Chapter 2
Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet

Dr. Phillip W. Brunst

2.1 Introduction

Although it is known that terrorists already routinely use the Internet for purposes such as spreading propaganda or conducting internal communication, the threat that results from this use is heavily debated. Especially the question whether a cyber terrorist attack is imminent or if it is only a purely fictitious scenario is subject to many discussions. One reason for these differences in opinion is a lack of exact terminology. Already for the term "terrorism", more than 100 different definitions with more than 20 definitional elements have been identified (for further details, see Record 2003). The addition of "cyber" to this word already fraught with meanings does not help to clarify this issue. Consequently, current interpretations of "cyber-terrorism" range from very narrow to very broad. A more narrow view is often worded close to common terrorism definitions and might include only politically motivated attacks against information systems and only if they result in violence against noncombatant targets (Pollitt 1998). Broader approaches often include other forms of terrorist use of the Internet and therefore might define cyberterrorism as almost any use of information technology by terrorists (National Conference of State Legislatures 2002). To complicate matters even more, additional terminology is being introduced into the discussion, e.g. "digital Pearl Harbor", "electronic Waterloo", "Cyber war", or "electronic Chernobyl". These terms, however, focus mainly on the effects of possible future attacks by terrorists. Therefore, they rather cloud the discussion about a precise terminology on cyberterrorism or a terrorist use of the Internet.

This chapter is divided into three parts that depict the problematic areas that are currently under discussion. Part one will deal with what is usually considered as "real" cyberterrorism: attacks that are carried out via the Internet and that are aimed either at other IT systems or at real-world property and human lives. Part two will then cover issues that might not be considered as cyber terrorism in a narrow sense,

Dr. P.W. Brunst (✉)
Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany
e-mail: phillip@brunst.de

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_2, © Springer Science+Business Media, LLC 2010

but rather a use of the Internet for terrorist purposes. Finally, part three will cover uses of the Internet that might commonly be regarded as conventional or even harmless. A look in more detail will reveal, however, that even the everyday use of the Internet can offer some specific advantages for terrorists.

This chapter will not go into further details of the problems of defining cyberterrorism or a terrorist use of the Internet. Instead, it will give – as outlined above – an assessment of the risks and thus the threat of terrorists who can use the Internet for their purposes. The underlying term "terrorism" is for this reason understood in a broad sense to allow an expanded view of the risks and chances.

Furthermore, to allow a realistic risk analysis, it is not sufficient to look only at cases of terrorist involvement that have officially been confirmed. Often, the facts of such cases will be kept confidential, e.g. because they affect issues of national security. Therefore, this analysis is based on cybercrime and cyberterrorism literature as well as on specialized security reports, case studies, and news reports. Only such a broad approach allows the inclusion of occurrences of the past and also gives consideration to possible future threats.

2.2 Attacks via the Internet

Attacks that are launched over the Internet are commonly known as integral parts of what is commonly called "cyber crime". Formerly, perpetrators in this area were often young hackers, keen on experimenting with security-related issues and curious about technology. In the meantime, however, this situation has changed. Instead of experimenting youngsters, highly organized groups that use attacks as a source of income, businesses that conduct industrial espionage, and states engaging in electronic warfare can be observed. The only group of actors that seem to be missing are the terrorists who rarely admit to computer-related aggression. Nevertheless, this is no reason for an all-clear. The events in Estonia in 2007, for example, have shown that even whole countries can be put at risk without the use of a single conventional weapon.[1] This will not go unnoticed by terrorists. A more thorough look at the motivation of terrorists for attacks over the Internet is therefore of the essence (Sect. 2.2.1) before looking at the concrete possibilities for terrorist attacks (Sect. 2.2.2).

2.2.1 Motivation

Some authors claim that, to date, not a single instance of cyberterrorism has been recorded (Sieber 2004). According to informal sources, however, many attacks have

[1]See the section " Denial-of-Service Attacks" for further details on the Estonian case.

already taken place, but are kept confidential due to the security threat to important infrastructures that would evolve from details becoming publicly known. Whatever the case may be, it is undeniable that the threat of terrorist action over the Internet is realistic. Already this fact can (and is) abused by terrorists as a form of psychological warfare: cyber-fear is generated by the fact that what a computer attack *could* do is too often associated with what *will* actually happen (Weimann 2006).

