

Chapter 2

Global Cyber-Security Policy Evolution

Abstract The aim of this chapter is to show how cyber-security has evolved as a policy issue globally and how the Swiss cyber-security approach has been influenced by this evolution. To this end, this chapter introduces factors that shape cyber-security policy development more generally and then introduces four different ways of “framing” the cyber-security issue: a technical, a crime-espionage, a civil defense, and a military variation. All four are interrelated and exist side by side in every country, but they can be distinguished by a main set of actors with that particular view, by the main referent object these actors/communities tend to focus on and on the particular threats/risks they would be mainly concerned with. This chapter gives examples of specific Swiss institutions and developments that belong to each of the four variations.

Keywords Cyber-security • Policy • Malware • Critical infrastructure protection • Cyber-crime • Cyber-espionage • Cyber-war • United States • Switzerland

2.1 Introduction

The aim of this chapter is to show how cyber-security has evolved globally as a policy issue. Discussions about cyber-security always were and still are influenced by the ongoing “information revolution,” which is substantially shaped by the USA, in the technical sphere, in the business sector, but also politically. At all times, US policy-makers have not only discussed its implications for international relations and security but also act on these assumptions, trying to shape the environment to their maximal benefit. Therefore, it can be said that the specific characteristics of this policy issue originated in the USA in the 1970s, built momentum in the late 1980s, and spread to other countries in the late 1990s. With this spread, a specific in/security logic was diffused, which was fashioned in US military colleges, think tanks, and US government circles. Quite tellingly, in most neo-liberally inclined and democratic states, variations in threat perceptions and proposed policy

solutions are variations of details, not actual substance (cf. Brunner and Suter 2008).

If we want to contextualize and better understand these variations rather than the commonalities, it is useful to take into account that any national cyber-security policy and related practices evolve in an environment shaped by

- directly or indirectly cyber-related policy formulation and actions of other states,
- a political process that involves extensive mobilization of resources from different bureaucratic units that actively shape threat perceptions and countermeasures and often engage in so-called “turf battles”,
- by business actors inside and outside of one’s territory as well as other non-state actors who use cyber-means for various deeds, including criminal behavior, and
- by “focusing events” (Kingdon 2003: 90–115), often, though not exclusively, in the form of malware.

The Brief will return to these influences after each description of the Swiss-specific developments (Chaps. 3–5) to show how they have shaped the Swiss approach. Furthermore, the type of turf battles that usually occur can be further specified by looking at four broad typologies or variations of the cyber-security debate, pushed by different communities: a technological, a crime-espionage focused one, one that is more about critical information infrastructures and their protection, and finally one that is more strategic military in character. After the persuasive insecurity of the information infrastructure is described first, all four variations will be treated in individual subsections below. In each of the four variations, a few examples of Swiss institutions and approaches fitting that particular typology will be given. All of these examples will be further contextualized in Chaps. 3–5.

2.2 The Undercurrent: Technological Insecurity

Overall, the debate about the information revolution and its political consequences was influenced by the larger strategic context after the Cold War, in which the notion of asymmetric vulnerabilities rose to key prominence. Fears about the vulnerabilities of a “sprawling, open country knitted together by transportation, power and communications systems designed for efficiency not security” (Brown 2006: 51) met fears about disembodied adversaries able to take advantage of these vulnerabilities through the anonymity provided by information networks.

Importantly, the cyber-security discourse was never been static, because the technical aspects of the information infrastructure are constantly evolving and keep influencing various aspects of the debate. As is well known, today’s version of cyberspace¹ emerged out of the Advanced Research Projects Agency Network

¹ In popular usage, the terms cyberspace and Internet are often used almost interchangeably, even though the Internet is just one part of cyberspace.

(ARPANET), which was funded by the Defense Advanced Research Projects Agency (DARPA) of the United States Department of Defense (DoD) from 1962 onward, mainly for optimized information exchange between the universities and research laboratories involved in DoD research. From the very beginning, the network designers emphasized robustness and survivability over security, since there was no apparent need for a specific focus on security at that time, when information systems were being hosted on large proprietary machines that were connected to very few other computers (Leiner et al. 1997).

The use of the same basic packet switching technology turned into a legacy problem when there was a tremendous increase in users, in connectivity, and in complexity (Libicki 2000). In addition to this, there are significant market-driven obstacles to IT security, which came into play when the commercialization of the Internet sets in: There is no direct return on investment, time-to-market impedes extensive security measures, and security mechanisms often have a negative impact on usability so that security is often sacrificed for functionality (Anderson and Moore 2006).

