://mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf*.

5 Commission of the European Communities. 2009. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. Available at: *http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf*.

6 NATO Parliamentary Assembly. 2009. Committee Report 027 DSCFC 09 E - NATO and Cyber Defence.Available at: *http://www.nato-pa.int/default Asp?SHORTCUT=1782.*

7 Swedish Emergency Management Agency. 2008. Information Security in Sweden – Situational Assessment 2008. Available at: *http://www.krisberedskapsmyndigheten.se/upload/17461/lagesbedomning_infosakerhet_%202008_eng.pdf.*

The report at hand has four parts:

1. The first part focuses on a) cybersecurity definitions and b) threat perceptions – i.e., which threats the strategies identify and what is threatened according to these documents.
2. The second part looks at the proposed responses. In general, the strategies focus on four measures: public-private collaboration for incident response and prevention; public awareness-raising; institutional responses (creation of agencies responsible for cybersecurity); and international cooperation.
3. In the third part, this report discusses the findings with a special focus on the implications for Switzerland.
4. Finally, an annotated bibliography gives an overview of the major recent and relevant documents and articles on cybersecurity.

8 Information Security Policy Council. 2008. Secure Japan 2008 – Intensive Efforts for Enhancing Information Security Infrastructure. Available at: *http://www.nisc.go.jp/eng/pdf/sj2008_eng.pdf.*

9 Allard, J.L. et al. 2008. Towards a Belgian Strategy on Information Security. Available at: *http://www.lsec.be/upload_directories/documents/TowardsaBelgianStrategyonInformationSecurity_BISI_080908.pdf.*

2 (IN)SECURITY IN AND FROM CYBERSPACE: DEFINITIONS AND THREAT PERCEPTIONS

This chapter describes how different countries define the threats to cybersecurity and what they perceive to be the key threats.

2.1 Cybersecurity definitions

According to a recent Chatham House publication, cybersecurity can be defined as the absence of a threat either via or to Information and Communication Technologies (ICT) and networks. Simply put, this means that cybersecurity is the security one enjoys in and from cyberspace.[10] The cybersecurity strategies and policy papers studied for this focal report implicitly follow this definition, but they rarely provide a clear definition of cybersecurity. The UK Cyber Security Strategy states that "[c]yber security embraces both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers"[11]. The US Cyberspace Policy Review defines cybersecurity policy broadly as the "strategy, policy, and standards regarding the security of and operations in cyberspace".[12] Referring back to the definition given at the beginning of this chapter, how can security in and from cyberspace be at risk? Two levels can be distinguished:

1. Technical level: While it is a commonplace that our societies are entirely and pervasively dependent upon ICT, the complexity and interconnectedness of this dependence is growing. With dependence comes vulnerability. On the first level, this vulnerability is linked to the danger of *system failures* that may have cascading effects affecting not only the individual use of ICT, but crippling the smooth functioning of entire branches of societal activity and security.
2. Actor level: Triggered by the pervasive societal dependence upon information and communication technology, the second area of vulnerability is the one linked to potential *malevolent agency*. This level is the one more commonly associated with the threat imagery, as will be shown below. The panoply of malevolent agents deploying their activities in and/or through cyberspace is vast, but can be generally categorized into four elements. These include – in decreasing order of gravity – state-sponsored actors, ideological and politically extremist actors, frustrated insiders, organized criminal agents, and individual criminal agents.[13]

These two levels are interrelated: While the security challenge posed by potential systemic failure is inherent to the nature of the technological development in ICT, the dangers caused by and through malicious agents are conditioned by the nature of ICT. It is in fact the interaction between the two threat levels that makes the issue of cybersecurity such a complex challenge since it "is not simply that increasing dependence on ICT creates vulnerabilities and opportunities to be exploited by the unscrupulous, but also that ICT has an increasingly important enabling function for serious and organized crime, ideological and political extremism, and possibly even state-sponsored aggression."[14]

Even though most experts would agree on this interrelation, there is an exclusive focus on the actor dimension of the threat spectrum in all of the cybersecurity strategies that were studied. This is not overly

10 Cornish, Paul, Rex Hughes, and David Livingstone (2009). Cyberspace and the National Security of the United Kingdom. Threats and Responses. Chatham House: A Chatham House Report.

11 UK Cyber Security Strategy, 2009: p. 9.

12 US Cyberspace Policy Review, 2009: p. 2.

13 Ibid.

14 Ibid.: p. vii.

surprising, as cybersecurity is considered to be one of the key national security challenges of today; and in the context of national security, the possibility of a human attack is of special interest. Even though the immediate response to a cyberspace incident has to be tailored to the actual event on the technical level, mid- or long-term strategies work on a different level, and the identity of the attacker is crucial for calibrating the right response: If the attack was perpetrated by a state actor, military responses can be activated; when the threat originates from sub-state actors, the primary response should consist of law-enforcement measures. The question of who or what is threatening thus remains an important aspect of cybersecurity.

2.2 Malevolent actors: Who threatens cybersecurity?

When we examine the countries' outlooks on who they consider to be the gravest threat in the domain of cyberspace, there is considerable diversity:

- The **UK** Cyberspace Policy Review views the "*established capable states*" as the potentially most sophisticated threat, even though it is recognized that "[t]hose who seek to use cyber space for malicious purposes include *criminals*, *terrorists*, and *states*, whether for reasons of espionage, influence or even warfare."[15]
- **The Estonian** cyber security strategy notes that "*terrorist organizations, organized criminals and state-sponsored actors* already pose a serious global threat."[16]
- The **US** Cyberspace Policy Review emphasizes "*the role of nations in exploiting information networks*".[17]
- The **Swedish** Emergency Management Agency (SEMA) considers the likelihood of a terrorist attack on Swedish critical information infrastructure to be relatively low, and instead emphasizes the danger of IT crime, which "*constitutes one of the largest threats to government agencie*s' electronic services being further developed and used by more people".[18]
- The **Belgian** policy report on information security also notes that "[a]s more and more applications go online, the greater the financial incentives for *online criminal behavior*."[19]