2.2.1.1 General Motivation

Beyond the potential for psychological warfare, five main issues are relevant for a general motivation to commit crimes over the Internet:

Location Independence

Attacks in the Internet are not bound to a definite physical place. Although it is necessary to visit the locality of a conventional attack, e.g. to "case" the target or place the bomb, cyber terrorists do not have to be physically present at the place of their deed. This is a great advantage over conventional attacks where the danger of being suspected during the preparation phase or even detected immediately before the commitment of the crime is omnipresent. For any cyber crime, it is sufficient to be connected to the Internet from any place on earth. This can be a static connection, e.g. at home or at an internet café, or a mobile connection, e.g. over a cellular telephone.

Often, it is assumed that many countries that host terrorist groups are not well enough equipped with Internet connections to pose a real threat. However, this is true only with regard to the current status. The Internet penetration rates of North America, Australia, or Europe are still clearly above those of Africa, for example (Miniwatts Marketing Group 2007). The increase of Internet users within the last years, however, was extremely fast, in some countries, even close to 5,000% within the last 7 years (Miniwatts Marketing Group 2007). Especially the number of Internet cafés that can be used for rates affordable even to the poor has rapidly increased in most major cities during the last years. This allows large parts of the population (and the terrorists among them as well) to access the Internet without any further control.

Speed

Attackers are hardly dependent on their own connection speed for attacks that are launched over the Internet. Instead, they can use the bandwidth and speed of third parties, e.g. to launch distributed denial-of-service (DDoS) attacks.[2] The party's

[2]DDoS attacks are a way to hinder the accessibility of computer systems. For further details, see below.

own connection speed is needed only to distribute commands to the systems attached or to receive feedback about the successes. In both cases, even slow, low-bandwidth connections are sufficient.

The aspect of independency is true also for those attacks that act without human interaction, e.g. viruses or worms. These programs – once released by their creators – act on their own. The speed of their spreading is determined solely by the connection speed of the victims that help them to spread. This could be observed, for example, by the speed in which the Sapphire-, the Melissa-, or the I-Love-You-Worms spread during 1999 and 2003. None of them was dependent on the link-up of their creators.

Finally, the possibility to create and test malicious computer programs can be used to prepare action for future events. This makes it possible to react in a seemingly spontaneous manner to incidents, even though the preparation took place long before ("cyber revenge").

Anonymity

The anonymity of perpetrators is often alleged as a core feature of Internet-based communication. It is necessary to remember, however, that an IP address at least is transmitted with every step taken on the Internet. This can be used to get evidence of the person who initiated certain actions over the Internet. In many cybercrime cases, this can successfully be used to arrest the real perpetrator who thought that just by using the Internet he would remain anonymous.

Technologically knowledgeable people, however, have ways of hiding their identity and camouflaging their trail to an extent that makes a prosecution hard or – in some cases – impossible (Brunst 2009). The IP address of a user of an Internet café, for example, is transmitted as it is in any other case. If the owner of the establishment is not obliged or fails to register their users, however, the lead will end at the Internet Café without any further possibility to identify the culprit. Similar problems arise with wireless networks (WLAN) that – if not especially protected by the possessor – can be used to access the Internet by almost anybody within the range of the access point.

Apart from these purely organizational means, a number of additional – more technical ways – of hiding the identity on the Internet can be used. Perpetrators, for example, use proxy servers, anonymity networks, or they simply route their traffic over hacked computers of innocent users. In any of these cases, the trace cannot be followed to the computer of the perpetrator, who then cannot normally be identified either.

Internationality

The Internet connects countries regardless of their physical borders or diplomatic or political relations. Nation states, however, are still acting according to their national sovereignty, not as an operator or supervisor of a globally active network. This is

actively being taken advantage of by criminals. The aspect of internationality therefore has to be seen in close context with the anonymity and independency of place.