There are additional forces keeping cyberspace insecure: Big Data is considered the key IT trend of the future, and companies want to use the masses of data that we produce every day to tailor their marketing strategies through personalized advertising and prediction of future consumer behavior (Morozov 2013). Therefore, there is little interest in encrypted (secure) information exchange. On top of this, the intelligence agencies of this world have the same interest in data that can be easily grabbed and analyzed (Böhme 2005). The NSA revelations of 2013 have further exposed that the intelligence services of this world are making cyberspace more insecure *directly*, in order to be able to have more access to data and in order to prepare for future conflict. The NSA has bought and exploited so-called zero-day vulnerabilities in current operating systems and hardware to inject NSA malware into numerous strategically opportune points of the Internet infrastructure (Greenwald and MacAskill 2013). It also has been revealed that the US government spends large sums of money to crack existing encryption standards—and apparently has also actively exploited and contributed to vulnerabilities in widespread encryption systems (Clarke et al. 2013).

Apart from bringing with it pervasive (and some would say “un-fixable”) insecurity, which is sure to make cyber-in-security an issue that will not go away, changes in the technical substructure also changed what was seen “in need of protection” in the policy debate (the so-called *referent object of security*): In the 1970s and 1980s, cyber-security (not yet under that name) was mainly about those parts of the private sector that were becoming digitalized and also about government networks and the classified information residing in it. The growth and spreading of computer networks into more and more aspects of life changed this limited referent object in crucial ways. In the mid-1990s, it became clear that key sectors of modern society, including those vital to national security and to the essential functioning of (post-)industrialized economies, had come to rely on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation. The new referent

object that emerged was the totality of critical (information) infrastructures that provide the way of life that characterizes our societies (Dunn Cavelty 2008a). This is the context in which most cyber-security policies emerged.

2.3 Variations of the Cyber-Security Discourse

When looking at the various voices that have shaped and still shape the debate today, four different ways of “framing” the cyber-security issue become apparent (Dunn Cavelty 2013).² All four are interrelated and exist side by side in every country, but they can be distinguished by a main set of actors with that particular view, by the main referent object these actors/communities tend to focus on, and by the particular threats/risks they would be mainly concerned with (see Table 2.1). Knowing about these variations helps to situate trends in specific national country settings and helps to explain why certain policy solutions are favored over others: Depending on which group of actors “wins” in the policy process, cyber-security policies have different focal points and different institutional actors get more resources.

Table 2.1 Four variations of cyber-security

	I: Technical	II: Crime-espionage	III: Civil defense	IV: Military
Referent objects	Computers	Private sector (business networks)	Critical (informa- tion) infrastructures	Networked armed forces (military networks)
	Computer networks	Classified information (government networks)	Society (par- ticularly its “functioning”)	Nation/state
Actors	Hacking subculture Computer (security) experts Antivirus industry	Business actors Antivirus industry Law enforcement Intelligence community	National security experts Civil defense/ homeland security	National security experts Military
Threat	Malware Network disruptions, system intrusions Hackers (all kinds)	Advanced persistent threats (malware) Cyber-criminals (non-state) Cyber-spies (state)	Disruptions in critical infrastructures Cascading effects Cyber-terrorists (non-state) Cyber-commands (state)	(Catastrophic) attacks on critical infrastructures Cyber-terrorists (non-state) Cyber-spies (state) Cyber-commands (state)

² A fifth could be added: one that focuses on the international, diplomatic dimension. However, this one is not as well developed or as influential as the others in many countries and is often not as clearly security-focused.

Below, each of the four discourses is described in more details. Recent trends are identified, and particular actors and institutions in Switzerland's cyber-security policy are assigned to the four discourses. This serves as a background for the more specific discussion that follows in Chaps. 3–5.

2.3.1 Technical Discourse

The technical discourse is focused on computer and network disruptions caused by different types of malware. Malware functions as “visible” proof of the pervasive insecurity of the information infrastructure. Also, the history of malware is a mirror of technological development: The type of malware, the type of targets, and the attack vectors always change with the technology and the existing technical countermeasures. Just as an example for how important malware was in shaping the discourse, in 1988, the ARPANET had its first major network incident: the “Morris Worm.” The worm used so many system resources that the attacked computers could no longer function and large parts of the Internet went down. Its technical effect prompted the DARPA to set up a center to coordinate communication among computer experts during IT emergencies and to help prevent future incidents: a Computer Emergency Response Team (CERT) (Scherlis et al. 1990). This center, later called the CERT Coordination Center, still plays a considerable role in computer security today and served as a role model for many similar centers all over the world.

The worm also had a substantial psychological impact, by making decision-makers aware of how insecure and unreliable the Internet was (Parrikka 2005). While it had been acceptable in the 1960s that pioneering computer professionals were hacking and investigating computer systems, the situation had changed by the 1980s: Society had become dependent on computing in general for business practices and other basic functions. Tampering with computers suddenly meant potentially endangering people's careers and property, and some even said their lives (Spafford 1989).