This diversity shows that there are different perceptions and assessments of the threats to cyberspace. However, it has to be noted that the strategies and policy papers lack clear definitions and remain vague when it comes to the description and evaluation of the different threats. The terms "criminal activity" and "terrorist act" are not clearly defined. This vagueness can hardly be avoided, as it is a distinctive characteristic of cyberspace that it interlinks different actors and thus blurs the boundaries between different fields of activities. The Estonian cyberstrategy even explicitly acknowledges that "[t]here are no general regulations for the prevention and combating [sic] cyber threats, nor even a set of common definitions of these threats."[20]

Nevertheless, the strategies do differentiate between different threats. The most explicit delineation is

15 UK Cyber Security Strategy, 2009: pp. 12f.

16 Cyber Security Strategy of Estonia, 2008: p. 10.

17 US Cyberspace Policy Review, 2009: p. 1.

18 Information Security in Sweden: Situational Assessment 2008: p. 17.

19 Towards a Belgian Strategy on Information Security, Version 2, 2008: p. 4.

20 Cyber Security Strategy of Estonia, 2008: p. 17.

made between states and non-state actors. The threats that are posed by states range from spreading disinformation to intelligence-gathering and large-scale attacks on critical infrastructures. In some documents, such activities are subsumed under the label "cyberwarfare".[21] Non-state actors, on the other hand, are described either as "cybercriminals" or as "cyberterrorists", depending on their motivation or their targets.

Despite this categorization of malicious actors into state and non-state actors, it remains unclear who poses the biggest threat, since there is not enough information on the capabilities and motivations of potential perpetrators. The difficulty of assessing the level and origin of threats to cybersecurity is acknowledged in most of the strategy and policy papers, and they avoid ranking the threats according to likelihood or severity.

2.3 Referent object: What is threatened?

When it comes to the referent object (=that which is threatened and in need of protection), there are two major issues: economic well-being and national security. The strategies and policy papers emphasize the importance of ICTs for the national economy and point to the high costs of cyberattacks for the corporate sector.[22] These costs are deemed to have a negative impact on the growth of national economy.[23] The second referent object that is prominently discussed in the documents is national security. With reference to the large-scale attacks on Estonia in 2007, it is stressed that cyberattacks can compromise the functioning of critical infrastructures, which are considered to be crucial to national security.[24]

However, rather than being two clearly separable dimensions, economic well-being and national security are closely interconnected, since critical information infrastructures are essential for both dimensions at the same time. This interconnectedness is reflected in most of the documents. The United States, for example, claims that: "The continued exploitation of information networks and the compromise of sensitive data, especially by nations, leave the United States vulnerable to the loss of economic competitiveness and the loss of the military's technological advantages."[25] The Swedish Assessment of Information Security also mentions both dimensions: "Deficient information security can threaten [...] the capability to deal with serious disturbances and crises. Furthermore, it can have a negative impact on combating crime, trade and industry's profitability and growth, as well as the personal integrity of the country's citizens".[26]

The nexus between economic and national security interests is even more accentuated by the fact that many of the cyberstrategies view cybersecurity as being directly related to other governmental strategies, especially the respective countries' national security strategies.[27] However, some of the strategies and

21 UK Cyber Security Strategy, 2009: p. 12; Cyber Security Strategy of Estonia, 2008, p. 10; Information Security in Sweden: Situational Assessment 2008: p. 18.

22 UK Cyber Security Strategy, 2009: pp. 12f.

23 Information Security in Sweden: Situational Assessment 2008: p. 3.

24 EU Commission, 2009: pp. 4ff.; US Cyberspace Policy Review, 2009: p. 2; Cyber Security Strategy of Estonia, 2008: p. 10; NATO and Cyber Defence, 2009 Committee Report, §1.

25 US Cyberspace Policy Review, 2009: p. 1.

26 Information Security in Sweden: Situational Assessment 2008: p. 3.

27 The UK realizes that: "Cyber security cuts across almost all the challenges outlined in the National Security Strategy, and interlinks with a wide range of Government policies, involving many departments and agencies" (UK Cyber Security Strategy 2009: p. 14). The US encourages the development of a new security strategy, noting that: "The national strategy should focus senior leadership attention and time toward resolving

policy papers also explicitly highlight the connection to information society and economic strategies. The Estonian Cyber Security Strategy, for example, states: "In developing the Cyber Security Strategy, the committee has taken into account national development plans that might also be relevant to information security and the information society, as well as plans relating to internal security and national defense."[28]

2.4 Conclusion: Threat Perceptions

The broad definition of cybersecurity as the absence of a threat either via or to ICT and networks allows for a wide range of interpretations. There are different perceptions concerning the questions of who is threatening and what is threatened.

Figure 1 summarizes four categories of threats that are referenced in the documents, arranged by the differences between those two questions. In theory, what one perceives as threatening and what one perceives as being threatened generates the focus of what is perceived to be in need of protection.[29] A clear prioritization of the threats would therefore lead to a prioritization of response strategies. However, as mentioned above, in the case of cybersecurity, it is neither possible to define which actor poses the biggest threat, nor can the two dimensions of economy and national security be viewed in isolation. In consequence, the link between threat perceptions and countermeasures is far less clear in the field of cybersecurity. In fact, even though the strategies do differ in their assessments of key threats (see chapter 2.2), they arrive at very similar countermeasures, as is shown in the next chapter.

