Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

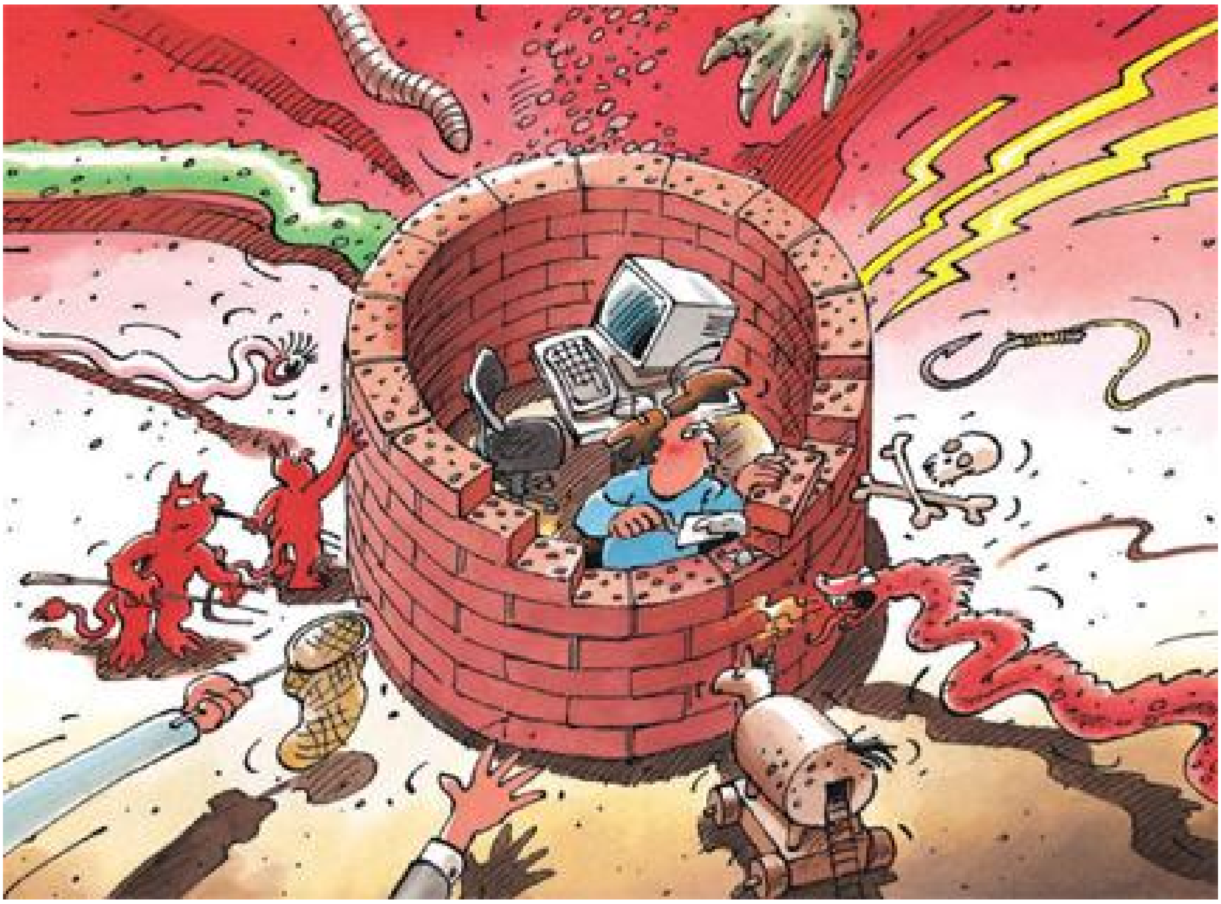
Federal Strategy Unit for IT FSUIT
Federal Intelligence Service FIS

Reporting and Analysis Centre for Information Assurance MELANI
www.melani.admin.ch

Information Assurance

Situation in Switzerland and Internationally

Semi-annual report 2010/I (January – June)



Contents

1 Focus Areas of Issue 2010/I

Espionage using IT resources – Growing threat

Several espionage cases became known over the past half-year, including against Google, Adobe, and also against the office of the Dalai Lama. In the most recent report on protection of the constitution, German Interior Minister Thomas de Maizière likewise warned of the growing threat of industrial espionage. Businesses and public authorities are particularly at risk. The espionage cases that have surfaced should not be seen as independent and isolated cases, but rather attention should be paid to the similarities with respect to infrastructure, for instance. A comprehensive analysis of the cases is therefore needed.

► Current topics internationally: Chapter 4.1

► Trends/Outlook: Chapter 5.1

Complicated data protection policies and settings of Internet services

Suppliers of Internet-supported devices, social networks, and other Internet communication services make life easier and offer the advantage that their customers can connect more easily with each other and exchange information. By gathering statistical usage data, services can be improved and (free) services can be paid for by increasingly targeted advertisement. For this reason, the suppliers of such applications want to gather as much information as possible about their users. Users wanting to protect their privacy must often wade through pages and pages of complicated data protection settings, often without understanding what configurations lead to what consequences.

► Trends/Outlook: Chapter 5.3

Infected systems and websites – MELANI's possibilities

In February, e-mails containing malware were observed which targeted persons working in the public sector as well as educational institutions. MELANI was able to identify the command & control server of the botnet and notify the competent authorities abroad. In Switzerland, the attack was not successful.

► Current topics in Switzerland: Chapter 3.4

To combat the misuse of Swiss Internet addresses and to defend against acute threats to Internet users, the revision of the Ordinance on Address Elements in Telecommunications includes a new provision allowing .ch domain names to be blocked under certain circumstances.

► Current topics in Switzerland: Chapter 3.5

Since April of this year, the Reporting and Analysis Centre for Information Assurance (MELANI) has operated a check tool to look for website infections on .ch websites. A first evaluation of the months June – August 2010 shows that a total of 148 websites with infections were found, representing 0.06% of the examined .ch domains.

► Current topics in Switzerland: Chapter 3.3

2 Introduction

The eleventh semi-annual report (January – July 2010) of the Reporting and Analysis Centre for Information Assurance (MELANI) presents the most significant trends involving the threats and risks arising from information and communication technologies (ICT). It provides an overview of the events in Switzerland and abroad, illuminates the most important developments in the field of prevention, and summarizes the activities of public and private actors. Explanations of jargon and technical terms (*in italics*) can be found in a **Glossary (Chapter 6)** at the end of this report. Comments by MELANI are indicated in a shaded box.

Selected topics covered in this semi-annual report are outlined in **Chapter 1**.

Chapters 3 and 4 discuss breakdowns and failures, attacks, crime and terrorism connected with ICT infrastructures. Selected examples are used to illustrate important events of the first half of 2010. Chapter 3 covers national topics, Chapter 4 international topics.

Chapter 5 discusses trends and contains an outlook on expected developments.

3 Current National ICT Infrastructure Situation

3.1 Communication of vulnerabilities

Some *vulnerabilities* have captured the media's attention in the past, such as the vulnerability of Internet Explorer in January 2010. But also vulnerabilities of Adobe Acrobat and the iPhone have been in the news. Such vulnerabilities are especially serious when countermeasures are not easy to seize. As a reaction to the vulnerability affecting several versions of Internet Explorer in January 2010, the German Federal Office for Information Security (BSI) recommended not using the Microsoft *browser* for the time being, but instead to use an alternate browser until a *patch* was made available. The cause of the warning was that running Internet Explorer in "*protected mode*" and turning off *active scripting* made attacks more difficult, but could not prevent them entirely. Publications of public warnings are regulated by law at the BSI and there are expectations of the politicians to warn citizens about vulnerabilities.

Whether in Germany or Switzerland, a federal authority is given close scrutiny with regard to the measures it recommends in the event of vulnerability. The media attention after the BSI recommendation not to use Internet Explorer was accordingly enormous, and also a subject for the Swiss media. On the one hand, the difficulty in making a recommendation consists in proposing a secure, but also feasible alternative. Naturally, companies cannot immediately switch to a different browser application. Such a switch must be planned long beforehand. Otherwise, overloaded hotlines as well as anxious and potentially irritated staff members are a sure thing. For instance, when the LNK vulnerability occurred in July 2010, exploiting a bug in the Windows shell relating to the evaluation of LNK and PIF file parameters, many businesses had to decide whether the recommended *workaround*, namely to remove the *shortcut icons*[1], was a feasible option. Using this emergency solution, potential malware was disabled, but it had to be taken into account that the disappearance of the accustomed icons would lead to great uncertainty among employees. It must always be taken into account how great the potential damage and how widespread the malware in question is, and how this weighs against the effort to implement the recommended measures. Ultimately, every business is responsible for this decision itself. In such cases, MELANI tries to supply operators of critical infrastructures with background information to facilitate such decisions. However, good communication is always enormously important for the implementation of workarounds, along with stronger support.

As a matter of principle, MELANI shows restraint when warning the public about vulnerabilities. Due to the large number of vulnerabilities in many different programmes, too many warnings would dull users' sensitivity. Experience also shows that issued recommendations are only implemented by a small number of users, since the recommendations are either too complicated or too restrictive. Every Internet user should therefore be aware that all programmes have critical weaknesses – even weaknesses that have not been publicly announced, but are already being exploited. The latter are usually used for purposes of espionage and may cause great damage to businesses and governments. A well-developed, permanent basic level of protection is therefore absolutely necessary.

Additionally, there are programmes that one can hardly do without anymore in everyday

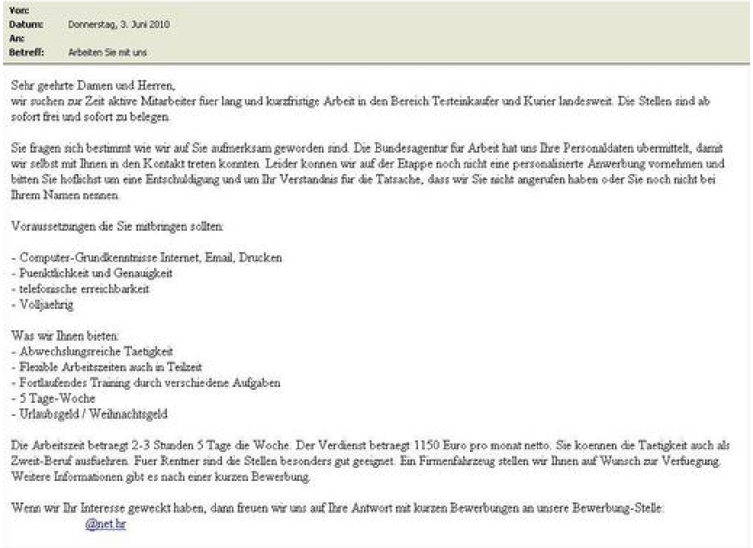
[1] As a consequence, the shortcuts still would have been available, but they would have all looked the same and not been distinguishable by different icons.

work. When such programmes are affected by a vulnerability, security risks can at most be counteracted using flanking measures, such as training of employees or blocking of well-known malware servers or e-mails. For this purpose, exchange of information between companies but also between providers is necessary. Between operators of *critical infrastructures*, such information exchange is available through the Reporting and Analysis Centre for Information Assurance (MELANI). Similar information portals for small and medium enterprises are still rare and in the testing phase.