2.3.1.1 Trends and Developments

While there was a tongue-in-cheek quality to many of the viruses in the early days, viruses have long lost their innocence. Pranklike viruses have not disappeared, but nowadays, computer security professionals are much more concerned with the rising level of professionalization coupled with the obvious criminal (or even strategic) intent behind attacks. Advanced malware is targeted: A hacker picks a victim, scopes the defenses, and then designs malware to get around them (Symantec 2010). The most prominent example for this kind of malware is Stuxnet, which will be discussed in the section about the military discourse. However, some IT security companies have recently warned against overemphasizing advanced

persistent threat attacks just because we hear more about them (Verizon 2010: 16). Only about 3 % of all incidents are considered so sophisticated that they were impossible to stop. The vast majority of attackers go after low hanging fruit, which are small-to-medium-sized enterprises with bad defenses (Maillart and Sorrette 2010). These types of incidents tend to remain under the radar of the media and even law enforcement but still cause considerable damage.

2.3.1.2 Technical Cyber-Security in Switzerland

In the 1980s, Switzerland was playing catch-up with regard to the development of its own information society, like most other countries. However, in the mid-1980s, nearly all the Swiss universities had a connection with an international data network and plans for a single academic network in Switzerland with a single technological standard were beginning to emerge. In October 1987, the “**Swiss Tele Communication System for Higher Education**” (SWITCH), a foundation, came into life, and a few months after the “.ch” domain had been entered into the “Domain Name System.” Since then, SWITCH is in charge of building up the Swiss university and research network but also has the responsibility of administering the “.ch” (and later .li) domain.³ A CERT function was added in 1996 when the SWITCH-CERT was created, the national “CERT.” This was mainly a reaction to the increasing amount of malware that also began to affect Swiss information networks and computers.⁴

SWITCH-CERT played a very important role in Switzerland’s official cyber-security efforts at least until 2008 (see Chaps. 3 and 4). Through the 2010 revision of the regulations on addresses in the telecommunication sector, SWITCH got the power to block domain names if the responsible parties do not remove detected malware within 24 h. In Switzerland, the responsibility for a site rests with whoever has registered it rather than the Internet hosting provider. Considering that a third of the 1.7 million Swiss domains are hosted on servers in other countries, this is an important feature of the technical approach to cyber-security.

2.3.2 Crime-Espionage Discourse

The crime-espionage discourse and the technical discourse are very closely related (and not always clearly separable), because cyber-crime and espionage are often conducted via malware. One of the key differences to the technical discourse is that the development of IT law (more specifically, Internet or cyber-law) plays a crucial role for this discourse, because it allows the definition and prosecution of

³ See www.switch.ch/about/profile/switch_history/.

⁴ See <http://www.switch.ch/security/>.

misdemeanor (Scott 2007). Cyber-crime has (overall) come to refer to any crime that involves computers and networks, like release of malware or spam, and fraud. However, a distinct national security dimension was established when computer intrusions (a criminal act) were exposed to serve an espionage purpose. Prominent hacking incidents such as the Cuckoo's Egg incident (Stoll 1989), the "Rome Lab incident," Solar Sunrise, or Moonlight Maze (United States General Accounting Office 1996) made apparent that classified or sensitive information could be acquired relatively easily by foreign nationals through hackers.

2.3.2.1 Trends and Developments

There are three more recent trends worth mentioning: First, tech-savvy individuals (often juveniles) with the goal of mischief or personal enrichment shaped the early history of cyber-crime. Today, professionals dominate the field. The Internet is a near-ideal playground for semi- and organized crime for activities such as theft (like looting online banks, intellectual property, or identities) or for fraud, forgery, extortion, and money laundering. Actors in the "cyber-crime black market" are highly organized regarding strategic and operational vision, logistics, and deployment. Like many real companies, they operate across the globe (Panda Security 2010). Over the years, this discourse has become particularly focused on advanced persistent threats, a cyber-attack category that connotes an attack with a high degree of sophistication and stealthiness over a prolonged duration of time. The attack objectives typically extend beyond immediate financial gain, so that states as instigators of cyber-misdemeanor, currently mainly in the form of cyber-espionage, are the main focus of attention.

Second, the cyber-espionage story itself has changed. There has been an increase in allegations that China is responsible for high-level penetrations of government and business computer systems in Europe, North America, and Asia. Because Chinese authorities have stated repeatedly that they consider cyberspace a strategic domain and that they hope that mastering it will equalize the existing military imbalance between China and the USA more quickly, many officials readily accuse the Chinese government of deliberate and targeted attacks or intelligence gathering operations. In May 2014, the USA even indicted five Chinese military-affiliated hackers for stealing commercial secrets (Ackerman and Kaiman 2014). Overall, the strategic cyber-espionage debate was brought to an entirely different level by Edward Snowden's NSA revelations in 2013, when the world started to look at the USA as one of the prime if not the most important actor in the cyber-espionage category, at least temporarily.

The third trend is the increased attention that hacktivism—the combination of hacking and activism—has gained in recent years (at least before Snowden). WikiLeaks, for example, has added yet another twist to the cyber-espionage discourse. Acting under the hacker-maxim "all information should be free," this type of activism deliberately challenges the self-proclaimed power of states to keep information, which they think could endanger or damage national security, secret.