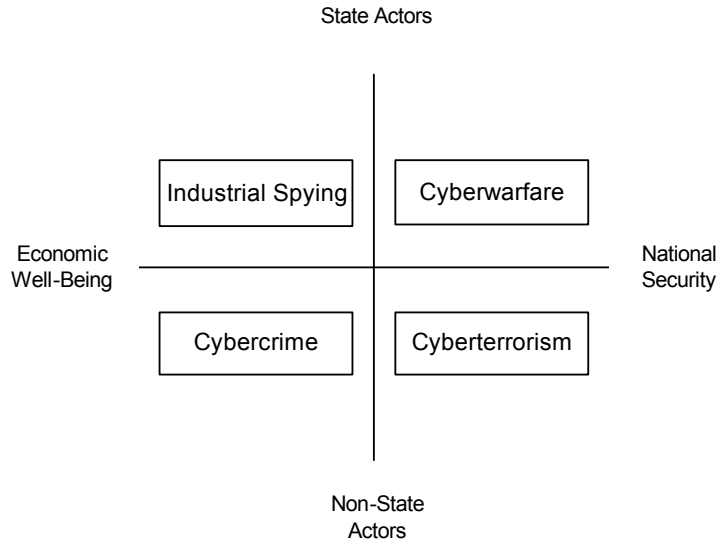

Figure 1: Threats to Cybersecurity

issues that hamper US efforts to achieve an assured, reliable, secure, and resilient global information and communications infrastructure and related capabilities" (US Cyberspace Policy Review 2009: p. 8).

28 Cyber Security Strategy of Estonia, 2008: p. 8.

29 See the writings of the so-called Copenhagen School, most prominently Buzan, B., Wæver, O. and de Wilde, J. (1998) Security: A New Framework for Analysis, Boulder, CO: Lynne Rienner; Wæver, O. (1995) 'Securitization and desecuritization', in Lipschutz, R. D. (ed.) On Security, New York: Columbia University Press, pp. 46–86.

3 RESPONDING TO CYBERTHREATS

In the absence of a clear picture of the severity and likelihood of different threats to cybersecurity, most strategy and policy papers define response strategies that reduce vulnerability to all forms of cyberattacks. Despite the differences between various kinds of attacks, there are also similarities that can be used to define general response strategies. For example, cybercriminals and cyberterrorists may exploit the same vulnerabilities to intrude into IT systems. Furthermore, both types of actors benefit from the lack of knowledge of many users and from the fact that they can start their attacks from the location of their choice, which can make it hard to prosecute them.

It is thus possible to mitigate the risk of all kinds of attacks by reducing vulnerabilities and improving national and international coordination and prosecution. Thus, even though strategies and policy papers sometimes differ in their threat description, they all identify similar response strategies.

- They promote an increase of public-private collaboration to enable a better exchange of information.
- They call for more coordination within the public sector in order to foster coherent responses.
- They highlight the importance of public awareness campaigns.
- They point to the need for more international cooperation.

In the following, these four response strategies shall be briefly discussed.

3.1 Public-Private Partnerships/ Information-Sharing

The latest EU Commission Communication on CIIP states that there is a need for "a risk management approach and culture, able to respond to known threats and anticipate unknown future ones, without over-reacting and stifling the emergence of innovative services and applications".[30] Such awareness is present in most of the strategies and policy reviews, which therefore recommend a variety of measures that should be implemented to serve as adequate responses to cyberthreats.

Most strategy papers, attempting to find the right balance that will ensure the protection of both public and private interests, propose some kind of public-private partnership.

- The **United States** suggests the development of public-private information-sharing: "The President's cyber security policy official should work with relevant departments and agencies and the private sector to examine existing public-private partnership and information sharing mechanisms to identify or build upon the most effective models."[31]
- The **United Kingdom** stresses that "[c]lose engagement to strengthen existing cross-cutting private sector partnerships and form new ones where required, will be fundamental to the current and longer term success of this strategy."[32]

According to the **Estonian** strategy, "cooperation between the public and private sectors is vital to reducing vulnerability of the critical infrastructure."

- One of the measures that **NATO** Parliamentary Assembly advises the parliamentarians to take in their home countries is "establishing strong partnerships between governments and private

30 EU Commission, 2009: p. 5.

31 US Cyberspace Policy Review, 2009: p. 18.

32 UK Cyber Security Strategy, 2009: p. 10.

computer firms in order to ensure the security of government networks".[33]

- The **EU** also highlights the fact that "this is a shared responsibility: no single stakeholder has the means to ensure the security and resilience of all ICT infrastructures and to carry all the related responsibilities."[34]

The idea of public-private partnerships (PPPs) is by no means a new development. In fact, the 1997 US Report on Critical Infrastructure Protection clearly states that "coping with increasingly cyber-based threats demands a new approach to the relationship between government and the private sector."[35] Already more than a decade ago, governments realized the crucial role of the private sector in information infrastructure protection, as it is the private companies that own most of the critical infrastructure and can therefore be crucial in sharing information that is required for the effective protection of such infrastructure elements. Considering that PPPs have been continuously promoted for many years, it is clear that so far, this concept has not reached its full efficiency potential. This is reflected in the current cybersecurity strategies and policy reviews – especially in the latest US strategy. According to the US Cyberspace Policy Review, "these groups perform valuable work, but the diffusion of effort has left some participants frustrated with unclear delineation of roles and responsibilities, uneven capabilities across various groups, and a proliferation of plans and recommendations."[36]

The crux of public-private partnership is that their implementation is demanding and that there is no single best way how to establish them. The design of partnerships must be in line with their function as well as with the specific characteristics of the public and private partners involved. A partnership approach must therefore be flexible in order to allow various ways of implementation, and it makes no sense to define the structure of partnerships on the level of a strategy paper. On the other hand, it is unsatisfactory to promote better PPPs without describing how the difficulties in their implementation shall be addressed. A potential solution is the definition of frameworks and programs for PPPs. Such frameworks are, for example, proposed by the US Cyberspace Policy Review[37] or by the Communication from the EU Commission on Critical Information Infrastructure Protection.[38]

3.2 Better Coordination and Integration

A second measure that is proposed in almost all strategies is better coordination and a more integrated approach on the domestic front, which would offer clear allocations of responsibilities and thus improve the efficiency of cybersecurity measures.