3.2 Looking for financial agents for money laundering

There are still people who are enticed by criminals to serve as "financial agents", especially when the effort is minimal and no special qualifications are necessary: financial agents need only take a bit of time each day to let money be transferred to their bank account, so that they can forward it from there to a third party. Financial agents are promised a certain percentage of the transferred amount as commission. Financial agents, i.e. money couriers who let themselves be used for laundering money obtained through online fraud, are sought after by criminals. Financial agents are scarce and are often only used for a single transaction, since they generally are exposed soon thereafter and are reported to the competent authorities.

Since June 2010, more and more e-mails have been circulating in Switzerland again for recruiting such money couriers, promising attractive compensation. People who respond to such offers generally receive a money transfer to their account shortly thereafter, which is to be transferred abroad, usually by way of Western Union. Anyone participating in such "business transactions" risks criminal prosecution as an accomplice to money laundering (Article 305bis of the Criminal Code).



Von:
Datum: Donnerstag, 3. Juni 2010
An:
Betreff: Arbeiten Sie mit uns

Sehr geehrte Damen und Herren,
wir suchen zur Zeit aktive Mitarbeiter fuer lang und kurzfristige Arbeit in den Bereich Testeinkaufer und Kurier landesweit. Die Stellen sind ab sofort frei und sofort zu belegen.

Sie fragen sich bestimmt wie wir auf Sie aufmerksam geworden sind. Die Bundesagentur für Arbeit hat uns Ihre Personaldaten ubermittelt, damit wir selbst mit Ihnen in den Kontakt treten konnten. Leider konnen wir auf der Etappe noch nicht eine personalisierte Anwerbung vornehmen und bitten Sie hoflichst um eine Entschuldigung und um Ihr Verstandnis für die Tatsache, dass wir Sie nicht angerufen haben oder Sie noch nicht bei Ihrem Namen nennen.

Voraussetzungen die Sie mitbringen sollten:

- Computer-Grundkenntnisse Internet, Email, Drucken
- Puenktlichkeit und Genauigkeit
- telefonische erreichbarkeit
- Volljaehrig

Was wir Ihnen bieten:
- Abwechslungsreiche Taetigkeit
- Flexible Arbeitszeiten auch in Teilzeit
- Fortlaufendes Training durch verschiedene Aufgaben
- 5 Tage-Woche
- Urlaubsgeld / Weihnachtsgeld

Die Arbeitszeit betraegt 2-3 Stunden 5 Tage die Woche. Der Verdienst betraegt 1150 Euro pro monat netto. Sie koennen die Taetigkeit auch als Zweit-Beruf ausfuehren. Fuer Rentner sind die Stellen besonders gut geeignet. Ein Firmenfahrzeug stellen wir Ihnen auf Wunsch zur Verfuegung. Weitere Informationen gibt es nach einer kurzen Bewerbung.

Wenn wir Ihr Interesse geweckt haben, dann freuen wir uns auf Ihre Antwort mit kurzen Bewerbungen an unsere Bewerbung-Stelle:
@net.hr

Sample financial agent e-mail

Such offers are not only distributed by e-mail, but also on various Internet sites with legitimate job advertisements. As a rule, caution is required when one is asked to take money one has previously received (whether intentionally or erroneously) and to transfer it to unknown third parties by way of cash transfer. In any event, offers promising large profits should be treated with caution. Also on the Internet, the rule generally applies that one cannot get rich quick without investing corresponding effort. One should never make one's own bank accounts available to third parties.

That not only private individuals are tricked by such job offers is shown by a case in which a social administration employee recommended such a job as a financial agent to an unemployed person. Especially in the field of social work/job placement, awareness must be raised concerning this danger, since otherwise persons already in a difficult situation may end up in deeper trouble.

3.3 MELANI checks .ch websites for infections

Since April of this year, the Reporting and Analysis Centre for Information Assurance (MELANI) has used a check tool to look for *website infections* on Swiss websites. First the tool checks the *source code* of the website for known signatures, then the site is visited regularly and automatically, and finally the tool analyzes what actions are triggered on the computer. A list defines permissible and prohibited actions and sounds an alarm accordingly.

A first evaluation of the months June – August 2010 shows that a total of 148 domains with infections were found, representing 0.06% of the examined .ch domains:

.ch domains with website infections	148
- .ch domains cleaned	116
- .ch domains infected	32
Total untersuchte CH-Domänen	237’421

Upon finding a website infection, the Reporting and Analysis Centre for Information Assurance (MELANI) directly informs the website user or provider, so that the necessary steps for cleaning the website can be taken, Since July 2010, MELANI also has the option of requesting SWITCH to block a .ch domain (see Chapter 3.4). So far, MELANI has not made use of this option, and it will only use it in future if other, less invasive measures are unsuccessful. Since practically all of the affected websites have been hacked, and since the user generally has no idea that malicious code is on the website, such infections can generally be addressed bilaterally.

There are different ways to upload manipulated websites onto a webserver. Under the most frequent method, stolen FTP access data are used to access the webserver. For this purpose, the attacker may, for instance, have a list with FTP login data. The data is then used to automatically log into the account; a web page is downloaded (usually the *index* page or an existing .js JavaScript file), the malicious code is smuggled in, and the page is then uploaded again. Other options include exploiting vulnerabilities in the *content management system (CMS)* or web applications installed on the website, as well as *cross-site scripting* in guestbooks or forums. The exploitation of vulnerabilities in ad servers, i.e. servers used to display web banners, is another possibility that is gaining popularity.

Measures for website-administrators upon recognizing a website infection

In general: The malware attempts to infect the user's computer even if the page is simply visited. We therefore recommend directly examining the source code on the server and to visit the page not at all or only with appropriate security measures until the infection is removed. (Turn off JavaScript and ActiveScripting, turn off iFrame, etc.)

- If *there is no CMS and the data have been uploaded to the server via FTP*, the simplest solution is to upload the locally stored web page to the server again. The date on which the page was last modified may give an indication of which pages have been

compromised. This modification date can be found in the FTP programmes. If no changes have been made in the last while, but the modification date indicates a recent change, this may be a clue that the page in question has been compromised.
It is important to subsequently change the password and to check whether the computer administering the website contains a trojan.

- *If a CMS is used to administer the website,* it must be determined where the malicious code was smuggled in. Usually, this happens in repeated elements such as headers or footers. The malicious code may also be programmed permanently in the CMS, however. If the location of the malcode cannot be found and removed, we recommend asking the hosting provider for help.
Very important: Regularly update the CMS and change the access data.

- Recently, *web banners* have also frequently been affected by website infections. Such infections have a particular wide range, since they are displayed on a large number of websites. Recently, the ad programme OpenX has been particularly prone to attacks.
It is very important to always update ad servers.

3.4 MELANI discovers botnet and initiates takedown

In the third week of February, MELANI received information concerning a targeted hacker attack by way of infected e-mails. These e-mails were sent to employees of the public sector and educational institutions.

The e-mails, written in English, contained a document concerning a NATO conference that was said to take place on 24/25 February 2010 with the title: "C4I cooperation in South-Eastern Europe (SEE) – the new look". Upon opening the file, the computer was infected and included in a *botnet*. The code's function was in particular to intercept login data for e-mails and social networks.

By analyzing the malicious document, MELANI was able to identify the *command & control servers* and an extensive list of infected systems. These data were then made available to the responsible authorities in order to deactivate the botnet. No victims were found in Switzerland.

In the described case[2], the e-mails targeted persons in the public sector and at specific educational institutions. The question therefore arises why the attack was addressed to this audience. There are two possible explanations: the first assumes that this really was a targeted (espionage) attack and that exactly these persons were the intended targets. For this purpose, *social engineering* is used in advance to obtain addresses and other information regarding the persons to be spied on. A second explanation is that this was not a targeted attack, but rather that the criminals wanted to stay below the radar of anti-virus manufacturers and only infect a small number of persons. The e-mail addresses were then bought from other criminals. Attackers have meanwhile realized that widespread attacks are often of little use, since they create a big stir and accordingly result in a greater response by

[2] In the first half of 2010, other similar cases occurred. These included the e-mail with the subject "Military operation of the EU NAVFOR Somalia", supposedly sent on behalf of the European Union (http://contagiodump.blogspot.com/2010/08/cve-2010-1240-with-zeus-trojan.html), or the e-mail with the subject "2020 Project" circulated on behalf of the "National Intelligence Council" (http://krebsonsecurity.com/2010/02/zeus-attack-spoofs-nsa-targets-gov-and-mil/).

anti-virus manufacturers, researchers, security experts, etc. Quiet attacks are more efficient, even though they reach fewer people.

3.5 Blocking of .ch domain names on suspicion of misuse

To combat the misuse of Swiss Internet addresses and to defend against acute threats to Internet users, the revision of the Ordinance on Addressing Resources in the Telecommunications Sector (TSRO, SR 784.104) includes a new provision. According to this provision, the register operator of .ch domains (SWITCH) must, under certain circumstances, block such domain names and suspend the corresponding assignment to a *name server*.

Pursuant to Article 14*f*$^{\text{bis}}$ TSRO[3], which entered into force on 1 January 2010, a .ch domain name may be blocked and the corresponding assignment to a name server may be suspended. This is the case when there is justified suspicion that the domain name is being used either to obtain sensitive data by unlawful means (*phishing*) or to distribute malware via the domain. Additionally, an anti-cybercrime authority recognized by the Federal Office of Communications (OFCOM) must request the blocking. For a duration of at most five business days, SWITCH may also seize measures autonomously, but must suspend them again if they are not confirmed by an authority entitled to make a request.