It emerges as a cyber-security issue in government discourse, because of the way a lot of the data have been stolen (in digital form) but also how it is made available to the whole world through multiple mirrors (Internet sites). Somewhat related are the multifaceted activities of hacker collectives such as Anonymous or LulzSec. Behaving deliberately hedonistic, uninhibited, and some might even say childish, they creatively play with anonymity in a time obsessed with control and surveillance and humiliate high-visibility targets by DDoS attacks, break-ins, and release of sensitive information.

2.3.2.2 Cyber-Crime and Cyber-Espionage in Switzerland

In terms of cyber-law, a number of articles in the Swiss Penal Code are of relevance for cyber-security:

- Article 143, unauthorized obtaining of data;
- Article 143 bis, unauthorized access to a data processing system;
- Article 144 and 144 bis, criminal damage and damage to data;
- Article 147, computer fraud.⁵

Also, Switzerland has signed and ratified the Council of Europe's Convention on Cybercrime in 2012. This agreement obliges the signatory states to make computer-related fraud, data theft, forging of documents by computer, or access to protected IT system offenses under the law. Although the Swiss Penal Code is applicable to a wide range of incidents, only a few cases have been prosecuted so far. Overall, the structure of the Swiss legal system makes prosecution difficult, due to the complexities of different laws (comprising laws on both the federal and cantonal levels) and law enforcement procedures.

Following a certain international trend, Switzerland also established a dedicated office for the fight against cyber-crime in 2003.⁶ The Cybercrime Coordination Unit Switzerland (CYCO), Switzerland's central office for reporting illegal subject matter on the Internet, was established as a cooperating project between the Confederation and most of the Swiss cantons. It has three areas of responsibility: monitoring (the systematic search of criminal content), analysis (of cases), and clearing (of incoming reports). Anybody can report suspicious subject matter on the Internet using their only complaints form.⁷ In 2013, CYCO received 9,208 Suspicious Activity Reports on Cybercrime (CySARs) via the online reporting form, which is an increase of 11.7 % over 2012, most of them regarding child pornography and child abuse (CYCO 2013: 1).

⁵ Swiss Penal Code, http://www.admin.ch/ch/e/rs/311_0/.

⁶ This unit will not be discussed in more detail in the following chapters.

⁷ <http://www.ejpd.admin.ch/content/kobik/en/home/meldeformular.html>.

However, CYCO has changed face over the years. The CYCO clearing and analysis units were merged into one unit as part of a reorganization that took place in 2004. This unit was subsequently incorporated into the Reporting and Analysis Center for Information Assurance (MELANI). MELANI is the strongest player in the Swiss cyber-security field (described in the following chapters). The biggest change happened in 2009, however, when CYCO and MELANI were separated: CYCO was incorporated into Fedpol's Federal Criminal Police Division, and MELANI was incorporated into the newly established Federal Intelligence Service (FIS). As a result, CYCO began to perform more and more operational tasks and police duties, such as coordinating national and international investigations and exchanging police data and far less strategic analytical work (CYCO 2013: 4).

For the Swiss debate, cyber-crime/espionage incidents were quite decisive in shaping the perception that urgent action was needed. For example, in 2007, hackers successfully tricked employees at the Foreign Ministry and at the State Secretariat for Economic Affairs (Seco) with a phishing scheme. It was suspected that the aim behind the sophisticated attack was espionage. In 2009, the computer network of the Swiss Foreign Ministry was the target of a "very professional" attack—computer systems were targeted with the intent of gathering specific information (MELANI 2009) (this attack has come to be known as "EDA Hack"). The same happened again in 2012.⁸ On December 6, 2010, in the wake of the leak of American embassy cables by WikiLeaks, the Swiss financial service PostFinance announced that it had closed an account in the name of WikiLeaks founder Julian Assange because he did not reside in Geneva as he had claimed when opening the account. In response, PostFinance's Web site was hit by denial-of-service attacks as part of Anonymous' Operation Payback. PostFinance's Web site went off-line and was not accessible for more than 10 h (MELANI 2010). In all of these cases, MELANI had to become active.

2.3.3 *Civil Defense Discourse*

Already in the late 1980s, documents started to appear which made a link between cyber-threats and critical infrastructures (cf. Computer Science and Telecommunications Board 1989; National Academy of Sciences 1991). The technological development in information processing and communication technologies and the rapid global dispersion of these technologies—most significantly, the ascent of "the Internet"—were seen to cause an ongoing transformation of all aspects of life through saturation with information and communication technologies. But most importantly, it added a variety of novel aspects to an older debate about vital systems (Collier and Lakoff 2008): first of all, the dependency of modern industrialized societies on a wide variety of national and international information infrastructures, characterized by highly interdependent software-based control systems, is characterized

⁸ All incidents are still under investigation.

as a new development bringing about novel vulnerabilities. Furthermore, the information revolution empowered new malicious actors, including state as well as non-state actors, and enhanced the overall capability of these actors to do harm by inexpensive, even more sophisticated, rapidly proliferating, easy-to-use tools in cyberspace.