Examples of this technique are manifold. Especially in the area of controversial contents, it can be observed that perpetrators actively seek countries with more liberal free-speech laws to host their contents. Because content that is made available on the Internet, e.g. on the World Wide Web, is accessible from all over the world, the physical places of someone offering information and of a person accessing these data can easily differ. Other examples concern attacks that are routed through different computers to hide the traces. Often, the routing is deliberately chosen to pass through countries that do not cooperate either in criminal matters or at least in cybercrime matters. Alternatively, the routing can pass through countries where it is known that the technical capabilities of investigating cybercrime are not developed far enough to successfully gather evidence – a particular problem when considering internationally operating terrorists.

Cost-Benefit Ratio

When choosing targets and weapons, terrorists are often bound to a rigorous cost-benefit analysis of their own definition. Actions that bear a great risk of being detected too early or that will not achieve high visibility (and therefore fear in the population) have to be disregarded in favour of more "efficient" instruments (Giacomello 2004). Attacks committed over the Internet – at least in general – have an extremely positive cost-benefit ratio.

On the one hand, such attacks require only minimal initial investment. Computers are cheap and nowadays, in many areas of the world, are already part of daily life. Furthermore, an up-to-date computer model is not required. Because speed does not play an important role (as shown above) a computer of the last product line or even the generation before will be sufficient. Even some of the newer mobile phones can be used for simple Internet access. If these options are – for any reason – not available, Internet cafés that are found in any major city can also be used to cheaply access the Internet. The information that is needed to find relevant security holes and technical possibilities for exploitation is also available cost free.

On the other hand, even small attacks against targets lead to high costs for their owners. Constant updating, state-of-the-art equipment, and permanent monitoring is required to protect systems even against the so-called script kiddies.[3] Therefore, costs for personnel, machinery, and software constantly put pressure on the owners of publicly accessible computer services.[4] The Internet can therefore be seen as

[3]"Script Kiddies" is a term commonly used to describe people who do not possess the knowledge to build attacking software by themselves and who therefore have to rely on "ready-to-use" construction kits. Successful attacks by script kiddies are thus often only possible against very poorly protected targets.

[4]The White House, for example, has just allocated a sum of 6 billion US dollars for the strengthening of its systems against cyber attacks (Johnson 2008).

a form of "force multiplier". This military term means that the striking power potential of a unit is increased without increasing the personnel at the same time (White 1990). Especially for smaller terrorist groups this is true, because the Internet allows them to create harm much larger than possible with their conventional capabilities. Furthermore, the Internet can be used by them to create the illusion of greater size and power as well as having more followers than is truly the case. This, in turn, will lead their opponents to defensive measures that are far-reaching (and therefore, again, more costly) then objectively necessary.

Specific Terrorist Motivation

These five main areas of motivation are valid for terrorists as well as for ordinary cyber criminals. Differences can, however, be observed with regard to the underlying agenda (Brunst 2008). Terrorists aim primarily at the generation of fear, the creation of economic confusion, or a discrimination of the political opponent. Apart from these main motives, the generation of monetary income or the gathering of information (either for conventional or for electronic attacks) can also be objectives. To conduct actions over the Internet is only one way to achieve these goals.

The problematic issue relating to the terrorist intention behind action on the Internet is, however, that it is often undetectable. If, for example, a hacking attack with the aim of shutting down important systems at an airport is successful, terrorists will probably have an interest in making this publicly known to arouse fear in the population. In this case, it is easy to determine terrorists because the source of a cybercrime act and also the underlying agenda is clear. If, however, a hacking attack is committed in the hope of gaining information on the automobile route of an important person, this might be kept secret so as not to endanger future plans for a bomb assassination of that person (Brunst 2008). In this case, it is unknown that the act was committed by terrorists. Additionally, even if this fact would emerge, the specific intention of the perpetrators, i.e. *why* the hacking attack occurred (e.g. test of technical capabilities, preparation of conventional attack or allotted victim), would still be unknown. Therefore, from a purely objective perspective, in many cases the distinction between ordinary cybercrime and cyberterrorism is hard to make.

2.2.2 Attacks

Any attack with a computer – maybe with the unlikely exception of physical attacks with computer hardware – is aimed at another computer system. However, with respect to the terrorist intention and the outcome of cyber attacks, a distinction should be made between attacks that are actually aimed "only" at other computer systems and those that are intended to harm human lives.