When blocking a domain name, the following approaches are distinguished: either modifications of the entry in the administrative infrastructure of the domain assignment are prevented ("freezing" of the domain record – but the website remains accessible), or the assignment to a name server is suspended, with the consequence that – after being updated in the *domain name system (DNS)* – the website can no longer be reached by entering the domain name. This latter measure merely prevents Internet users from being harmed by accessing this Swiss address. The contents on the webserver are not deleted, however, and the criminals may at any time use another domain name to reach the content. To that extent, it is a minor measure to improve the options for defending against threats in the Swiss address space of the Internet and to protect Internet users when they surf on .ch websites.

Since 15 June 2010, the Reporting and Analysis Centre for Information Assurance (MELANI) has been recognized by the Federal Office of Communications (OFCOM) as the competent authority in this regard. MELANI may now request SWITCH to block and suspend the assignment to a .ch domain name server upon justified suspicion of phishing or distribution of malware.

MELANI will show much restraint in using this option, and will only employ it as a last resort if the threat cannot be eliminated by other means. As already mentioned in the last semi-annual report, malware is currently often spread via hacked websites. In such cases, contacting the legitimate website operator or hosting provider can usually eliminate the problem. Using this informal approach, MELANI achieved significant success already before the TSRO revision.

Pursuant to an amendment to SWITCH's domain name registration contract, according to which a domain name can only be used after payment of a fee, abusive registrations of .ch domain names have practically vanished with respect to phishing and have been substantially reduced with respect to malware.

[3] http://www.admin.ch/ch/d/sr/784_104/a14bist.html (as of 27 August 2010)

3.6 The Federal Council submits dispatch on ratification of the Cybercrime Convention[4]

The Council of Europe Convention on Cybercrime of 23 November 2001[5] is the first and so far only international convention dealing with computer and network crime. The Contracting States are obliged to adjust their legislation to the challenges of new information technologies, and the Convention aims to harmonize computer penal law. The Convention also provides rules for penal proceedings (especially gathering and securing of electronic data as evidence), and co-operation among the Contracting States is intended to be fast and efficient. Switzerland already largely meets the requirements under the Convention.[6]

A legislative amendment will be necessary with respect to the criminal offence of unauthorized access to a data processing system (Article 143bis of the Criminal Code, also referred to as "hacking"). The envisaged amendment will move up criminal liability in analogy to the criminal provision against *computer viruses* (Article 144bis(2) of the Criminal Code[7]): criminal liability already attaches to persons who make programmes, passwords or other data available and know or should know that these will consequently be used for purposes of illegal access to a computer system.[8]

According to the Federal Council's dispatch[9], the distribution of "*dual use*" devices and data will continue to be permissible, however, under certain circumstances and with appropriate measures. Security tests of computer systems, i.e. vulnerability assessments, carried out by the operator or a mandated third party, as well as the development of new software for such purposes are considered acts carried out or mandated by an authorized party and are therefore not subject to punishment. Quality assurance measures concerning one's own systems and on behalf of third parties are likewise not considered punishable, and the training of ICT security experts, in which the use of hacking tools is discussed and implemented, remains legal.

In contrast, the intentional dissemination of programmes and other data is considered punishable (with respect to both the act itself and further use of the data) as well as the irresponsible dissemination of datasets whose sensitive content, circle of addressees, or other circumstances makes the criminal use of the tools appear obvious. The irresponsible dissemination of hacking tools in an environment prone to offences[10] should not remain without punishment. "*Reasonable disclosure*" in the event of vulnerabilities will continue to be possible – but public "*full disclosure*" should be punishable in future.

The ratification draft of the Federal Council was submitted to Parliament and must now be approved by both chambers of Parliament. Ratification is also subject to facultative treaty referendum.

[4] Dossier at the Federal Office of Justice: http://www.bj.admin.ch/bj/de/home/themen/kriminalitaet/gesetzgebung/cybercrime__europarat.html (as of 27 August 2010)

[5] Convention on Cybercrime, ETS 185: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/ConventionOtherLg_en.asp (as of 27 August 2010)

[6] http://www.bj.admin.ch/bj/de/home/dokumentation/medieninformationen/2010/ref_2010-06-181.html (as of 27 August 2010)

[7] http://www.admin.ch/ch/d/sr/311_0/a144bis.html (as of 27 August 2010)

[8] Formulation according to draft: http://www.admin.ch/ch/d/ff/2010/4747.pdf (BBl 2010 4749) (as of 27 August 2010)

[9] http://www.admin.ch/ch/d/ff/2010/4697.pdf (as of 27 August 2010)

[10] The public area of the Internet must certainly be included here.

3.7 Misuse of domains: danger of forgetting to renew domain registration

On 10 June 2010, for a short time websites of the cable network provider Cablecom were only partially available. The reason was a failure to renew the cablecom.net domain, which is used as the name server for Cablecom services. Once the omission was noticed, the domains were immediately renewed for 10 more years.

What in this case had no major consequences other than perhaps a chuckle or two is a problem that should not be underestimated and affects all businesses – but also private individuals – maintaining a website. There is a veritable market for expired domain names, regardless of whether renewal of the registration was forgotten or whether the domains are really no longer used. This is especially serious e.g. in the case of school websites, which may be used for *hosting* salacious content once the domains are released.

In another Swiss case, the original website was copied after the domain became available, and the same domain was again uploaded to the net. However, the new-old website was furnished with various additions such as click ads and even malware. The advantage of this domain abuse (squatting) is obvious: since the domains are already known, they attract a large number of visitors, and many links already (or rather, still) lead to the website. The damage to the business includes loss of reputation, loss of time and money to regain the domain, and loss of potential clients.

What is often forgotten is that all e-mails sent to the old domain can be read without difficulty by the new domain user. The new user does not even need to know the exact e-mail address: with the "catch-all" function, all e-mails sent to a domain are intercepted and forwarded to a central address.

All domain owners should make such that they renew and also pay for their domains in a timely manner.[11] Even if a domain is relinquished intentionally, one should still be aware that anyone with any sort of business model – however dubious – may subsequently use that address to conduct business.

3.8 Hacking and its physical consequences – Example: automobile

3.8.1 Wireless interference in Arbon

Car drivers parking their cars last year in the southern part of the old town of Arbon often encounter the problem of not being able to use their electronic keys to unlock their cars. In February of this year, specialists from the Federal Office of Communications (OFCOM) figured out what the problem was. An older wireless loudspeaker had been transmitting on the same frequency used by electronic car keys. Wireless car keys use frequencies between 433.0-434.79 MHz, which is also referred to as the *Industrial, Scientific and Medical Band (ISM Band)*[12][13]. Other wireless uses are also permitted in this band, however, including

[11] Various registration services expressly reserve the right to release the domain if payment is not on time. This obviates the effort for them to send out costly reminders.

[12] http://www.bakom.admin.ch/themen/frequenzen/00652/00653/index.html?lang=de (as of 27 August 2010)

[13] http://de.wikipedia.org/wiki/ISM-Band: ISM bands (Industrial, Scientific and Medical bands) refer to frequency bands that can be used by high frequency devices in industry, science, medicine, at home and for similar applications. ISM

wireless weather stations, wireless loudspeakers and earphones. Amateur radio operators can also use this band – with considerably more power than car keys do. All these wireless uses may interfere with car receivers waiting for a key signal, causing them to stop working.

In this case, the interference was unintentional. But criminals do use exactly this type of interference to break into cars. If someone sends a jamming signal at precisely the moment when the driver tries to lock the car, and the driver does not check whether the car is really locked, then the car doors are open to the criminal, who can then search the car for valuables undisturbed.

3.8.2 100 cars disabled wirelessly

Owners can block their stolen cars using a wireless immobilizer system. This system can also be used in mobile computers, so that laptops can be blocked remotely or even data deleted and the hard drive reformatted. Using MobileMe, iPhones and iPads can likewise be remotely deleted from any computer.[14]

That such systems are not immune from manipulation is obvious. In the US, this happened in the last half-year. A former employee of a car dealership deactivated more than 100 customers' cars via the Internet. With the Webtech Plus system used in this case, car dealers are able to prevent customers from starting their cars if they fail to make their financing or leasing payments on time.

Such services, including the central administration of immobilization systems or access blocks on computers and mobile telephones, will be offered more frequently in future. Although these services are in principle a good thing and mean greater security, they also harbour certain risks, since such tools are administered centrally. Manipulations with major consequences are possible in this way. As the example above shows, this does not necessarily mean the hacking of a system; it may also be an employee or former employee who deliberately or through inappropriate behaviour manipulates the system.

3.8.3 Manipulation of modern cars

More and more electronics are integrated in modern cars. Almost the entire steering system is monitored by onboard systems. It is therefore not astonishing that even cars could become the target of hacker attacks. This is currently still utopia. Nevertheless, researchers at American universities over the past half-year have shown how to penetrate the onboard system of a moving car and take control of it. For instance, the driver's control of the brakes was disabled, and the engine was turned on and off. The only thing not subject to remote control was the steering mechanism, which in this case was still mechanical.

Since the onboard systems of today's cars generally do not have a wireless connection, a cable connection to the car was still necessary in this case, which means that the manipulator either would have to sit in the car himself or herself, or such a wireless

devices such as microwave ovens and medical appliances for short wave radiation require only a general license. Some ISM bands are also used for audio and video transmission or data transmission such as WLAN and Bluetooth without individual frequency assignments for these purposes. These are not ISM applications, however, and are subject to their own regulations. In especially frequently used bands, such as the 433 MHz and 2.54 GHz bands, the overlapping can easily cause interference between different devices. (As of 27 August 2010)

[14] http://www.apple.com/mobileme/features/find-my-iphone.html (as of 27 August 2010)

connection would have to be installed first. Should onboard systems be connected to the Internet in future, however, this would open the gates to manipulation.