As previously mentioned, this debate took place in the broader context of a shifting threat landscape after the end of the Cold War. Global information networks were seen to be making it much easier to attack the USA asymmetrically, as such an attack no longer required big, specialized weapon systems or an army: Borders, already porous in many ways in the real world, were nonexistent in cyberspace. Subsequently, it was established in various reports and publications that the information revolution had made the USA asymmetrically vulnerable, due to the disappearance of borders and the dependence of military forces on vulnerable civilian infrastructures. At a later stage, a number of computer intrusions demonstrated how a small group of hackers could easily and quickly take control of defense networks. Even more significant were exercises such as “The Day After” in 1996, or “Eligible Receiver” in 1997 (Molander et al. 1996; Anderson and Hearn 1996). The exercises were designed to assess the plausibility of information warfare scenarios and to help define key issues to be addressed in this area. As will be shown in Chap. 3, these exercises played a decisive role in Switzerland’s own cyber-security strategy shaping as well.

2.3.3.1 Trends and Developments

In the latter 1990s, critical infrastructures became the main referent object in the cyber-security debate. Whereas critical infrastructure protection (CIP) encompasses more than just cyber-security, cyber-aspects have always been the main driver in this “new” policy issue. Following the Oklahoma City bombing, President Bill Clinton set up the Presidential Commission on Critical Infrastructure Protection (PCCIP) to look into the security of vital systems such as gas, oil, transportation, water, and telecommunications. The PCCIP presented its report in the fall of 1997 (PCCIP 1997). It concluded that the security, economy, way of life, and perhaps even the survival of the industrialized world were dependent on the interrelated trio of electrical energy, communications, and computers. Further, it stressed that advanced societies rely heavily upon critical infrastructures, which are susceptible to classical physical disruptions and new virtual threats. While the study assessed a list of critical infrastructures or “sectors”—for example, the financial sector, energy supply, transportation, and the emergency services—the main focus was on cyber-risks. There were two reasons for this decision: First, these were the least known because they were basically new, and secondly, many of the other infrastructures were seen to depend on data and communication networks. The PCCIP linked the cyber-security discourse firmly to the topic of critical infrastructures. Thereafter, CIP became a key topic in many other countries, including Switzerland.

One of the key challenges for protection efforts arises from the privatization and deregulation of many parts of the public sector since the 1980s and the globalization processes of the 1990s, which have put a large part of the critical

infrastructure in the hands of private enterprise. This creates a situation in which market forces alone are not sufficient to provide security in most of the CI “sectors.” At the same time, the established expert opinion is that the state is incapable of providing the public good of security on its own, since an overly intrusive market intervention is a flawed and undesirable option, because the same infrastructures that the state aims to protect due to national security considerations are also the foundation of the competitiveness and prosperity of a nation. Therefore, any policy for CIP must absorb the negative outcomes of liberalization, privatization, and globalization, without canceling out the positive effects.

Public–private partnerships (PPP), a form of cooperation between the state and the private sector, are widely seen as a panacea for this problem in the policy community, and cooperation programs that follow the PPP idea are part of all existing initiatives in the field of CIP today. A large number of them are geared toward facilitating information exchange. While some of these arrangements are successful, others have scarcely generated more joint statements of intent of the actors involved. In recent years, therefore, increasing criticism has been heard condemning the lack of efficiency in existing arrangements or even questioning the validity of the entire cooperation concept.

2.3.3.2 Cyber-Security and Civil Defense in Switzerland

From the very beginning, Switzerland framed its cyber-security efforts as part of CIP, as will be shown in Chaps. 3–5. In brief, what emerged from this was the Reporting and Analysis Center for Information Assurance (MELANI), organized as dedicated public–private partnership organization, which will be the sole focus of Chap. 4. However, for reasons of (mild) departmental power plays and overall political sensitivities, the more cyber-related (information) infrastructure-focused efforts and the more traditional, physical CIP were treated separately until about 2012, even though a clear distinction is and was almost impossible on a conceptual and operational level. For the more “traditional” CIP issues, the Federal Council mandated the Federal Office of Civil Protection (FOCP) to coordinate efforts in the area of CIP and to establish a CIP Working Group (CIP WG) in which all relevant authorities were represented, in order to ensure cross-sectoral coordination and design a consolidated approach at the national (federal) level. Typically, for Switzerland, the undertaking was built upon existing structures, organizations, and networks in order not to step on anybody’s toes. The FOCP never took a decisive lead, but positioned itself mainly as information-sharing platform, in which to exchange views and experiences. This particular strategy-finding process will be described in Chap. 5.

The topic also made it into the top-level strategic document, the Security Policy Report 2000. In that, the Swiss Federal Council defined CIP as a primary goal of its security policy and defined its objectives as follows:

The Federal Council’s primary objective regarding the security of this infrastructure is to maintain the Switzerland’s ability to decide and to act, and to create the conditions ensuring the functioning of the Swiss ‘information society’ (Federal Council 1999: 54–55).