- The **Estonian** Cyber Security Strategy notes "[i]t is necessary to acknowledge cyber threats much more widely, and to improve interdepartmental

33 NATO and Cyber Defence, 2009 Committee Report, §56.

34 EU Commission, 2009: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience." Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, p. 5.

35 "Critical Foundations: Protecting America's Infrastructures", The Report of the President's Commission on Critical Infrastructure Protection, October 1997: p. x.

36 US Cyberspace Policy Review, 2009: p. 18.

37 US Cyberspace Policy Review, 2009: p. 38.

38 EU Commission, 2009: p. 6.

coordination system related to the prevention and combating of cyber attacks on a national level."[39]

- The **Swedish** Emergency Management Agency realizes that: "the so-called expert agencies have not been given sufficiently clear mandates, which hinders work to communicate a cohesive picture from the agencies." [40]
- The **United States** contends that: "A more integrated approach to policy formulation would ensure mutually reinforcing objectives and allow the United States to leverage its international opportunities with consistent, more effective positions."[41]
- The **United Kingdom** holds that "[g]overnment must lead a coherent UK response to the security challenges that arise from these threats and risks and a strategic approach is fundamental to achieving this aim."[42]
- The **EU** also realizes that "[a] more structured exchange of information and good practices across the EU could considerably facilitate fighting cross-border threats."[43]
- **Japan** also clearly states that "[i]n order to grasp the cross-sectoral situation to improve critical infrastructure protection throughout the nation, the government will make efforts to understand what kind of potential threats each critical infrastructure has and what kind of interdependency exists as to what impact will ripple through other critical infrastructures when an IT-malfunction occurs in a critical infrastructure."[44]

In order to implement greater coordination at the practical level, many strategies suggest the development of new structures or offices that would be responsible for overseeing the activities of all of the agencies that deal with cybersecurity-related issues. This trend is particularly observable in the cases of the United States and the United Kingdom, but also on a more organizational level in the case of the NATO Parliamentary Assembly.

- The **United States** Cyberspace policy review suggests that the President appoints a *cybersecurity policy official* at the White House (a so-called "cyber czar"), who would coordinate all of the national cybersecurity related policies and activities. This office would in turn require clarification of "cyber security related roles and responsibilities of federal departments and agencies while providing the policy, legal structures, and necessary coordination to empower them to perform their missions."[45]
- The **United Kingdom** recommends establishing a *Cyber Security Operations Center* involving representatives from across the government and key stakeholders, which will have several tasks including: monitoring cybersecurity developments, trends analysis, technical response coordination to incidents in cyberspace, information dissemination across all sectors, and promotion of better understanding of risks. Hence, this center, headed by the Office of Cyber Security, will "provide policy guidance, expertise and situational awareness to those elements of government that deal directly

39 Cyber Security Strategy of Estonia, 2008, p. 15.

40 Information Security in Sweden: Situational Assessment 2008, p. 20.

41 US Cyberspace Policy Review, 2009: p. 20.

42 UK Cyber Security Strategy, 2009: p. 9.

43 EU Commission, 2009: p. 7.

44 Secure Japan 2008: Intensive Efforts for Enhancing Information Security Infrastructure, Information Security Policy Council; p. 36.

45 US Cyberspace Policy Review, 2009: pp. iii; 7f.

with national security threats, and to the private sector and the public."[46]

- The **NATO** Parliamentary Assembly proposes the creation of Cyber Defense Management Authority, a "NATO-wide authority charged with initiating and coordinating 'immediate and effective cyber defense action where appropriate.'"[47]

By defining new structures, the strategies can be useful for achieving better coordination in cybersecurity. Often, there are too many governmental agencies involved. In consequence, it has often been impossible to attribute responsibilities, which hindered the effective response. At the same time, however, it should be noted that the implementation of new structures is a cumbersome process and reorganization could also destroy mechanisms that have been working quite effectively. While new developments may require institutional reforms, it is also important to ensure a certain degree of stability and continuity. A cybersecurity strategy should therefore try to define an institutional framework for cybersecurity that is not only able to tackle the short-term problems, but is also flexible enough to deal with potential new problems.

3.3 Awareness Campaigns and the Promotion of Education, Training, and Research

All the strategies and policy papers highlight the fact that cybersecurity can only be improved if the whole society becomes more aware of the problem. According to international research, the worldwide security awareness on the part of internet users is very low, with 97% of users unable to distinguish between secure and insecure websites and 80% of surveyed users having installed programs considered dangerous in terms of cybersecurity.[48] Therefore, in order to recognize the public vulnerability to cyberthreats and the importance of public participation in building cybersecurity policies, several strategies and policy reviews have developed the idea of public-awareness campaigns.

- **Estonia** notes that an important precondition for ensuring cybersecurity is "raising the public's awareness of threats in cyberspace and of the necessary remedies".[49]
- The **United States** recommends that "[t]he Federal government, in partnership with educators and industry, should conduct a national cyber security public awareness and education. The strategy should involve public education about the threat and how to enhance digital safety, ethics, and security."[50]
- **Japan** recognizes that "[i]n order to raise public awareness of information security, given the reality of rapidly advancing and complicated threats to information security, the competent agencies will actively provide each individual with appropriate information, and implement promotions and PR activities using media, etc."[51]
- The **United Kingdom** notes that "the government will improve knowledge and awareness".[52]
- **Belgian** experts suggest the establishment of a Belgian Information Security Awareness Forum, which would enable information exchange re-

46 UK Cyber Security Strategy, 2009: p. 16.

47 NATO and Cyber Defence, 2009 Committee Report: §47.

48 Estonia, p. 15 but also: "Adware and Spyware: Unraveling the Financial Web." McAfee White Paper, August 2006.

49 Cyber Security Strategy of Estonia, 2008: p. 15.

50 US Cyberspace Policy Review, 2009: p. 13f.

51 Secure Japan, 2008: p. 49.

52 UK Cyber Security Strategy, 2009: p. 16.

garding information security initiatives, standards and lessons learned in implementation, information security management, IT security techniques, etc., and would serve as a platform for security initiatives for the national government and its bodies.[53]

In addition to the awareness-raising campaigns, the governmental strategies and policy papers also emphasize the need for: enhanced support of cyber-education from elementary schools to colleges and universities; training of a capable and technologically advanced workforce, as well as research in the rapidly evolving field of cyberspace, which should lead to better protection.