3.9 Switzerland now has digital identities (SuisseID)

With the Federal Law of 19 December 2003 on Certification Services relating to Electronic Signatures (Electronic Signatures Act, SR 943.03)[15], the legal basis has been created in Switzerland to offer certification services relating to *electronic signatures* and to have these services recognized by the State. Since *certificates* in conformity with the Electronic Signatures Act can be used solely for qualified electronic signatures, these certificates are issued as a SuisseID together with a certificate that can also be employed for authentication and therefore as a standardized electronic identity. This makes it possible to use online services from a wide range of suppliers and to prove to the supplier without a doubt that one's identity is authentic. In addition to several private suppliers, the following federal agencies currently accept the use of SuisseIDs: The Federal Office of Justice (criminal register portal), the Swiss Alcohol Board (application for distillation licences and registration of production and sales volumes for assessment), the Federal Tax Administration (various VAT services) and the Federal Customs Administration (reimbursements and audits).
Until the end of 2010 (or as long as supplies last), the federal government is subsidizing the private purchase of a SuisseID (smartcard or USB stick) with an amount of CHF 65.00 in order to promote the spread of SuisseIDs.

So far, there have been no studies on any security risks associated with SuisseID. The technology used corresponds to the generally recognized, current standards. However, risks may arise from the fact that SuisseID combines authentication and the qualified electronic signature on a single chip – for instance, when the owner of the SuisseID uses the same *PIN code* for authentication and for creating a legal signature for the sake of convenience. As with any security technology, user behaviour must be included in any overall assessment. Despite advanced legislation, qualified electronic signatures have so far not established themselves or become prevalent either at the national or international level. It remains to be seen whether SuisseID will provide the necessary impulses in this regard.

3.10 Improved identification of mobile Internet users

Due to the rapid growth of smartphones and mobile Internet access, the number of Internet connections has risen dramatically. In order to avoid the need for a separate *IP address* for every device, mobile communications providers are using Network Address Port Translation (NAPT). With NAPT, several thousand clients use the same IP address, but different *ports*. To identify a connection and its user, typically the IP address and the date and time are needed. These data are regularly stored in the web services' log files. To identify mobile users, the port number used would also have to be known. But this information is seldom recorded. This is one of the reasons why Parliament is calling for the registration of *wireless* prepaid cards.[16] The envisaged obligation to ensure that users can also be identified within private networks (i.e. behind a single IP address) is also probably a good thing – but it should not be ignored that more data may be necessary for identification than are usually available.

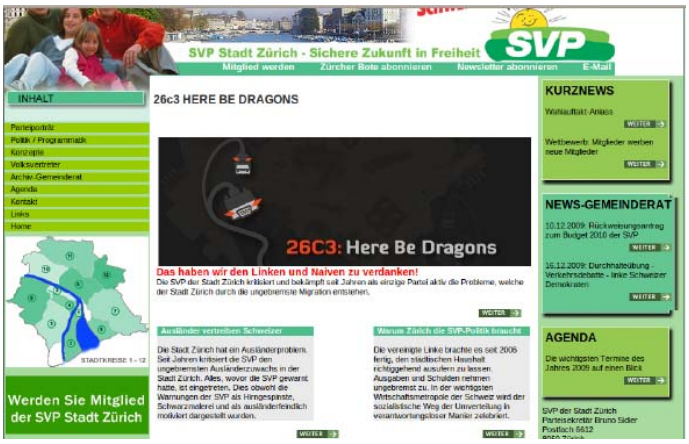
[15] http://www.admin.ch/ch/d/sr/c943_03.html (as of 27 August 2010)

[16] http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20073627 (as of 27 August 2010)

The current revision[17] of the Federal Law on the Surveillance of Postal and Telecommunications Traffic[18] and the design of the implementing ordinances thereof must take this fact into account.

3.11 Hackers do mischief with SVP and the European Union

At the end of 2009/beginning of 2010, the website of the SVP political party in the city of Zurich was defaced several times with the writing: "26C3 – Here be Dragons". A YouTube video referring to the minaret ban initiative was also uploaded. The video is based on the advertisement of a Swiss herbal candy manufacturer known for the slogan: "Who invented it?" "Here be Dragons" was the slogan of the 26th Congress of the Chaos Computer Club (CCC) in Berlin. The congress takes place between Christmas and New Year's each year and attracts up to 3,000 interested hackers, geeks, network artists, data protection experts, and so on. After the website was cleaned up, it was defaced again, this time with a hoax video titled "300 – SVP must die" based on the movie "300". This website defacement probably exploited a vulnerability in the content management system.



26c3 HERE BE DRAGONS

Das haben wir den Linken und Naiven zu verdanken!
Die SVP der Stadt Zürich kritisiert und bekämpft seit Jahren als einzige Partei aktiv die Probleme, welche der Stadt Zürich durch die ungebremste Migration entstehen.

Ausländer vertreiben Schweizer
Die Stadt Zürich hat ein Ausländerproblem. Seit Jahren kritisiert die SVP den ungebremsten Ausländerzuwachs in der Stadt Zürich. Alles, wovor die SVP gewarnt hatte, ist eingetreten. Dies obwohl die Warnungen der SVP als Hirngespinste, Schwarzmalerei und als ausländerfeindlich motiviert dargestellt wurden.

Warum Zürich die SVP-Politik braucht
Die vereinigte Linke brachte es seit 2006 fertig, den städtischen Haushalt richtiggehend ausufern zu lassen. Ausgaben und Schulden nehmen ungebremst zu. In der wichtigsten Wirtschaftsmetropole der Schweiz wird der sozialistische Weg der Umverteilung in verantwortungsloser Manier zelebriert.

Wahlauftakt-Anlass

Wettbewerb: Mitglieder werben neue Mitglieder

10.12.2009: Rückweisungsantrag zum Budget 2010 der SVP

16.12.2009: Durchhalteübung - Verkehrsdebatte - linke Schweizer Demokraten

Die wichtigsten Termine des Jahres 2009 auf einen Blick

SVP der Stadt Zürich
Parteisekretär Bruno Sidler
Postfach 6612
8050 Zürich

Werden Sie Mitglied der SVP Stadt Zürich

Screenshot of the compromised SVP page.[19]

Already immediately after the minaret ban initiative, more than 5000 sites were hacked, including sites run by the SVP local sections and the Young SVP. Most of these attacks were suspected of having been committed by perpetrators from Turkey. In this case, the attackers probably were from Germany or German-speaking Switzerland and participants in the CCC congress. The website was in any event listed as a target by the CCC. It is unknown, however, who exactly committed the attack. No criminal charges were filed.

Another case hit the headlines in January 2010. Because of a *cross-site scripting vulnerability* on the website of the Spanish EU presidency, www.eu2010.es, it was possible to infiltrate a picture of the comedian Rowan Atkinson (alias Mr. Bean) instead of the picture of Prime Minister Zapatero by clicking a prepared link.[20] This script inject, which uploaded

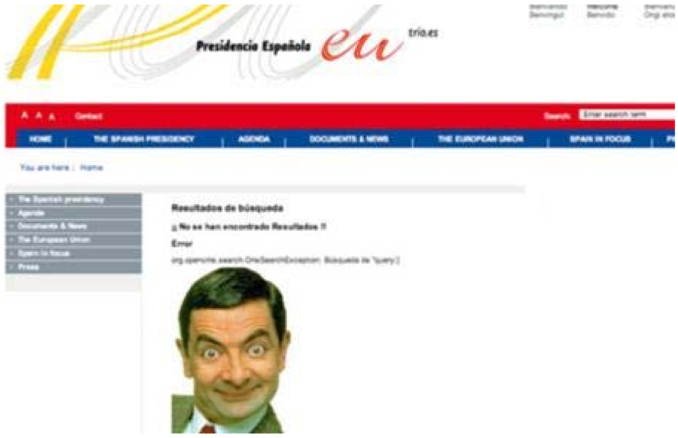
[17] http://www.bj.admin.ch/bj/de/home/themen/sicherheit/gesetzgebung/fernmeldeueberwachung.html (as of 27 August 2010)

[18] http://www.admin.ch/ch/d/sr/c780_1.html (as of 27 August 2010)

[19] Source: http://yfrog.com/j5svpp (as of 27 August 2010)

[20] http://www.la-moncloa.es/IDIOMAS/9/ActualidadHome/2009-2/04012010_AttackOnSpanishEuPresidencyWebsite_Communique.htm (as of 27 August 2010)

the Bean picture from another server, had apparently been smuggled in using the website's search function. The prepared link was then distributed via different channels. The defacement met with an overwhelming response, so that the website crashed temporarily due to the surge of curious visitors.



Resultados de búsqueda

¡ No se han encontrado Resultados !!

Error

org.opencms.search.CmsSearchException: Búsqueda de "query |

Screenshot after accessing the prepared link.

A cross-site scripting (XSS) attack does not attack the webserver as such. The webserver is only misused to smuggle foreign content into a website by way of the user's browser. The actual website is not modified. Usually, this method is used to steal login and credit card data by displaying a phishing site with a trustworthy web address. This defective function is caused by poor or missing verification of input fields. If, for instance, an interactive field fails to filter out the *HTML code* in the search function of a website, the code is interpreted by the browser on the result page. In this way, pictures but also entire forms, for example, can be smuggled in. XSS is one of the most frequent methods of attack on the web.

4 Current International ICT Infrastructure Situation

4.1 Selected espionage cases in the first half of 2010

Several espionage cases became known over the past half year, including against Google, Adobe, and also against the office of the Dalai Lama. In the most recent report on protection of the constitution, German Interior Minister Thomas de Maizière likewise warned of the growing threat of industrial espionage. Businesses and public authorities are particularly at risk. The German Federal Office for the Protection of the Constitution has classified the threat of industrial espionage in Germany originating in Russia and China as very serious.[21] The espionage cases that have surfaced should not be seen as independent and isolated cases, but rather attention should be paid to the similarities with respect to infrastructure, for instance. This will be discussed in more detail in Chapter 5.1.

4.1.1 Google reports cyber attacks

At the beginning of the year, Google announced that it had become the victim of targeted hacking attacks. Apparently, the case also affected other companies in the Internet, finance,

[21] German Report on Protection of the Constitution 2009:
http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2009/ (as of 27 August 2010)

and military fields. According to Google, the attacks took place in December 2009 and January 2010 and were launched against Google and at least twenty other companies. These hacker attacks were highly developed and targeted. In the case of the Google, the attacks primarily targeted Google Mail accounts. The focus was on the accounts of Chinese human rights activists. The hackers were unable to obtain sensitive data, however. In two cases, Google's research showed that the hacker had at least succeeded in displaying the inbox. The contents of the e-mails were not accessible, however. It was also noted that some Google Mail accounts of American, European and Chinese human rights activists had been spied on for quite some time. Access to these accounts had not been obtained using malicious software, however, but rather using *phishing* attacks against the account owners.