2.3.4 Military Discourse

Information technology had been firmly coupled with military affairs since at least the Second World War and specifically so in the wake of the more general debate in the Cold War about technological innovation and warfare (Gray 1997). Furthermore, concrete ideas of information warfare date back at least to the 1970s, when it was argued in strategic communities that communications and information support networks were sufficiently linked and cross-dependent to be inviting targets (Rona 1976). Also, thinking about vulnerabilities and critical targets had become a well-established part of US air power theorists' culture during the Cold War.

The Second Persian Gulf War of 1991 created a watershed in US military thinking about cyber-war. Military strategists saw the conflict as the first of a new generation of information age conflicts, in which physical force alone was not sufficient, but was complimented by the ability to win the information war and to secure "information dominance." As a result, American military thinkers began to publish scores of books on the topic and developed doctrines that emphasized the ability to degrade or even paralyze an opponent's communications systems (cf. Campen 1992; Arquilla and Ronfeldt 1993, 1997). In the mid-1990s, the advantages of the use and dissemination of ICT that had fuelled the revolution in military affairs were no longer seen only as a great opportunity providing the country with an "information edge" (Nye and Owens 1996), but were also perceived as constituting an overproportional vulnerability vis-à-vis a plethora of malicious actors, which was then taken up in the civil defense discourse.

At the same time, the development of military doctrine involving the information domain continued. For a while, information warfare—the new type of warfare in the information age—remained essentially limited to military measures in times of crisis or war. This began to change around the mid-1990s, when the activities began to be understood as actions targeting the entire information infrastructure of an adversary—political, economic, and military, throughout the continuum of operations from peace to war (Dunn Cavelty 2010a). NATO's 1999 intervention against Yugoslavia marked the first sustained use of the full spectrum of information warfare components in combat. Much of this involved the use of propaganda and disinformation via the media (an important aspect of information warfare), but there were also Web site defacements, a number of DDoS attacks, and (unsubstantiated) rumors that Slobodan Milosevic's bank accounts had been hacked by the US armed forces (Dunn 2002: 151). The increasing use of the Internet during the conflict gave it the distinction of being the "first war fought in cyberspace" or the "first war on the Internet." Thereafter, the term cyber-war came to be widely used to refer to basically any phenomenon involving a deliberate disruptive or destructive use of computers.

2.3.4.1 Trends and Developments

The discovery of Stuxnet in 2010 changed the overall tone and intensity of the debate. Stuxnet is a computer worm that was discovered in June 2010 and has been called “[O]ne of the great technical blockbusters in malware history” (Gross 2011). In August 2010, the security company Symantec noted that 60 % of the infected computers worldwide were in Iran. It was also reported that Stuxnet damaged centrifuges in the Iran nuclear program. Due to the attribution problem, which refers to the difficulty of identifying those initially responsible for a cyber-attack and their motivating factors, it was impossible to know for certain who was behind this piece of code, though many suspected one or several state actors. In June 2012, it was suggested that the development of Stuxnet was part of a US and Israeli intelligence operation called “Operation Olympic Games” and that it was indeed programmed and released to sabotage the Iranian nuclear program (Sanger 2012). Though neither state has ever officially admitted to the release of this malware, state involvement is considered a fact worldwide.

For many observers, Stuxnet meant that the “digital first strike” has occurred, which they saw as marking the beginning of the unchecked use of (clandestine) cyber-weapons in military-like aggressions (Gross 2011). Stuxnet provided a platform for an ever-growing host of cyber-war experts to speculate about the future of cyber-aggression. Internationally, Stuxnet has had two main effects: First, governments all over the world started releasing or updating cyber-security strategies and set up new organizational units for cyber-defense (and cyber-offense). Second, Stuxnet can be considered a “wake-up” call: Ever since its discovery, increasingly serious attempts to come to some type of agreement on the non-aggressive use of cyberspace between states are undertaken (Dunn Caveltly 2011). Ever since its discovery, a militarization of cyberspace can be observed as an increasing amount of states have invested heavily into cyber-defense capabilities (and most likely also cyber-offense) (Farwell and Rohozinski 2011).

Furthermore, Snowden’s NSA revelations have confirmed that the USA is actively preparing for a future cyber-war by exploiting vulnerabilities in the existing information infrastructure and actively creating new ones in the form of backdoors. It is unknown which computer systems have been compromised—but it is known that these backdoors or sleeper programs can be used for different purposes (surveillance, espionage, disruption, etc.) and activated at any time.

2.3.4.2 Military and Cyber in Switzerland

In Switzerland, the military dimension of cyber-security has developed separately to the rest of the policy efforts. The Swiss military is in a somewhat special

position in comparison with other armies, due to the country's militia system (only about 5 % of soldiers are "professional," the rest are (mainly male) citizen conscripts) and because of Switzerland's long history of neutrality. The Swiss armed forces' main task is defense against an armed attack, whether on the ground or in the air. Also, they also have a task to protect important installations and traffic routes in the event of heightened tensions, special events, or clear threats (subsidiary operations).