2.2.2.1 Attacks Aimed at Other IT Systems

Attacks that are aimed at other IT systems can serve different intentions. Often, a first aim will be to get access to the computer system. This can be achieved either with technical means or with the help of deceiving users and administrators (see the following section on "Illegal Access"). If such an attack is successful, data that is stored or otherwise handled through this computer can be changed (see the section "Data Alteration") or secretly copied from the machine (see the section "Data Espionage"). In many cases, however, terrorists will not even try to gain access to the computer. Instead, it might be sufficient – as with a conventional attack – to hinder the system from functioning correctly. The use of either denial-of-service (DoS) attacks (see the section "Denial-of-Service Attacks") or even conventional attacks on computer infrastructure (see the section "Conventional Attacks on IT Infrastructure") can be a successful means to achieve these goals. Finally, a combination of classic conventional and new electronic attacks is regarded as a main threat by many experts (see the section "Hybrid Attacks").

Illegal Access ("Hacking")

Hacking, i.e. the illegal access to computer systems and data, is the scenario where problems, action, and results of terrorists and other cyber criminals probably differs the least. In general, a differentiation between illegal access by only technical means and access with human help can be made. An example of purely technical access would be the use of a computer program that uses software flaws that have been identified to gain access to a system (so-called exploit). Some exploits have already been available for a long time and will work only if a system administrator was not able to keep their computer up-to-date. Other exploits, however, are not known to the public or even the software manufacturers. These "zero-day exploits" or "less than zero-day exploits" can be acquired on the black market and will give access to systems, even if the administrator installed all possible security fixes that were available from the software company that developed the product (Wilson 2005).

The second category refers to access with human help. This can be achieved, for example, in the form of so-called social engineering, i.e. deceiving the user to give passwords or other protected information. Other ways to gain access with human help include the infiltration of dedicated personnel or the bribing of existing staff members. In general, the choice of the right technique (or a combination thereof) depends on the individual circumstances. Therefore, successful attacks against protected targets often require technical and social skills.

According to a study of the *Center for the Study of Terrorism and Irregular Warfare*, the capabilities that are needed for successful attacks can be divided into three groups (Nelson et al. 1999):

- "*Simple – unstructured*: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control or learning capability.

- *Advanced – structured*: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis capability and command and control structure for sequential attacks from a single location. Some learning ability – can assimilate some new technologies and train personnel.
- *Complex – coordinated*: The capability for coordinated attacks capable of causing mass-disruption. Ability to analyse vulnerabilities, penetrate integrated, heterogeneous defences (including cryptography) and create attack tools. Strong ability to conduct target analysis and high confidence in results. Strong command and control structure capable of employing multiple, simultaneous attacks from different locations. Strong organizational learning capacity – can keep up with latest technology, train personnel, diffuse knowledge throughout the organization, make necessary doctrinal and organizational changes to enhance capabilities".

Already attacks of the lowest level, i.e. "simple – unstructured" can – under some circumstances – be sufficient to successfully gain access to a computer system. However, these forms of attack will only work if it is sufficient to attack *any* system. In this case, a computer system can be sought that is vulnerable to a certain form of attack, e.g. where a certain version of a software product is installed. If it is necessary to attack a *given* target, however, the efforts to successfully attack are incomparably higher. In this case, it might be necessary to acquire certain specialized tools, like the above-mentioned "zero-day exploits".

Attacks of the highest level, i.e. "complex – coordinated", will require a high degree of innovation and technical effort. In exchange, they allow access even to systems that are extraordinary well protected. An example for a successful combination of *social engineering* and an individually developed malicious program was shown in the year 2006 by a security company. To gain access to the systems of their client (who hired them to test their computer security), the company prepared USB sticks with a custom-designed, newly developed Trojan horse program that could not be detected by virus scanners. Twenty of these sticks were "lost" on the premises of the client. Of these, 15 sticks were found by employees – and promptly connected to the company network where the Trojan started to collect passwords and other valuable information and e-mailed this data back to the offenders (Weimann 2005). Of course, such an attack would be a powerful way for a terrorist organization to initiate counterespionage.