E-mails were also frequently sent to companies and public authorities using prepared *PDF files*. For instance, a Swiss company received targeted PDF documents infected with malicious code. In this case, a vulnerability was to be exploited which had been published already on 15 December 2009 but was not closed until the beginning of January 2010. It has been noted that, in contrast to previous cases where targeted hacker attacks often used Office documents as infection vectors, PDF files are now usually used.

Attacks of this kind have been known for a long time and frequently documented: see, for instance, "Tracking Ghostnet" of March 2009[22] or the Northrop study for the US-China Economic and Security Review Commission of October 2009 ("Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation")[23]. While the attack reported by Google was technically sophisticated, its complexity cannot be compared with other attacks such as the attack against the Swiss Federal Department of Foreign Affairs.

4.1.2 "Shadows in the Cloud": Chinese espionage network

On 6 April 2010, the groups "Information Warfare Monitor" and "Shadowserver Foundation" published a report titled "Shadows in the Cloud".[24] The report discusses espionage activities against Tibetan NGOs and the office of the Dalai Lama which were carried out using ICT resources. After "Tracking Ghostnet – Investigating a Cyber Espionage Network", this is the second report by these authors about possible Chinese espionage activities against targets of this kind.

Already in 2005, the New York Times published a report on an FBI operation named "Titan Rain". This case concerned infected computer systems of US authorities in which documents and information were skimmed over a extended period of time. China was named as a potential perpetrator. Also in Switzerland, such attacks have been carried out against the weapons industry and government offices. In these cases, attackers sent prepared documents with false senders to key persons in the enterprises in question. The messages were tailored to the recipients, which may indicate that intelligence services gathered information beforehand.

This report is a follow-up report to the GhostNet investigations. The researchers discovered that the computers infected by GhostNet also contained other malware. This led to the

[22] Tracking Ghostnet: http://www.tracking-ghost.net (as of 27 August 2010)

[23] Northrop study - http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (as of 27 August 2010)

[24] Shadows in the Cloud - http://shadows-in-the-cloud.net/ (as of 27 August 2010)

discovery of another espionage network. Victims in more than 36 countries were identified; most of the victims were in India. According to the report, 115 affected systems were discovered in Switzerland. Major enterprises and operators of critical information infrastructures were not affected.

4.1.3 The elite soldier's pretty Facebook friend

Social networks constitute a security risk for the armed forces of many countries. Soldiers communicate a wide range of information via Internet, thereby not infrequently providing useful clues to enemies. Awareness-raising campaigns are only imperfectly able to address this problem, and prohibitions are sometimes counterproductive.[25]
At the beginning of the year, an Israeli soldier announced the last operation of his unit before home leave on Facebook, mentioning the day and the West Bank village in question. As a consequence, the planned operation was cancelled and the solider was put on trial.[26]
Shortly thereafter, it turned out that an enchanting young woman had become friends with Israeli military officers on Facebook and elicited secrets from them. According to a press report, 200 elite soldiers fell into this trap.[27] The false profile was presumably a cover for the Lebanese Shi'a militia Hezbollah.

It can be speculated whether this story is true or only part of the army's major awareness-raising campaign[28]. On the other side, Israel is alleged to use the Internet and social networks to obtain information from its enemies.[29]

4.2 German conference of interior ministers plans measures against Internet crime

On 27 and 28 May 2010, the Standing Conference of Interior Ministers and Senators of the German States (IMK) met for its spring meeting. It chairman, Hamburg Interior Senator Ahlhaus, announced in the press before the meeting that the IMK planned to put together a comprehensive package of measures to counter the growing threat of criminals on the Internet. For this purpose, a central Internet office was envisaged to collect all findings from the federal government and the states. In addition to specialists from the security authorities, experts from the Internet industry would also be represented. In a second step, an equivalent international contact office would be created. Additionally, a requirement would be envisaged at the EU level for reporting hacker attacks, new types of viruses, and outbreaks of fraud on the Internet. As a preventive approach, the interior ministers also planned a broadly based

[25] http://news.bbc.co.uk/2/hi/8540236.stm; http://www.scmagazineus.com/army-ends-ban-on-facebook-flickr-other-social-media-sites/article/138392/; http://www.computerworld.com/s/article/9136255/Marines_solidify_ban_on_Facebook_Twitter; http://www.marinecorpstimes.com/news/2010/02/military_socialmedia_update_022610w/ (as of 27 August 2010)

[26] http://computer.t-online.de/israel-facebook-eintrag-verhindert-militaeraktion/id_40993294/index; http://www.sueddeutsche.de/digital/israel-dank-facebook-nachricht-im-militaergefaengnis-1.15999; http://news.bbc.co.uk/2/hi/middle_east/8549099.stm (as of 27 August 2010)

[27] http://www.blick.ch/news/ausland/soldaten-ueber-facebook-ausspioniert-147053; http://www.spiegel.de/politik/ausland/0,1518,694582,00.html (as of 27 August 2010)

[28] http://www.independent.co.uk/news/world/middle-east/israel-warns-of-facebook-spies-1687139.html; http://news.bbc.co.uk/2/hi/7343238.stm (as of 27 August 2010)

[29] http://www.theregister.co.uk/2010/04/07/facebook_spying_gaza/; http://news.bbc.co.uk/2/hi/middle_east/8585775.stm (as of 27 August 2010)

awareness-raising campaign about risks on the Internet. An action to this effect was already launched in Hamburg the end of April.
At the conference, the IMK agreed to review and, as appropriate, to implement the decision made by its competent working group on the report titled "Strategy for Combating Information and Communication Crime" and the steps initiated by the working group for implementing the recommendations for action contained in the report.

The threat emanating from the phenomenon of Internet crime is currently one of the main challenges in the field of combating and preventing crime. Since the approach generally pursued until now – namely improving cooperation of the individual regional and national police forces – has not achieved the desired successes, alternative paths are currently being reviewed. Internet crime does not stop at national borders, and the victims of an offence are frequently located in different countries. Efficient prosecution depends on extensive knowledge about the current situation, an overall view of the specific incidents, as well as coordination of the available resources. The EU Commission is also pushing in the same direction and is considering the creation of a police unit against Internet crime that would operate throughout Europe.
Through public-private partnerships, law enforcement authorities must work together with the private sector, Internet users, and victims' associations in order to compile precise status assessments, protect users, and prosecute criminals. Traditional police investigation and evidentiary methods are only imperfectly applicable in the field of Internet crime. Successfully combating Internet crime also requires prevention through sensitization and information of citizens, institutions, and organizations.

4.3 EC card problem or the 2010 bug

Ten years ago, the world waited anxiously to see whether computers would survive the change of millennium. The Y2K problem kept many software and hardware manufacturers in suspense – and in the end, nothing happened, and no problems occurred. Ten years later, another unexpected date problem has popped up: German cash machines and retail terminals had problems processing *EMV chips* starting 1 January 2010. Due to a programming error, the year 2010 could not be processed properly. According to estimates, about 30 million cards were affected. The French manufacturer Gemalto took the blame. In order for the cards to work again in the short term, the cash machines and payment terminals were reprogrammed so that the card readers would again only access the data stored on the magnetic strip. Since this reprogramming was not implemented abroad, inventive credit card users got the idea to cover up the chip with tape to force the card reader to fall back on the magnetic strip. However, this method also had the potential to destroy the card reader.

To prevent a costly exchange of the cards, the chip software was reprogrammed and repaired at cash machines and special card readers. For this purpose, the software on the card first has to be released using a secret key. This key is transmitted to the cash machine via a secure channel. Unlike magnetic strips, chips can be protected effectively against duplication, thus preventing skimming.

This approach was criticized, however, because neither the Federal Office for Information Security (BSI) nor the Federal Financial Supervisory Authority (BaFin) was consulted when solving the problem.[30]

[30] http://www.faz.net/s/Rub645F7F43865344D198A672E313F3D2C3/Doc~EB6DD9EEC40AA4E1FB4EB70152FD024D2~ATpl~Ecommon~Sspezial.html (as of 27 August 2010)

A significant characteristic of chip cards is that no subsequent modifications should in theory be possible once the software is stored on the card. Chip cards can be changed, but not without major effort. A key for reprogramming is provided for this purpose. Of course, this not only raises the question of appropriate encryption and security between the bank and the client, but also in general of who holds this key and what all can be done with the credit card if one possesses the key.

4.4 Mariposa

In 2009/2010 the Defence Intelligence group[31] discovered a botnet with one of the most extensive networks ever observed. A *sinkholing* conducted between December 2009 and February 2010 made it possible to detect 11 million unique IP addresses. The network was called "Mariposa" (Spanish for "butterfly"), since the botnet was created using the Butterfly malware kit. The Spanish name is due to the fact that the botnet operators were Spaniards.

The main purpose of the botnet was to steal sensitive data from infected computers. This included information about accounts, names of users, passwords, and details concerning online bank accounts. Part of the infected computers also included malware to launch *DDoS (distributed denial of service)* attacks. Clients of the 40 largest banks worldwide as well as computers of at least half of all Fortune 1000 companies were victims of this botnet. The victims came from 190 countries.

The Butterfly malware kit was developed by a hacker named Iserdo. The 23-year-old was recently arrested in the Slovenian city of Maribor[32]. The botnet operators were arrested in Spain the beginning of the year. The operation conducted by the Guardia Civil[33] led to the arrest of three Spanish citizens. These were identified by the pseudonyms they used on the Internet and their ages: Netkairo, 31, Johnny Loleante, 30, and Ostiator, 25.

However, the Spanish justice authorities had to follow their own country's criminal code. According to statements by Major Cesar Lorenzana[34], the deputy director of the technological crimes unit of the Guardia Civil, it is not a crime in Spain to operate a botnet or to disseminate malicious code. The only possible indictment would be for data theft.

As a marginal note: Two months after their arrest, two operators of Mariposa applied for a job at Panda Security, one of the members of the Mariposa Working Group. They found out that having "operator of a botnet" on their résumé is not necessarily the best precondition for getting a job.

4.5 Google inadvertently collects WLAN user data

During picture-taking drives for Google Street View, Google also recorded *WLAN* data in parallel. Google did not limit itself to the *MAC addresses* and *SSIDs* of the WLAN router, but also recorded user data transmitted by WLAN. User data includes general Internet traffic transmitted by and to wireless routers, but the data traffic must be unencrypted for that purpose. If this is the case, passwords can, for instance, be read off in clear text.