- **Estonia** recognizes that "there is a growing need for qualified mid-level information security experts in both the public and the private sectors."[54]
- The **United Kingdom** also stresses the need for the growth of skills and expertise for the government, but also industry, noting that research and development efforts should be "focused, coordinated and exploited to the best effect."[55]
- The **United States** makes it clear that "the Federal government [...] should expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy."[56]
- **Belgian** experts agree that "there is an urgent need to coordinate initiatives related to education, training and research in information security."[57]

Awareness-raising campaigns as well as education, training, and research have been continuously emphasized in strategy and policy papers. The 1997 report on critical infrastructure protection in the United States already includes a clear call for ingraining infrastructure protection "in our culture, beginning with a comprehensive program of education and awareness".[58] Since then, many awareness campaigns have been conducted, often together with private companies that share an interest in informing the public about cybersecurity.[59] While all of the strategies emphasize the importance of awareness and education programs, they rarely specify how or by whom such programs should be implemented. Some refer to previous established and still ongoing programs,[60] while others refer to implementation plans that will be issued later.[61] It also often remains unclear who should be targeted by such campaigns (the strategies and policy papers mention company leaders, students, government officials, or the general public as potential addressees). Although it is not necessary to define every detail of awareness and education programs at the level of a strategy, it would still be beneficial to have better specifications, which would make it possible to analyze which programs are already implemented (and by whom) and which have still to be developed.

3.4 International cooperation

Despite the fact that international cooperation is in many ways already taking place,[62] virtually all of the

53 Towards a Belgian Strategy on Information Security, 2008: p. 6f.

54 Cyber Security Strategy of Estonia, 2008: p. 16.

55 UK Cyber Security Strategy, 2009: p. 19.

56 US Cyberspace Policy Review, 2009: p. 14

57 Towards a Belgian Strategy on Information Security, 2008: p. 7

58 "Critical Foundations: Protecting America's Infrastructures", 1997: p. xi.

59 Examples for such programs are http://www.etsafeonline.org in the United Kingdom or http://www.onguardonline.org in the United States.

60 UK Cyber Security Strategy, 2009: p. 18.

61 Cyber Security Strategy of Estonia, 2008: p. 34.

62 There are several international initiatives regarding cyber space. The Council of Europe Convention on Cyber Crime was

examined strategies and policy papers underscore the need for expanded and more efficient cooperation, realizing that cyberthreats and the perpetrators of cybercrimes do not recognize national boundaries.

- The **United Kingdom** considers it necessary "to work coherently across all sectors in the United Kingdom, as well as with international partners, to ensure that the benefits of cyber space can be delivered in a rules-based, global environment."[63]
- **Estonia** concludes that "[i]t is important to raise global awareness of cyber security and to support international cooperative, preventive and protective measures."[64]
- The **United States** feels a need "to develop a strategy designed to shape the international environment and bring like-minded nations together on a host of issues, including acceptable norms regarding territorial jurisdiction, sovereign responsibility, and use of force".[65]
- **Japan** holds "[a]s threats to information security are becoming more ubiquitous, frequent and diverse, the competent agencies will more actively facilitate cooperation within multinational frameworks".[66]
- The **NATO** Parliamentary Assembly emphasizes that the "measures to address the threat to states from cyber attack have to be global and all inclusive, drawing on government capabilities, companies and society at large."[67]
- The **EU** considers mutual aid to be "an essential element of a proper response to large-scale threats and attacks to CIIs".[68]

The initiatives for enhanced international cooperation should be applauded, especially bearing in mind that cyberthreats are not territorially based. It should be noted however, that one of the reasons for the lack of efficient cooperation is the difference in perceptions of terms such as 'cyberterrorism,' 'cyberattack', 'cyberwarfare', etc. This contributes to the status quo, which is characterized by a lack of coherent international approach. There are also different perceptions of cooperation from different international actors. While some countries would like to treat information system attacks merely as criminal offences against public and private property, as suggested in the Council of Europe's Convention on Cybercrime, other actors would like to see the response to such offences to be escalated to the level of a national security issue. Other differences include the distinction between small- and large-scale attacks as well as ordinary computer systems and critical infrastructure systems.[69] Therefore, while the demands for more international cooperation constitute a positive phenomenon, international cooperation will continue to be insufficient unless there is a real will for unity concerning these essential terms and basic regulations.

opened for signature in 2001 and entered into force in 2004. The Forum of Incident Response and Security Teams (FIRST) brings together a variety of Computer Security Incident Response Teams (CSIRTs) from national governments as well as commercial and education organizations; the European Network and Information Security Agency (ENISA) promotes cooperation on the level of EU members and institutions; the International Telecommunication Union is a UN agency for information and communication technology issues; and the Meridian Process is a platform providing governments worldwide with a means of discussing and working together on policies regarding critical information infrastructure protection.

63 US Cyberspace Policy Review, 2009: p. 14.

64 Cyber Security Strategy of Estonia, 2008: p. 22.

65 US Cyberspace Policy Review, 2009: p. 20.

66 Secure Japan, 2008: p. 62

67 NATO and Cyber Defence, 2009 Committee Report: §55.

68 EU Commission, 2009: p. 6.

69 NATO and Cyber Defence, 2009 Committee Report: §38.

4 CONCLUSIONS AND IMPLICATIONS FOR SWITZERLAND

4.1 General Conclusions

The analysis of recently released strategies and policy papers related to cybersecurity revealed that all of these documents contain thoughts that are already well established, rather than any new ideas. In addition, these documents are quite alike with regard to their description of the threats as well as with regard to the protection measures they propose. First, the documents are all rather vague in describing the threats, since they aim to avoid excluding certain types of threats. They all take into account the fact that cybersecurity concerns both national security and the national economy. Second, they unanimously identify public-private partnerships, improved policy coordination, awareness campaigns, and international coordination as the most important measures for enhancing cybersecurity, but most of them fail to outline how such programs shall be implemented.