There were several concerted efforts in Switzerland to build capabilities for conducting (defensive) information operations. For a considerable number of years, for example, a conceptual study was drafted, which used an extensive network of professionals from the federal administration, industry, and academia to define a coherent, doctrinal basis for information operations (cf. [digma 2004](#)). However, when the study was finalized in 2005, it created quite a ruckus politically (and in the media) and all plans for building up a dedicated information operation unit were stopped immediately. This was due among other factors to legal ambiguities, financial and personnel shortfalls, and political reservations, for instance with regard to so-called psychological operations, which are mainly about perception management, sometimes even within one's own territory ([Dunn Cavelty 2008b, 2010b](#)).

In general, it is the Armed Forces Command Support Organisation (CSO) that is in charge of cyber-security issues [together with Information Security and Facility Protection (ISFP)]. The CSO is ICT service provider for the armed forces in all situations, which entails a high degree of availability and security. It runs the Electronic Operations Centre (EOC) that provides services for the intelligence service. The EOC employs cryptologists and runs the sector for computer network operations (CNO), which is thus enabled to analyze threats and incidents and to conduct operations. The CSO also operates the Military Computer Emergency Response Team (milCERT) that monitors ICT infrastructure which is relevant for the armed forces. The CSO primarily supports the armed forces, but also the political leaders, and keeps respective resources available. This unit coordinates with the Government Computer Emergency Response Team (GovCERT), which is an important component of the Reporting and Analysis Center for Information Assurance (MELANI). Overall, it can be said that the Swiss military remains marginalized in the Swiss cyber-security setup, as will be shown in Chap. 5.

2.4 Conclusion

This chapter provided some background information for understanding the specific cyber-security policy solutions that began to emerge in the latter half of the 1990s, including Switzerland's emerging policy at the time. This chapter has introduced a set of national and international factors that shape cyber-security policy formulation more generally and then introduced four different variations of how cyber-security is often framed: as a technical, a crime-espionage, a civil defense,

and a military strategic issue. All four are interrelated and exist side by side in every country, but not all of them are equally influential.

For each of the four ways of framing cyber-security, this chapter gave examples of policy solutions that emerged in Switzerland. As will be shown in more detail in what follows, it is mainly a combination of the technical, the crime, and the civil defense variation that has shaped Switzerland's cyber-security efforts, whereby the military is marginalized. In the following chapters, three phases of Switzerland's cyber-security policy development are described in more details.

References

*All links accessed 4 July 2014.

- Ackerman S, Kaiman J (2014) Chinese military officials charged with stealing US data as tensions escalate. *The Guardian*, 20 May 2014. <http://www.theguardian.com/technology/2014/may/19/us-chinese-military-officials-cyber-espionage>
- Anderson RH, Hearn AC (1996) An exploration of cyberspace security R and D investment strategies for DARPA: "The Day After ... in Cyberspace II". RAND, Santa Monica
- Anderson R, Moore T (2006) The economics of information security. *Science* 314(5799):610–613
- Arquilla J, Ronfeldt DF (1993) Cyberwar is Coming! *Comp Strategy* 12(2):141–165
- Arquilla J, Ronfeldt DF (eds) (1997) *In Athena's camp: preparing for conflict in the information age*. RAND, Santa Monica
- Böhme R (2005) Vulnerability markets—What is the economic value of a zero-day exploit? Paper held at the 2005 Chaos Communication Congress Berlin, Germany. http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf
- Brown KA (2006) *Critical path: a brief history of critical infrastructure protection in the United States*. George Mason University Press, Arlington
- Brunner E, Suter M (2008) *The international CIIP handbook 2008/2009—An inventory of protection policies in 25 countries and 6 international organizations*. Center for Security Studies, Zurich
- Campen AD (ed) (1992) *The first information war: the story of communications, computers and intelligence systems in the Persian Gulf War*. AFCEA International Press, Fairfax
- Clarke RA, Morell MJ, Stone GR, Sunstein CR, Swire P (2013) *Liberty and security in a changing world: report and recommendations of the President's review group on intelligence and communications technologies*. Washington, DC. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
- Collier S, Lakoff A (2008) The vulnerability of vital systems: how 'critical infrastructure' became a security problem. In: Kristensen KS, Dunn Cavelti M (eds) *The politics of securing the homeland: critical infrastructure, risk and securitisation*. Routledge, London
- Computer Science and Telecommunications Board (1989) *Growing vulnerability of the public switched network: implications for national security emergency preparedness*. National Academy Press, Washington
- CYCO (2013) *Cybercrime coordination unit Switzerland CYCO, annual report 2013*. Available at http://www.fedpol.admin.ch/content/fedpol/en/home/dokumentation/berichte/jb_kobik.html
- digma (2004) *Zeitschrift für Datenrecht und Informationssicherheit*, Special Issue on Information Operations, 4(2). http://emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/03/digma_2004.2_fokus_io.pdf
- Dunn M (2002) *Information age conflicts: a study of the information revolution and a changing international operating environment*. Zurich contributions to security policy and conflict analysis Nr. 64. Center for Security Studies, Zurich