[31] http://defintel.com (as of 27 August 2010)

[32] http://www.theregister.co.uk/2010/07/28/mariposa_vxer_ciffed/ (as of 27 August 2010)

[33] A Mariposa Working Group was established in addition to the law enforcement authorities, consisting of Defence Intelligence, Panda Security, Neustar, Directi, the Georgia Tech Information Security Center and other researchers.

[34] http://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time/ (as of 27 August 2010)

A software developer at Google had integrated the recording of user data into the Street View recording software. This was a violation of the internal data protection rules of the company. The developer is now threatened with consequences. Additionally, the Hamburg Office of the Public Prosecutor initiated investigations against Google on 19 May 2010 on grounds of the data recording.

Beyond a doubt: Anyone operating a WLAN router must encrypt it sufficiently to ensure that no third parties can record data or misuse the router for criminal purposes. It makes no difference in this case that user data were collected systematically. But a company that has earned money with public and personal information has a special responsibility in this regard. In particular, open communication and clear guidelines for employees are necessary on how to deal with data.

Even with clear rules, the question will arise more frequently in future as to what is publicly accessible and what is private. This transition is increasingly fluid and no longer stops at one's garden fence. This will be debated no matter what – not just since Google Street View. Facebook, Twitter and co. are also factors in this debate. All of these services demand a high level of information competence from users, which they unfortunately do not always have (yet).

4.6 Single gang was responsible for two thirds of all phishing attacks

According to the most recent trimester report[35] of the Anti Phishing Working Group (APWG), 66% of all phishing attacks over the past six months were due to the Avalanche botnet. Avalanche is operated by one of the largest criminal groups engaged in phishing. Two thirds of all phishing sites registered in the second half of 2009 (84,250 of 126,697) were managed by this botnet.

Various security experts believe that the Avalanche botnet is run by the criminal gang Rock Phish. Both botnets use the same technique, such as regular registration of domain names, the use of *fast flux*, and the insertion of six websites per domain name. Avalanche was first discovered the end of 2008, just when Rock Phish had disappeared from the stage. According to the APWG report, Avalanche uses the same technique as Rock Phish, but in an improved and refined form.

4.7 Disruption of .de domain

On 12 May 2010, a *DNS breakdown* of the top-level domain at the German registration authority DENIC resulted in partial unavailability of .de websites. DENIC is the central registration authority for more than 13 million domains.[36] Top-level domains of other countries as well as domains such as .com and .net were not affected, but due to the dependencies of the various services, some failures also occurred outside of Germany. This is for instance the case if .com sites are resolved via .de DNS servers. According to speculations, the breakdown may have been due to the relocation of the registration service from Amsterdam to Frankfurt. When a DNS service breaks down, this not only affects surfing

[35] http://www.apwg.org/reports/apwg_report_Q4_2009.pdf (as of 27 August 2010)

[36] http://www.heise.de/netze/meldung/DNS-Fehler-legen-Domain-de-lahm-3-Update-999068.html (as of 27 August 2010)

on the World Wide Web; much more serious is the breakdown of the e-mail infrastructure, since e-mails are no longer able to reach their destination.

DNS servers play an important, if not the most important role, on the Internet. They constitute the link between IP addresses, which are understood by computers, and domain names, which can be memorized more easily by human beings. Criminals have also noticed this, which is why they launch efficient DDoS attacks directly against name servers, thereby making all websites resolved via this DNS server unavailable. There is currently no defence against such attacks. Another scenario is the manipulation of DNS queries, in which victims are for instance redirected to a manipulated server even though the web address is entered correctly. This is called DNS spoofing.

4.8 Introduced data retention rules violate German Basic Law

According to recent legislation, telecommunication service providers in Germany were required to store all information necessary to reconstruct who communicated or tried to communicate with whom and at what time, how long, and from where. Neither the content of the communication would be stored nor which Internet sites were accessed by the users. In its judgment of 2 March 2010 (1 BvR 256/08)[37], the Federal Constitutional Court of Germany (BVerfG) decided that the controversial provisions on *data retention*[38] as introduced violate the Basic Law (the German Constitution) and are therefore void.

According to the Federal Constitutional Court, the retention of data is not in principle unconstitutional – but it must be designed according to the principle of proportionality: an adequate limitation of the intended uses of the data must be carried out, and data security must be ensured by the entity storing the data. There must also be legal clarity concerning the transparency of data transmission and legal protection. The Court thus did not reject data retention as such, but rather criticized its implementation.

The retention of data without a specific occasion, allowing an IP address to be matched to a specific Internet connection owner, may indeed be constitutional. However, these data may also not be used without restrictions. The legislative power must regulate the rights of authorities to obtain information. The German Federal Government must now revise the legislation and introduce constitutionally compatible provisions.

In Switzerland, the norms concerning data retention and disclosure by telecommunication service providers are laid down in the Telecommunications Act[39], the Telecommunications Services Ordinance[40] and the Federal Law on the Surveillance of Postal and Telecommunications Traffic[41] and the associated ordinance[42]. The legislation concerning the surveillance of postal and telecommunications traffic is currently being revised.[43]

[37] http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html (as of 27 August 2010)

[38] §§ 113a and 113b TKG (Telecommunications Act) and § 100g StPO (Code of Criminal Procedure).

[39] FMG, SR 784.10: http://www.admin.ch/ch/d/sr/c784_10.html (as of 27 August 2010)

[40] FDV, SR 784.101.1: http://www.admin.ch/ch/d/sr/c784_101_1.html (as of 27 August 2010)

[41] BÜPF, SR 780.1: http://www.admin.ch/ch/d/sr/c780_1.html (as of 27 August 2010)

[42] VÜPF, SR 780.11: http://www.admin.ch/ch/d/sr/c780_11.html (as of 27 August 2010)

[43] http://www.bj.admin.ch/bj/de/home/themen/sicherheit/gesetzgebung/fernmeldeueberwachung.html (as of 27 August 2010)

4.9 Hacker attack against emissions trading / Access data of companies stolen

Trading in emissions certificates is an important tool for reducing the emission of pollutants. Using market-based regulation, national economies and individual companies are induced to gradually emit fewer pollutants arising for instance from the burning of fossil fuels: surplus emissions certificates not used by companies can be sold using a special trading system to companies that pollute the environment more than they are allowed.

On 2 February 2010, attackers used a simple phishing attack to obtain the access data of users of emissions trading authorities. The phishing e-mail was concealed as a message (warning of hacker attacks!) from the German Emissions Trading Authority (DEHSt), and recipients were asked to click on a link and re-register their user information and passwords.

The scammers sold the stolen pollution rights; as a consequence, the official register for emissions trading was crippled throughout much of Europe. The Swiss Emissions Trading Register of the Federal Office for the Environment (FOEN) warned its clients on its website.

What is striking about this attack is not such much the technical approach, but rather the target. Phishing attacks against financial service providers have practically died out in Switzerland. Nevertheless, this method is very popular among attackers, who predominantly operate in the North African region. Targets are unlimited, as long as they are only protected by login and password and can be used to make money. The main targets are credit card operators, e-mail providers, and auction platforms.

4.10 Microsoft announces reporting centre for stolen access data

In the first half of 2010, the software manufacturer Microsoft announced the creation of a reporting centre for identity and data theft. Thanks to the Internet Fraud Alert Center[44] under the direction of Microsoft, which is operated by the National Cyber-Forensics & Training Alliance[45], potential victims of data and identity theft such as financial and e-commerce institutions are to be brought together with researchers and government agencies. The goal is to facilitate the exchange of information about such offences in order to act quickly and efficiently. If, for instance, an Internet specialist finds stolen credit card numbers on the drop server of a botnet, he can now forward them to the Internet Fraud Alert Center, which would provide the information to the affected companies.

4.11 DNS servers hacked: Porn and adware hiding behind government domains

As reported by Sunbelt[46], members of the website FLVDirect managed to manipulate the

[44] https://www.ifraudalert.org/default.aspx (as of 27 August 2010)

[45] http://www.ncfta.net/main/home/ (as of 27 August 2010)

[46] http://sunbeltblog.blogspot.com/2010/07/flvdirect-affiliates-hacking-government.html (as of 27 August 2010)

domain name servers of several US government websites (.gov) so that their visitors[47] were redirected to FLVDirect adware and the pornographic website XXXBlackBook.com. The criminals also used new *subdomains* such as tubes-1911.empria-kansas.gov to redirect users.

5 Trends / Outlook

5.1 ICT-style espionage and data theft

Since the publication of the first MELANI semi-annual report in 2005, the theft of data has been a recurring topic. Unauthorized access to data is perpetrated for purely financial or criminal interests but also as part of state-sponsored espionage. The topic experienced a renaissance in the media with the attacks on Google and other ICT companies known as "Operation Aurora", which were discussed by the press and expert bodies in detail the end of 2009 and the beginning of 2010. This type of targeted, malware-assisted attack was given a *branding* in the ICT security community, culminating in the term "Advanced Persistent Threat (APT)". This was accompanied by several technical commentaries calling for a long-term response to such attacks used to gain information and data. This insight, which became widespread among ICT security companies by the end of 2009, is welcome, but it doesn't change anything about the fact that such espionage activities have been commonplace for years already.

Already in 2005, the New York Times published a report on an FBI operation named "Titan Rain". This case concerned infected computer systems of US authorities, in which documents and information were skimmed over an extended period of time. China was mentioned as a possible perpetrator. Whether this assessment is true or not, it is not the most pressing issue. Rather, it is important to realize that the perpetrators will not be satisfied with a single attack. Espionage is a long-term process which lives off of building up sources, exploiting them, and placing new ones again and again, not least of all when already existing information suppliers are discovered or replaced. This basic methodology of espionage also applies to the world of ICT.

An organization or state with the goal of obtaining classified information from another state or organization must, one way or another, build up the infrastructure and base of operations. The individuals managing the sources are only one part of the whole enterprise. The stolen documents must be reviewed, evaluated, and the sources must be told what kind of information will henceforth be needed and what other organizations or authorities are of interest. Such machinery also has the disadvantage, however, that certain processes, methods and resources can be changed only tediously, so that a similar basic pattern can often be observed when such actions are carried out. In the real world, this may concern the way sources are acquired, the way they are managed, or the physical on-site installations. Also in the world of ICT, in which no human source need be acquired per se and in which technology permits certain rapid adjustments and creativity, certain pieces of the overall infrastructure remain the same and can be identified along with the methods used.