The similarities between the different strategy and policy papers show that most governments face similar problems in formulating and implementing cybersecurity policies. The underlying problem is that it remains unclear what is threatened, who is threatening, and what the potential consequences of cyberattacks could be. A cybersecurity strategy has to take into account very diverse types of threats, ranging from criminally motivated phishing activities to terrorist attacks on critical infrastructures. The likelihood of occurrence for these threats varies greatly, as does their potential impact on the security of society. Does it then make sense to include all these threats in one cybersecurity strategy, or should there rather be separate strategies for cybercrime, cyberwar, and cyberterror? The problem is that the different threats are interlinked and the connections between them are not as clear. Cybercriminals may offer their services to terrorists or states, and they all exploit the same vulnerabilities. Treating different threats separately would be inconsistent with the so-called "all-hazards approach", which has proven to be a useful concept to strengthen cybersecurity. It is thus not possible to separate the different kind of threats completely from each other, and cybersecurity strategies should take all of them into account. Nevertheless, it would be preferable to have better definitions than those found in most of the strategies and policy papers.

There is no international agreement on these definitions. However, certain trends can be distinguished. A pragmatic and useful way to differentiate between the different types of threats is to focus on the *intention* and the *effect* of the activities. This way, a cyberthreat escalation ladder can be constructed: from rung to rung, the potential effects are increasingly serious.[70] The escalation ladder presented here is just one possible version: additional rungs (like cyber-extortion, etc.) could be added in between.

- *Rung 1: activism:* activism is the normal, non-disruptive use of the internet in support of a (political) agenda or cause.
- *Rung 2: hacktivism:* Hacktivism is the marriage of hacking and activism, including operations that use hacking techniques against a target's internet site with the intention of disrupting normal operations.
- *Rung 3: cybercrime:* includes theft of intellectual property, extortion based on the threat of Dis-

70 These definitions are based on Dorothy Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', in John Arquilla and David F. Ronfeldt (eds), Networks and Netwars: The Future of Terror, Crime, and Militancy (Santa Monica, 2001), pp. 239–88, Bruce Schneier, 'Schneier on Security: A Blog Covering Security and Security Technology', <http://www.schneier.com/blog/archives/2007/06/cyberwar.html>, accessed 2 June 2008, and Myriam Dunn Cavelty, 'Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', Journal of Information Technology and Politics, 4/1 (2007): 19–36.

tributed Denial of Service attacks (DDoS) attacks, fraud based on identity theft, etc. The intention of the attacker is economically driven.

- *Rung 4: cyberterrorism:* consists of unlawful attacks against computers, networks, and the information stored therein, to intimidate or coerce a government or its people in furtherance of political or social objectives. Such an attack should result in violence against persons or property, or at least cause enough harm to generate the requisite fear level to be considered cyber-terrorism.
- *Rung 5: cyberwar:* the use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems.

Such definitions – though not set in stone – will make it easier to put the different countermeasures into context. The design of PPPs, for example, will vary depending on the function of the partnership. While PPPs for critical infrastructure protection are small and based on direct exchanges of information between the government and individual CI owners and operators, PPPs for the fight against cybercrime require broader coalitions, as criminals may attack all kinds of companies (not only those operating critical infrastructures). As mentioned above, clearer definitions are also required in order to develop a coherent international approach for cybersecurity, as the different perceptions of threats still hinder collaborative efforts. Finally, a clear delineation of cyberthreats is required to define the responsibilities of different government agencies, which would be the first step towards better coordination of cybersecurity efforts. The inter-mixing of cybercrime with cyberwarfare and cyberterrorism, for example, often impedes a clear division of responsibility between military and civil agencies.

In sum, it can be noted that the vague definitions of threats in the strategy papers lead to rather vague concepts for countermeasures. Most strategies fail to set priorities and to provide well-defined cybersecurity programs. This clearly impairs their value and may even jeopardize the benefits of having a cybersecurity strategy. However, one should not jump to the conclusion that cybersecurity strategies are completely unnecessary. Developing a cybersecurity strategy can be valuable for two reasons: First, the process of developing a strategy is valuable in its own right. The discussions about the existing cybersecurity policy that accompany the formulation of a strategy can be fruitful and may stimulate processes that lead to important advancements. Second, a strategy can help to raise awareness of the issue of cybersecurity in general, but can also underline the importance of individual countermeasures. The mention of PPPs as important instrument for more cybersecurity, for example, supports the existing public-private collaborations and can help to establish new PPPs.

Cybersecurity strategies will certainly not directly resolve the problem of insecurity in cyberspace, and they often even fail to provide clear definitions and well-defined policies. Nevertheless, they can be valuable because of their indirect effects; and if they are well designed, they can be useful tools for the further development of policies in cybersecurity.

4.2 Implications for Switzerland

The findings of this report are also of interest for the Swiss context, since in 2008 the Swiss parliament accepted a motion by *Ständerat* Didier Burkhalter (member of the Council of States) requesting the federal government, in collaboration with the cantons and the private sector, to develop a strategy to fight cybercrime.[71] The following section will therefore briefly discuss what can be learned from the analysis of existing strategies for such an undertaking.

A first lesson that can be drawn from the analysis of cybersecurity strategies is that such a strategy should not exclusively focus on one threat, but should address all relevant cyberthreats. This point is important, as the parliamentary motion requests a strategy for cybercrime (*Internetkriminalität*), but also mentions the threats of spying and of terrorist attacks. The analysis of existing strategies has shown that it is hard to separate cybercrime from other cyberthreats. It is thus more sensible to apply the broader concept of cybersecurity in a strategy, as this concept encompasses all types of threats.