The assessment as to what extent hacking terrorists are realistic threats differs immensely. In many countries the information about actual incidents is classified and hard to verify. According to experts, however, terrorist groups had considered the integration of hacking into their repertoire already by the end of the 1990s (Borland 1998). Today, at least some terrorists are known to possess considerable hacking skills (Embar-Seddon 2002).

Apart from the actual skills, the time that is needed to educate a group on relevant hacking skills is also under debate. Members of the US *Naval Postgraduate*

School, for example, estimated in 1999 that it would take from 2 to 4 years to acquire the skills necessary to launch "advanced – structured" attacks. For "complex – coordinated" attacks a time-frame of 6–10 years is expected (Desouza & Hensgen 2003). Because access to the Internet and therefore the amount of freely available information has enormously increased since 1999, however, it has to be doubtful that those figures can still be regarded as realistic.

Furthermore, terrorists do not have to rely on their knowledge alone. Experts assume that it is a realistic option for professional hackers to be hired by terrorist groups – in some cases without knowing about the true expectations of their customer (Borland 1998). On the other hand, most terrorist organizations have worked in conspiratorial and close environments where weapons, attacks, and personnel were chosen and tested carefully and put to use only if no risk was to be expected. Therefore, a final assessment whether terrorists would use this form of "outsourcing" remains speculative.

Data Alteration

After a successful hacking attack, a perpetrator has many options on what to do with the system. A comprehensible first reaction would be to delete information or shut down the system. However, this technique would not be successful (at least not for any length of time), because administrators would immediately notice the failure and could reconstruct the system from backup files or switch to reserve systems. The amount of damage that would result from such an attack would therefore not be too high. However, in some areas, e.g. certain industrial production facilities or in medical environments, even short outages could have disastrous consequences.

Defacements

Alterations that are visible to a large audience are often considered to be better, because they can demonstrate the technical capabilities and create fear of what other systems could fall foul of future attacks. An example of an attack that is widely recognizable is a so-called defacement that often takes place after a hacker has gained access to a web server. In this case, a page on the web server, often the prominent entry page, is altered. Often insults (e.g. to the technical incapability of the system administrators) are put on the page together with hints as to the identity of the perpetrator (e.g. the name of a hacking group). By leaving this form of "digital business card", the perpetrator can keep record of their successful break-in and therefore of their technical capabilities. While other forms of cyber crime often remain in the dark, defacements are clearly meant to be seen by a large audience.

A large-scale series of defacements could be interesting for terrorists, especially if servers that belong to security agencies, the military, or other important services are concerned. This has already been observed. In the year 2001, for example, the group "Pentaguard" demonstrated its capabilities when it simultaneously defaced a

multitude of government and military websites in the UK, Australia, and the United States. This attack was later evaluated as one of the "largest, most systematic defacements of worldwide government servers on the Web" (Leyden 2001). In another case, pro-Palestinian hackers used a coordinated attack to break into 80 Israel-related sites and deface them (Conway 2002; Vatis 2001). Even al-Qaeda used the technique of defacement to demonstrate its technological as well as its conventional dangerousness when it deposited images of the hijacked (and later beheaded) Paul Marshall Johnson, Jr. on the hacked website of the Silicon Valley Landsurveying, Inc. (Musharbash 2004).

Other Forms of Data Alteration

Other forms of data alterations are discussed mainly as theoretical threats. Unlike the defacements that were discussed above, other alterations are usually not as obvious and therefore hard to recognize. This enables them to result in great damage.

Targets that are discussed in the literature as exceptionally disastrous are, for example, databases with social security numbers, data sets of banks and other financial institutions, or collections with military and classified information. Unnoticed attacks on any of these databases could have disastrous effects on the economy of a country and result in a continuing lack of trust of the people in their systems and institutions if changes were not to be detected (and repaired) within a short period of time (Berinato 2002).

Some authors claim that activities such as a manipulation of large and central databases would exceed the capabilities of terrorist groups that are often not composed of long-time experienced hackers. Planning games such as "Eligible Receiver"[5] and current information regarding recent attacks have shown, however, that even top-secret military computers and research laboratories that are handling nuclear materials are not immune against all possible forms of electronic attacks (Vatis 2001; Wilson 2005). For a realistic risk assessment, at least the possibility that terrorists are considering or evaluating such attacks has to be taken into account.