What is standard practice in classical counter-espionage of every country and business, namely the linking of individual incidents in order to recognize similarities and assign the

[47] These websites include: yaceycountync.gov, uppersiouxcommunity-nsn.gov, woodfin-nc.gov, dumontnj.gov, emporia-kansas.gov

incidents to an overall cluster of cases, is rather seldom in the world of the Internet and ICT. This may have to do with the classical approach of ICT security, in which primarily an infected system or an individual incident has to be solved in order to ensure that operations are up and running again as quickly as possible. Linking such incidents together over a longer period of time into a single event happens only rarely or not at all. In terms of rapid reporting, these individual incidents – such as Aurora, GhostNet, Titan Rain, the FDFA incident, and so on – are presented in the media, but generally only as isolated, individual incidents of ICT-based espionage. But by taking a closer look, many of these incidents could be assigned to a small number of clusters of cases, which would provide information about who uses ICT for purposes of espionage and data theft, for what purposes, and where exactly. This permits more precise and balanced observation of the circles of perpetrators and therefore also an informed deployment of preventive resources, since the fundamental threat situation can be assessed more accurately. Distinguishing between untargeted criminal mass attacks and specifically adjusted, individualized attacks is often difficult for unpractised analysts.

At the level of the federal government and for the attention of the critical infrastructures in Switzerland, one of the mandates of the Reporting and Analysis Centre for Information Assurance (MELANI) is to undertake such an evaluation of individual incidents and, where possible, to generate an overall picture of such a cluster of cases. Also in other countries, the trend is moving in the direction of linking such ICT incidents together in order to more precisely define and recognize the organizations and structures behind them. Especially in the context of private enterprises subject to the latent threat of espionage, the establishment of capacities is advisable that go beyond classic incident-handing in the field of IT. Such capacities make it possible to provide bases for decision-making at a strategic level that are not limited to ICT, but rather concern the securing of information and data in general.

5.2 Expiry of Windows XP Update Service

In the first half-year, Microsoft announced the end of support for Windows XP SP2[48] (13 July 2010) and Windows Vista (13 April 2010) without a Service Pack. Windows XP has been on the market since October 2001 and is still the most widespread Windows version[49]. According to the statistics firm StatCounter, about 53% of users still work with Windows XP, while Windows 7 and Windows Vista each have about 20% market share. From now on, XP support is only offered to users with Service Pack 3. Microsoft plans to end all support for Windows XP in April 2014. According to Gartner[50], it should already be expected at the end of 2012 that new versions of many XP applications will no longer be supported.

As is the case for hardware, there is only a limited guarantee period for software, and also replacement parts are not available forever. Windows XP is so strongly established among businesses but also private individuals, so that a total and global replacement is not yet feasible. Considering how fast the development in the field of ICT has been over the past few years, this is astonishing. The end of XP will inevitably occur, however, and since especially businesses have to plan software changes far in advance and cannot undertake them from one day to the next, forethought is necessary to ensure that there is sufficient time for

[48] There is no Service Pack 3 for the 64-bit version of Windows XP. If you are running the 64-bit version of Windows XP with Service Pack 2, you are on the latest service pack and will continue to be eligible for support and receive updates until April 8, 2014. Source: http://windows.microsoft.com/en-us/windows/help/learn-how-to-install-windows-xp-service-pack-3-sp3 (as of 27 August 2010)

[49] http://support.microsoft.com/gp/lifesupsps (as of 27 August 2010)

[50] http://www.cio.de/knowledgecenter/pc-support/2236656/index1.html (as of 27 August 2010)

planning and testing. In the case of control devices, which are used for instance in industrial production, at universities and in hospitals, it may not always be possible to migrate to a new operating system in a timely manner, since software and control cards are tailored to the operating system and are sometimes also certified.

In addition to businesses, the situation of private users must also be considered. As a rule, private individuals do not change operating systems on the same computer, but rather old computers are replaced with new computers on which a (new) operating system is installed. The main thing here is that the system works smoothly. Why would anyone want to get rid of a smoothly functioning computer? The problem in this case is that, after the end of the life cycle, the critical security updates are no longer provided. This means that newly discovered vulnerabilities can no longer be fixed. Should Windows XP still have a disproportionately high market share in 2014, this could become a major problem.

An overview of the lifespan of individual Windows products is available here:

http://support.microsoft.com/gp/lifeselect

5.3 Goliath and David's data

Internet-supported devices (*smartphones, eBook readers*, etc.), social networks, and other Internet communication services make life easier and offer the advantage that their customers can connect more easily with each other and exchange information. By gathering statistical usage data, services can be improved and (free) services can be paid for by increasingly targeted advertisement. For this reason, the suppliers of such applications want to gather as much information as possible about their users. Users wanting to protect their privacy must often wade through pages and pages of complicated data protection settings, often without understanding what configurations lead to what consequences. Moreover, new possibilities for linking and evaluating data collections are always being developed. Even if one consciously chooses what data to make available to Internet service providers, it is easy to lose control over what happens with them. Only in the rarest cases are data collection, processing and use transparent. A dataset compiled for a particular purpose today may be linked with new data tomorrow, giving rise to completely new, unexpected statements. Since there is freedom of contract in Switzerland, providers and buyers/users can in principle – within the framework of the legal order – agree anything, since no one is forced to buy a particular product or make use of a particular service. Changes to the terms and conditions or the privacy policy may, however, typically be changed unilaterally by the provider without considering the customer. Anyone who does not agree with the new terms usually only has the option of cancelling the service in question or no longer using the product. It appears questionable, however, whether someone who by now administers his or her contacts almost exclusively through social networks will be able and willing to say goodbye to that service, or whether someone will give back their beloved smartphone simply because the provider reserves extensive rights to collect, process and forward data. Many people do not even bother to read the pages and pages of complex terms and conditions. Typically, one just wants to use a product or service, not spend hours reading boring texts and grappling with complicated configurations. Most people think:
"Whatever is in the terms and conditions is probably okay, and the basic configuration can't be too bad." Users must take responsibility for themselves, however, and keep up to date. Most of all, this means reading the small print and making sure whether one really wants to divulge certain information. Users must act with the awareness that very extensive personality profiles can be prepared with the help of their data – they "pay for" (free) services with their personal data that they supply in return. And the providers of such services generate their income with advertising. This income rises the more people use such services, and the more targeted the analysis of the users' needs is. The business models are based on

the idea that users are willing to make information available if they receive a useful product in return that makes their life easier: staying in contact easily with friends, finding the right recipe for dinner or a good restaurant in the neighbourhood, or receiving interesting offers from stores during a walk through the city. In their search for as many new users and advertising options as possible, providers constantly make new applications available.

It should also be considered that one frequently also disseminates data from third parties: An online address book contains detailed contact information, and also in non-public albums photographs of friends and acquaintances are made available to the provider. In this connection, it should be noted that face recognition software is becoming better all that time, and that several smartphones with a *GPS* function mark every photograph with a "geotag", which pinpoints the exact location where the photograph was made. This opens up possibilities that even just a little while ago, one hardly would have imagined when uploading pictures. Location-based services, which allow one to notify friends of one's current location,[51] certainly have indisputable benefits, but they also harbour dangers which in the best case might lead to slight inconveniences – and in a worse case to a break-in at home (since one is apparently not there).[52]

The most important suppliers of social networks and similar services today are most frequently from the United States, where there are usually no generally valid data protection rules. As a rule, the generally stricter data protection requirements in European countries are ignored, to the detriment of the rights of citizens and the competitiveness of European providers with similar services. It is to be hoped that with the increased sensitization of clients to the treatment of personal data, the market will play in favour of data-protection-friendly products and services.

5.4 Web services – Fundamental problems for the legislator

Technological and social developments constantly create new possibilities and new risks. If, as a consequence of these changes, problems arise, there is often a call for new laws. Politicians and private individuals are under the illusion that they can use legislation to prohibit Street View, control Facebook, or make disliked content on the Internet inaccessible. Even if such measures are in principle conceivable, the question of proportionality arises with respect to the implementation and enforcement of new law. Over-regulation can inhibit the economy and may limit legitimated uses for users. A prohibition backed up by sanctions is only effective if it can and will be enforced.

Laws should be technology-neutral and formulated in a general-abstract way. Even measures enacted by a regulator should take into account that a too narrow formulation may leave out potential future developments,[53] while too general rules may provide too much leeway and perhaps too little legal certainty. It is problematic when specific offers or services are treated separately and laws are enacted because of specific applications: Google Street

[51] For instance GPS-based services such as Foursquare, Gowalla, Facebook Places or Google Latitude – but locations are also often communicated via Twitter tweets or Facebook status updates.

[52] http://pleaserobme.com/ (as of 27 August 2010)

[53] This happened with the Ordinance of 31 October 2001 on the Surveillance of Postal and Telecommunications Traffic (VÜPF, SR 780.11: http://www.admin.ch/ch/d/sr/c780_11.html), according to which only access providers must be able to monitor the e-mail box of their clients – pure e-mail service providers do not appear to be covered. This may be due to the fact that at the time, e-mail accounts were primarily offered by access providers and pure e-mail services were hardly known in Switzerland.

View is not the only service offering pictures of streets, and Facebook is not the only social network. Neither a Street View law nor a Facebook regulation would cover all equivalent services – and would likely not be enforceable.

As a rule, law follows the principle of territoriality. Swiss rules are not necessarily applicable to fact patterns on the Internet. As soon as a foreign company is involved, for instance, it must first be reviewed whether Swiss law applies, a Swiss authority is competent, and how any decisions might be enforced. If, for instance, an American social network were to commit serious violations of data protection provisions under Swiss law, but US law is not violated, then the Swiss consumer likely has no means to defend himself or herself.