A second lesson is the need for clear definitions. By applying a broad approach to cybersecurity, strategies risk becoming vague. This makes it all the more important for strategies to provide clear definitions. The better the threats and also the responses are defined, the easier it is to allocate resources and responsibilities appropriately. In Switzerland, many concepts in the field of cybersecurity have already been defined in previous policy papers. In order to ensure continuity in the cybersecurity efforts, the Swiss strategy should build on these existing policies, which are described in the policy paper "Vulnerable Information Society – Challenge Information Assurance"[72] for the field of information assurance, and in the "Basic Strategy for Critical Infrastructure Protection"[73] for CIP.

This leads to the third lesson, which is the importance of coordination. Cybersecurity concerns many different agencies, and it is crucial to ensure that they all pull in the same direction. The strategy should therefore be developed in close collaboration with those agencies that are already active in the field of cybersecurity. In Switzerland these would include the Reporting and Analysis Centre for Information Assurance (MELANI); the Cybercrime Coordination Unit (CYCO); the Special Task Force on Information Assurance (SONIA); the ICT Infrastructure Unit of the Federal Office for National Economic Supply; the Federal Office for Civil Protection (FOPC); the GovCERT, Awareness Campaigns; PPPs such as Infosurance and CLUSIS, etc.; as well as all relevant stakeholders from the private sector. Many of the involved actors already cooperate in the CIP Working Group, lead by the FOCP, and it will be possible to profit from the experiences made in this process, but the elaboration of a cybersecurity strategy in collaboration with all relevant stakeholders will still be demanding and time-consuming. Nevertheless, such an effort is worthwhile, as it ensures consistency and coherence and is a precondition for successful implementation of the strategy.

71 Motion Burkhalter; http://www.parlament.ch/ab/frameset/d/s/4804/270041/d_s_4804_270041_270171.htm.

72 Swiss Federal Strategy Unit for Information Technology, 2002: "Vulnerable Information Society – Challenge Information Assurance". Available at: http://www.isb.admin.ch/dokumentation/publikationen/00162/index.html.

73 Federal Office for Civil Protection, 2009: "Basic Strategy for Critical Infrastructure Protection". Available at: http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/aktuell.parsys.56405.downloadList.76495.DownloadFile.tmp/skigrundstrategiede20090518.pdf.

5 ANNOTATED BIBLIOGRAPHY

This annotated bibliography contains a) government reports and other policy documents from the scan described on page 2; b) recently released academic contributions on the topics of CIP and CIIP.

5.1 Policy documents/reports

US Government. 2009. Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communication Infrastructure. Available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

The cyberspace policy review was directed by US President Barack Obama to evaluate existing US policies and structures for cybersecurity. The review was carried out by a team of government cybersecurity experts, who received a great deal of input from all relevant stakeholders. As a major result of the review, the report highlights the need for increased leadership on the federal level. It is argued that the federal government cannot entirely delegate or abrogate its role in securing the nation from cyberattacks, and must therefore lead the way forward. In doing so, the government should work together closely with experts from the private sector. Furthermore, the federal government should collaborate with like-minded nations to push cybersecurity on the international level. The reviewers propose an action plan for the government that includes the appointment of a cybersecurity political official (the so-called "cyber czar").

Chatham House. 2009. Cyberspace and the National Security of the United Kingdom. Threats and Responses. Available at: http://www.chathamhouse.org.uk/files/13679_r0309cyberspace.pdf

The report aims to inform the debate on cybersecurity and to make the case for a more coherent, comprehensive, and anticipatory policy response. It starts with a description of different cyberthreats and delineates three major sources of threats: States, ideological and political extremists, and organized crime. The report highlights the importance of keeping responses to these threats proportionate and cost-effective. This means that the risks should neither be ignored nor exaggerated. Collaboration between technology and security experts is required for developing appropriate responses. On the policy level, the report calls for a clear distribution of the responsibilities in cybersecurity between the private, commercial, and governmental domains.

Cabinet Office of the United Kingdom. 2009. Cyber Security Strategy of the United Kingdom. Safety, Security and Resilience in Cyber Space. Available at: http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf

The strategy was issued in June 2009 and outlines the UK government's present and future approach to cybersecurity. It stresses the need for a coherent approach in which the government, organizations across all sectors, the public, and international partners all have a part to play. On the administrative level, the strategy proposes the establishment of an Office of Cyber Security to provide strategic leadership ensuring coherence across government and a Cyber Security Operations Center to monitor the UK networks and users and provide advice to the public and businesses.

German Federal Ministry of the Interior. 2009. National Strategy for Critical Infrastructure Protection (CIP Strategy). Available at: http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34403/kritis_englisch.pdf;jsessionid=A41B91D73D1C8017C7D7435D0510D4DC

The new CIP strategy summarizes the German federal government's aims and objectives and its political-strategic approach. The strategy also reviews the results achieved so far and is the starting point for the further development of CIP policy in Germany.

Commission of the European Communities. 2009. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. Available at: http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf

This report focuses on prevention, preparedness, and awareness and defines a plan of immediate actions to strengthen the security and resilience of CIIs.

The proposed action plan includes the definition of minimal standards for national CERTs; the establishment of a European Public-Private Partnership for Resilience (EP3R); a European forum for information-sharing between member states; a fostering of the European Information Sharing and Alert System; and support for pan-European exercises on large-scale network security incidents.

International Telecommunication Union. 2009. ITU National Cybersecurity/CIIP Self-Assessment Tool. Available at: *http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf*

The ITU National Cybersecurity/CIIP Self-Assessment Tool is a practical initiative by the International Telecommunication Union to assist national government officials in examining their cybersecurity/CIIP policies, procedures, norms, institutions, and relationships. It provides guidelines on how to develop a consistent national cybersecurity policy by identifying risks, key stakeholders, and existing programs. The Self-Assessment-Tool is a work in progress and will be updated on a regular basis.