Data Espionage

For terrorist groups, the acquisition of information about their opponent is as important as for any other organization. If, for example, it becomes known that communication channels between members of the group are being monitored or that plans for a future operation have leaked to government agencies, appropriate action needs to be taken. Because most of today's communication structure is computer based, data espionage is on the rise throughout.

Commonly, the clandestine exploration and obtaining of protected digital information was originally particularly known between states that try to acquire security

[5]For more detailed information about the experiment "Eligible Receiver", see Sect. 2.2.3.

relevant information from other states to gain tactical advantages. However, in the meantime, industrial espionage has also become an important factor for many economies. With regard to electronic espionage that is directed against digital information, the boundaries between the activities of individual hackers, organized groups, and state-sponsored fractions become increasingly blurred.

In a case that took place in 1999 and that was later named "Moonlight Maze", for example, hackers allegedly were able to get access for a period of more than 1 year to computer networks at the US Energy Department nuclear weapons and research labs, at the National Aeronautics and Space Administration, and at numerous university research facilities and defence contractors. Although no classified computers were known to have been breached, even the unclassified networks are said to contain confidential and sensitive data that could potentially be valuable to any foreign government or terrorist group (Drogin 1999; Thornburgh 2005a). Experts therefore claimed that the value of the information that was gathered was "in the tens of millions – perhaps hundreds of millions – of dollars" (Testimony of James Adams, Chief Executive Officer, Infrastructure Defence, Inc. 2000).

Although evidence indicated in the beginning that the attacks of "Moonlight Maze" originated from Russian computers and that the attacks were state sponsored (Drogin 1999), this was later refuted by government officials (FCW Staff 1999). As in many cases, in the end, it remained unclear as to what extent which kind of information had been accessed. In addition, it could not be determined if the computer that was really used to attack was the computer of the actual attacker, if the attacker was acting on their own or on behalf of a government, or if the computer was only a hacked computer that was used to camouflage the traces to the real offender.

Almost the same is true for a series of attacks that started in 2003 and were named "Titan Rain" by the US government. Although evidence indicated, according to experts, that it would be "unlikely to come from any other source than the [Chinese] military" (AFP News Agency 2005), the exact source of the attack, the amount of data that was acquired, and the precise nature (i.e. state-sponsored, corporate espionage, or random hacker attacks) remain unclear (AFP News Agency 2005; Espiner 2005; Graham 2005; Thornburgh 2005b).

Apart from cases where data espionage is handled either by technical means as described above or by ways of social engineering, terrorist organizations can also try to get access to sensitive information by legal means. One example concerns the Japanese Metropolitan Police Department, which hired a company for the development of a software system for the tracking of their (also partly unmarked) cars. It later turned out that a part of the software was developed by members of the Aum Shinrikyo cult – the same group that was responsible for the gassing of the Tokyo subway in 1995. This was possible because the software developers were engaged as subcontractors, thus enabling personnel clearance to be circumvented. As it turned out later, members of the cult had developed not only this piece of software, but they were engaged in activities for at least 80 firms and 10 government agencies (Weimann 2005).

Another case concerned the company Ptech in Boston. The firm was, among others, working for the US Air Force, NATO, the US Congress, and it was developing

counterterrorism software for the FBI. Accordingly, the company had access to sensitive military and similar sensitive security relevant information. According to news reports, Yassin Al Qadi, a Saudi millionaire with alleged connections to Osama Bin Laden and al-Qaeda, had invested several millions of dollars into the company (Desouza & Hensgen 2003). Therefore, the US government feared that security-relevant information could have leaked to the terrorist organization, and they raided the company premises in 2002.

Denial-of-Service Attacks

Denial-of-service (DoS) attacks are targeted at the unavailability of a system or service and have a long tradition in computer crime. Modi operandi range from a crude cutting of power cables to complex exploitations of security weaknesses. Since the last couple of years, individual attacks have been replaced by DDoS attacks. So-called bot-nets, with hundreds or even thousands of Trojan horse-infected computers, are commanded by individuals to send massive requests to single targets. These computers are often not able to handle the enormous amount of traffic and are no longer able to send answers to either the computers of the bot-net or to other – legitimate – requests. Computers that are under the attack of a bot-net therefore seem to be unreachable (Brunst 2008; Janczewski & Colarik 2005; Wilson 2005).