The legislative power may well require providers of legal infrastructure[54] and lawful services[55] to control and filter all content and to thoroughly check all clients before engaging in a business relationship in order to protect Swiss consumers on a preventive basis. But to do so, a censorship apparatus like in a totalitarian state would have to be built up, and all measures would have to be paid for with higher prices – only to find out that the Swiss business location ultimately has become massively less attractive and that the envisaged protection of the incapacitated consumer is still lacking. Far more efficient would be clear processes for how to counter identified abuses and for employing the proper resources for that purpose.[56]

In this connection a parliamentary motion is of note[57], the purpose of which is to ban commercial pornographic services on mobile telephones (according to the title of the motion – the text generally refers to "telecommunication devices"[58]) on grounds of youth protection. As an alternative, the motion proposes "to require providers of basic supply services to block all connections to commercial premium rate services with erotic or pornographic content for persons under the age of 16 and to require providers of premium rate services not to let persons under the age of 16 access erotic or pornographic content" – even though the existing legal situation[59] already makes it punishable to provide, show, give or make available pornography to persons under the age of 16, regardless of whether free or not, online or offline. Particularly in the special case of pornography, a company would make itself criminally liable right from the moment when it gains knowledge of the facts and fails to curtail access. In the case of other offences, however, companies brokering services may not be punishable. So what is in need of clarification is the time from which a pure brokering company[60] can be assigned what kind of responsibility, given that such companies typically cannot be assumed to know what kind of content is being brokered and transmitted.

Even data retention, which recently has been debated fiercely in Germany, is an interesting example to illustrate the problem for the legislative power: civil rights advocates cite data protection and general suspicion, while the police and victims' organizations want tools to breach anonymity and often see data protection as protection of the perpetrator. Here again, the goal must be to find a healthy balance between various interests and to identify a practicable solution. While even the regulation criticized by the Federal Constitutional Court

[54] E.g. access providers.

[55] E.g. companies using short SMS numbers to broker services.

[56] Such as blocking short SMS numbers of domain names, see Chapter 3.5.

[57] http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20063884 (as of 27 August 2010)

[58] This formulation also includes the Internet. – But it is probably not the intent of the parliamentarian submitting the motion that only (but at least) free pornography should be allowed on the Internet.

[59] Article 197 paragraph 1 of the Criminal Code (StGB, SR 311.0): http://www.admin.ch/ch/d/sr/311_0/a197.html (as of 27 August 2010)

[60] Internet access providers, telecom companies, holders and lessees of SMS premium rate numbers, operators of online payment systems, etc.

of Germany[61] did not permit the recording of websites visited by a user, precisely these data may be decisive for identifying mobile Internet users (given that several people often share the same address)[62], since the traditional method (IP address and time) cannot be used to conclusively identify which participant was up to no good in a particular chat room at a given time.

Especially in the context of information and communication infrastructures, it is often very difficult to close in on the circle of perpetrators or to clearly determine the location of the perpetrators. The Internet as a means to a criminal end is inherently global, and even a distinction between public and private actors is often impossible. For this reason, legislation often attempts to control or punish preparatory acts. However, this approach often fails in the field of ICT given the fact that the tools employed are almost always dual-use resources, i.e. they can be used either for harm or for protection. Considering the principle of proportionality, such approaches may inhibit the legitimate and innovative use of new technologies. In the end, the use of available technologies is the same everyone, and only intent distinguishes between abuse and no abuse. The project on ratification of the Cybercrime Convention tries to do justice to this fact.[63]

[61] See Chapter 4.8

[62] See Chapter 3.10

[63] See Chapter 3.6

6 Glossary

This glossary contains all terms in *italics* in this semi-annual report. A more detailed glossary with more terms can be found at:
http://www.melani.admin.ch/glossar/index.html?lang=de.

Active scripting	Technology developed by Microsoft to download small applications, so-called ActiveX controls, to the client's computer from where they run when web pages are viewed. They enable different effects and functions to be carried out. Unfortunately this technology is often abused and represents a security risk. For example, dialers are downloaded through ActiveX to the computer and run. ActiveX problems only concern Internet Explorer because the other browsers do not support this technology.
Ad server	Ad servers are used to measure the success of Internet advertisements. Both the physical server on which the ad server software is running as well as the software itself can be referred to as the ad server.
Botnet	A collection of computers infected with malicious bots. These can be fully remotely controlled by the attacker (the owner of the botnet). Depending on its size, a botnet may consist of several hundred to millions of compromised computers.
Browser	Computer programmes mainly used to display Web content. The best-known browsers are Internet Explorer, Netscape, Opera, Firefox und Safari.
Command & control server	Most bots can be monitored by a botmaster and receive commands via a communication channel. This channel is called command & control server.
Content management system (CMS)	A content management system (CMS) is a system that makes possible and organizes the joint preparation and processing of content, consisting of text and multimedia documents, generally for the World Wide Web. An author may operate such a system even without programming or HTML knowledge. The information to be displayed is referred to as "content".
Cross-site scripting	Cross-site scripting (XSS) refers to the exploitation of a computer vulnerability in web applications by taking information from a context in which it is not trustworthy and putting it into another context in which it is considered trustworthy.
DDoS	Distributed denial of service attacks A DoS attack where the victim is simultaneously attacked by many different systems.
DNS	Domain Name System .With the help of DNS the internet and its services can be utilised in a user-friendly way, because

	users can utilise names instead of IP addresses (e.g. www.melani.admin.ch).
Dual use	Dual use is a term otherwise used in export controls and refers to the potential uses of an economic good in principle.
eBook reader	An e-book reader is a portable device for reading electronically stored books (e-books).
Electronic signature	An electronic signature is data linked with electronic information used to identify the signer or the creator of the signature and to verify the integrity of the signed electronic information.
EMV chip	The abbreviation EMV refers to a specification for payment cards furnished with a processor chip. The letters EMV stand for the three companies that jointly developed the standard: Europay International (now MasterCard Europe), MasterCard, and VISA.
Fast flux	Fast flux is a DNS technique used by botnets to conceal phishing or malware-spreading sites by distributing them among different hosts. If a computer fails, the next computer steps into the breach.
Financial Agent	A financial agent works as a legal money broker and thus engages in financial transfers. Recently, this term has been used in connection with illegal financial transactions.
FTP	File Transfer Protocol FTP is a network protocol for transferring data via TCP/IP networks. FTP can be used, for instance, to load websites onto a webserver.
Full disclosure	Full disclosure of details concerning a vulnerability.
Protected mode	The protected mode, for instance in Internet Explorer, is a feature that makes it more difficult to install malicious software on a computer.
GPS	Global Positioning System (GPS), officially NAVSTAR GPS, is a global navigation system for determining position and measuring time.
Host	This was used and is still used in IT to refer mainly to computers with vast computing power (banking). Today, however, this also refers to smaller computer systems (computers of private users, web servers etc.).
HTML code	HyperText Markup Language Pages for the World Wide Web are written in HTML. This allows to determine the properties of the web page (e.g. page representation, links to other sites, etc.). Because HTML is made up of ASCII characters, a HTML page can be edited using a normal word processing programme.

IP address	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
ISM band	ISM bands (Industrial, Scientific and Medical bands) refer to frequency bands that can be used by high frequency devices in industry, science, medicine, at home and for similar applications. ISM devices such as microwave ovens and medical appliances for short wave radiation require only a general license.
Critical infrastructure	Important component in national security policies and defence planning. Generic term to describe concepts and strategies to protect critical infrastructures / critical information infrastructures.
MAC address	Media Access Control Unique and globally identifiable hardware address of a network adapter. The MAC address is written in the ROM of the adapter by the respective manufacturer (e.g. 00:0d:93:ff:fe:a1:96:72).
Man-in-the-middle/man-in-the-browser attack	Man-in-the-middle attacks (MITM) Attacks in which the attacker infiltrates unnoticed the communication channel between two partners and is thereby able to spy on or even modify their data exchanges.
Name server	A name server is a server offering name resolution. Name resolution is the process allowing the names of computers and services to be resolved into an address that can be processed by computers. See also Domain Name System (DNS).
Patch	Software which replaces the faulty part of a programme with a fault-free version. Patches are used to eliminate security holes. See also Hotfix.
PDF file	The Portable Document Format (PDF) is a platform-independent file format for documents developed by Adobe Systems and published in 1993.
Phishing	Fraudsters phish in order to gain confidential data from unsuspecting Internet users. This may, for example, be account information from online auctioneers (e.g. eBay) or access data for Internet banking. The fraudsters take advantage of their victim's good faith and helpfulness by sending them e-mails with false sender addresses.
PIN code	A Personal Identification Number (PIN) or secret code is a number known only to one or just a few persons for authenticating themselves to a machine.
Port	A port is part of an address that assigns data segments to a network protocol. This concept is provided in TCP, UDP and SCTP, for instance, in order to address protocols at the higher layers of the OSI model.

Source code	In computer science, source text (or source code) refers to the text of a computer programme written in a programming language that humans can read.
Reasonable disclosure	Reasonable disclosure of the details of a vulnerability, ideally in a form that helps users take countermeasures, but does not help criminals exploit the vulnerability.
Vulnerability	A loophole or bug in hardware or software through which attackers can access a system.
Sinkhole	Method for redirecting botnets to a specific command & control server to which one has access, in order to gather as much information as possible about the infected systems.
Smartphone	A smartphone is a powerful mobile phone that expands the functionality of a mobile phone by that of a personal digital assistance (PDA).
Social engineering	Social engineering attacks take advantage of people's helpfulness, credulity or lack of self confidence in order to gain access to confidential data or to prompt them to perform certain actions, for example.
Social networks	Websites for communication among users by means of personally designed profiles. Often, personal data such as names, dates of birth, images, professional interests, and hobbies are disclosed.
SSID	Service Set Identifier Identifies the WLAN network names. All WLAN access points and end devices must use the same SSID in order to communicate with each other.
Subdomain	A subdomain is a domain below another domain in the hierarchy.
Token	Hardware components, which provide an authentication factor (cf. two-factor authentication) e.g. smartcards, USB tokens, SecureID, etc.).
Shortcut icons	Shortcut icons are small symbols that open the desired programme when clicked on.
Virus	A self-replicating computer program with harmful functions that attaches itself to a host program or host file in order to spread.
Data retention	Retention of data over a certain period of time that are necessary to reconstruct who communicated or tried to communicate with whom and at what time, how long, and from where.
Website infection	Infection of a computer with malware simply by visiting a website. Often the websites concerned contain reputable offerings and have already been compromised beforehand for the purposes of spreading the malware. The infection

	occurs mostly by trying out exploits for vulnerabilities not yet patched by the visitor.
Wireless (WLAN)	WLAN stands for Wireless Local Area Network.
Workaround	A workaround is a way to bypass a known problem within a technical system by way of an auxiliary construction. It is a temporary solution that does not remedy the actual source of the error.
Digital certificate	A digital certificate consists of structured data used to confirm the owners and other properties of a public key.