- Dunn Cavelty M (2008a) *Cyber-security and threat politics: US efforts to secure the information age*. Routledge, London
- Dunn Cavelty M (2008b) Information operations: trends and controversies. *CSS analysis in security policy*, No. 34, May 2008
- Dunn Cavelty M (2010a) *Cyberwar*. In: Kassimeris G, Buckley J (eds) *The Ashgate Research Companion to Modern Warfare*. Ashgate, Aldershot
- Dunn Cavelty M (2010b) *Cyberwar: concept, status quo, and limitations*. *CSS analysis in security policy*, No 71, April 2010
- Dunn Cavelty M (2011) The dark side of the net: past, present and future of the cyberthreat story. *AIIA Policy Commentary* 10: 51–62
- Dunn Cavelty M (2013) From Cyber-Bombs to political-fallout: threat representations with an impact. *Int Stud Rev* 15(1):105–122
- Farwell JP, Rohozinski R (2011) Stuxnet and the future of Cyber War. *Survival: Glob Politics Strategy* 53(1): 23–40
- Federal Council (1999) *Security through cooperation—Report of the federal council to the federal assembly on the security policy of Switzerland*, Berne, June 1999
- Gray CH (1997) *Postmodern War—The new politics of conflict*. Routledge, London
- Greenwald G, MacAskill E (2013) Obama orders US to draw up overseas target list for cyber-attacks, *The Guardian*. <http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas>
- Gross MJ (2011) Stuxnet worm: a declaration of cyber-war, vanity fair. <http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104>
- Kingdon JW (2003) *Agendas, alternatives, and public policies*, 2nd edn. Harper Collins College Publishers, New York
- Leiner et al. (1997) 'A brief history of the internet', Website of the Internet Society. <http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet>
- Libicki MC (2000) *The future of information security*. Institute for National Strategic Studies, Washington
- Maillart T, Sornette D (2010) Heavy-tailed distribution of cyber-risks. *Eur Phys J B* 75(3):357–364
- MELANI (2009) Semi-annual report 2009/2. Bern, Reporting and Analysis Centre for Information Assurance MELANI. <http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html>
- MELANI (2010) Semi-annual report 2010/2. Bern, Reporting and Analysis Centre for Information Assurance MELANI. <http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html>
- Molander RC, Riddle AS, Wilson PA (1996) *Strategic information warfare: a new face of war*. RAND, Santa Monica
- Morozov E (2013) To save everything, click here: technology, solutionism, and the urge to fix problems that don't exist. Allen Lane, UK
- National Academy of Sciences (1991) *Computer science and telecommunications board, computers at risk: safe computing in the information age*. National Academy Press, Washington
- Nye Jr JS, Owens WA (1996) America's information edge. *Foreign Aff* 75(2):20–36
- Panda Security (2010) *Panda security report: the cyber-crime black market: uncovered*
- Parrika J (2005) Digital monsters, binary aliens—computer viruses, capitalism and the flow of information. *Fibreculture Journal* Issue 4—contagion and the diseases of information. <http://vxheavens.com/lib/mjp00.html>
- President's Commission on Critical Infrastructure Protection (1997) *Critical foundations: protecting America's infrastructures*. US Government Printing Office, Washington
- Rona TP (1976) *Weapon systems and information war*, Boeing Aerospace Co. Research Report, Seattle
- Sanger DE (2012) Obama order sped up wave of cyberattacks against Iran. *The New York Times*, 1 June 2012
- Scherlis WL, Squires SL, Pethia RD (1990) *Computer emergency response*. In: Denning P (ed) *Computers under attack: intruders, worms, and viruses*. Addison-Wesley, Reading

- Scott MD (2007) Internet and technology law desk reference. Aspen Publishers, New York
- Spafford EH (1989) The internet worm: crisis and aftermath. *Commun ACM* 32(6):678–687
- Stoll C (1989) The cuckoo's egg: tracking a spy through the maze of computer espionage. Doubleday, New York
- Symantec (2010) Internet security threat report, vol 16. Mountain View
- United States General Accounting Office (1996) Information security: computer attacks at department of defense pose increasing risk. GAO/AIMD-96-84. General Accounting Office, Washington
- Verizon (2010) 2010 data breach investigations report: a study conducted by the Verizon risk team in cooperation with the United States secret service, New York



<http://www.springer.com/978-3-319-10619-9>

Cybersecurity in Switzerland

Dunn Cavelty, M.

2014, X, 75 p. 2 illus., Softcover

ISBN: 978-3-319-10619-9