Ministry of Defence of Estonia. 2008. Cyber Security Strategy. Available at: *http://mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf*

Published in 2008, the Estonian Cyber Security Strategy discusses the status quo in Estonia defines policies for enhancing cybersecurity. These include the development and implementation of a system of security measures, increasing competence in cybersecurity, improving the legal framework for cybersecurity, bolstering international cooperation, and raising awareness on cybersecurity.

NATO Parliamentary Assembly. 2009. Committee Report 027 DSCFC 09 E - NATO and Cyber Defence. Available at: *http://www.nato-pa.int/default.Asp?SHORTCUT=1782*

This committee report discusses cyberthreats and highlights the example of Estonia. It describes various national policies and outlines the potential role of NATO. In particular, it highlights the potential role of NATO's Cooperative Cyber Defence Centre of Excellence (CCD CoE), which will be established in Estonia. This center will provide cyberspace-related doctrines and concepts; host and conduct workshops and exercises; conduct research and development activities; study past or ongoing attacks; and provide advice during ongoing attacks.

Swedish Emergency Management Agency. 2008. Information Security in Sweden – Situational Assessment 2008. Available at: *http://www.krisberedskapsmyndigheten.se/upload/17461/lagesbedomning_infosakerhet_%202008_eng.pdf*

The annual report on information security in Sweden describes current threats and vulnerabilities, recent incidents in Sweden, and new trends in cybersecurity. The report highlights the threat of cybercrime and notes that in 2008 more numerous, small and targeted attacks were discovered. Very large networks of hijacked computers are being created that can be leased commercially to conduct attacks.

Allard, J.L. et al. 2008. Towards a Belgian Strategy on Information Security. Available at: *http://www.lsec.be/upload_directories/documents/TowardsaBelgianStrategyonInformationSecurity_BISI_080908.pdf*

This whitepaper is published jointly by several academic and private associations with expertise in information security. These organizations propose several measures to improve Belgian information security: establishing an information security awareness forum; creating information security standards; promoting research and education; establishing a Belgian CERT and a governmental information security body; and re-evaluating existing laws and regulations.

Information Security Policy Council. 2008. Secure Japan 2008 – Intensive Efforts for Enhancing Information Security Infrastructure. Available at: *http://www.nisc.go.jp/eng/pdf/sj2008_eng.pdf*

The annual report of the information security policy council reviews the efforts undertaken by the Japanese government to improve information security

and describes the next steps in this field. The report provides a very detailed list of actions to be implemented in the next two years, ranging from the promotion of PPPs for the protection of critical information infrastructures to the establishment of educational and awareness programs.

5.2 Academic literature

Hare, F.B. 2009. Private Sector Contributions to National Cyber Security: A Preliminary Analysis. Journal of Homeland Security and Emergency Management, 6 (1): Article 7.

The article examines the factors motivating private-sector actors to contribute to a national cybersecurity regime. It is a case study about two companies that participated in Cyber Storm II, a series of exercises hosted by the DHS that brings together experts from the private and public sectors. The paper shows that the companies were motivated to participate in the exercise by civic-mindedness on the one hand (they feel it is an important contribution they can make to homeland security) and by self-interest (they hope to improve their individual cybersecurity).

Papa, M. and S. Shenoi (eds.). 2009. International Federation for Information Processing, vol. 290; Critical Infrastructure Protection II. Available at: *http://www.springerlink.com/content/xukx44033853/?p=b292b7d4861f49f48434bb806e786a4e&pi=9*

This volume, edited by the International Federation for Information Processing, contains 20 papers on various aspects of CIP that were presented at the International Conference on Critical Infrastructure Protection held at George Mason University in March 2008. The chapters are organized into six sections: themes and issues, infrastructure security, control systems security, security strategies, infrastructure interdependencies, and infrastructure modeling and simulation.

Willis, H.H., G. Lester, and G.F. Treverton. 2009. Information Sharing for Infrastructure Risk Management; Barriers and Solutions. Intelligence and National Security 24 (3): pp. 339-365.

The article discusses the importance, but also the difficulties of public-private information-sharing for the protection of critical infrastructures. Based on interviews with representatives of the private sector, the authors first describe which information the private sector wants, then highlight the barriers to effective information-sharing, and conclude with recommendations ON how to improve information exchange. They propose a re-conceptualization of information-sharing: public and private actors need not to share information, but should jointly produce useful information on threats to critical infrastructures.

Geers, K. 2009. The Cyber Threat to National Critical Infrastructures: Beyond Theory. Information Security Journal: A Global Perspective 18 (1): 1-7.

The author, a member of the Cooperative Cyber Defence Centre of Excellence of Estonia, discusses the threat of cyberattacks on national critical infrastructures. He describes the attacks on Israel and Estonia to highlight how such attacks work and how they can be fought. He concludes by emphasizing the importance of crisis management and international cooperation.

McCarthy, J.A.; M. Dion; O. Pachecho; and C. Burrow. 2009. Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts. In: F. D. Kramer, S. H. Starr, and L.K. Wentz (eds.), Cyberpower and National Security, pp. 543-556.

This book chapter discusses the importance of the information infrastructure for critical infrastructure protection. It stresses that an accident or an attack on the critical information systems could have devastating effects and assesses the US policies to prevent such incidents. The authors recommend a stronger leadership on the part of the federal government in cybersecurity.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** specializes in research, teaching, and information services in the fields of international relations and security policy. The CSS also acts as a consultant to various political bodies and the general public. The Center is engaged in research projects with a number of Swiss and international partners, focusing on new risks, European and transatlantic security, strategy and doctrine, state failure and state building, and Swiss foreign and security policy.

The **Crisis and Risk Network (CRN)** is an Internet and workshop initiative for international dialog on national-level security risks and vulnerabilities, critical infrastructure protection (CIP) and emergency preparedness.

As a complementary service to the International Relations and Security Network (ISN), the CRN is coordinated and developed by the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland. (www.crn.ethz.ch)