An impressive example of the use of bot-nets was the "Estonian Cyberwar" that took place in 2007. During a longer period of time, Estonian government, news, and banking sites were under massive attacks by bot-nets. At the same time, coordinated hacking and defacement attacks took place (Davis 2007). According to Estonian Defence Minister Aaviksoo, more than one million computers worldwide were engaged in the attacks (Sliva & Ritter 2006). Because most of the attacks originated from Russia and some evidence indicated that the coordination of the attacks was of a quality unseen before, it was assumed that the Russian government was involved in the attack. Later, however, these charges had to be dropped, because it was not possible to determine whether the attacking computers were the origin of the attack or if they were only used to disguise the real perpetrators (Davis 2007; Rolski 2007; Sliva & Ritter 2006; Traynor 2007).

DDoS attacks do not necessarily have to be launched only with technical means. To call attention to the involvement of the German airline Lufthansa in the deportation of illegal alien residents, supporters of an online demonstration were asked to open the web page of the company at the same date and time. More than 13,000 people followed the call. In return, the Lufthansa server was unable to reply to the sudden peak of requests, and the web page became unavailable to customers during this time frame (OLG Frankfurt a.M. 2006). This technique is also known as "swarming", "virtual blockade", or "virtual sit-in" and it shows that even technically non-adept organizations can use the power of distributed attacks against targets on the Internet (Denning 2001; Weimann 2004a).

Instead of launching a DDoS attack by themselves or motivating followers to engage in such activities, terrorist organizations can also "outsource" activities.

Prices for attacks range from approximately 150–400 US dollars, depending on the target and the duration of the attack. Some bot-net operators even offer discounts for multiple orders (Brunst 2008; Sieber & Brunst 2008).

In the past, it could be observed that groups were actively using DDoS attacks to push their goals. For example, six different Hizbollah sites, the Hamas site, and other Palestinian information sites were brought down by a so-called FloodNet attack of pro-Israeli hackers. The service virtually "flooded" the respective servers with pings resulting in the unavailability of the servers for all other requests. Even after a relaunch with a slightly different spelling, the sites were still unreachable because the hackers immediately adjusted the attack to the new names (Conway 2002; Denning 2001).

Conventional Attacks on IT Infrastructure

Terrorists are free in the choice of their weapons and their targets. It is only the expected success, the necessary effort, and the possible consequences that guide terrorists. Because IT infrastructure and especially the use of the Internet have become essential parts of the everyday life of most individual and corporate users, conventional attacks might also be considered as an option by terrorists. Three examples show possible scenarios.

The domain name system (DNS), for example, is essential for many services that use the Internet. It is necessary to translate a human-readable domain name (e.g. www.mpicc.de) into the IP address (e.g. 194.94.219.193) that is needed by the computer to contact the appropriate server. If an attacker was able to disrupt DNS services, large parts of the Internet would be unusable. The attempt to hamper the functioning of the 13 root-DNS servers in 2002 was therefore evaluated by some authors as an attack against the "heart of the Internet" (Weimann 2004a). However, the consequences of these attacks were hardly noticeable due to built-in safeguards of the DNS systems: no slowdowns or even outages were caused. The same is true for a recent attack that took place in February 2007: even though the aggression lasted for almost 12 hours, the influence was hardly noticeable (ICANN 2007). If, however, terrorists were able to find a way to successfully disrupt the functioning of the DNS – even for a limited region – the consequences would be noticeable immediately by all of the affected users. This, on the one hand, could result in dramatic consequences for the economy that is largely dependent on the Internet as a main connector to their customers and other businesses. On the other hand, a destruction of Internet communication could also be used in connection with conventional attacks.[6] The incidents in Estonia, for example, have shown what happens if a whole population is no longer able to access independent information about recent incidents, because Internet connections are not available. Therefore, a terrorist organization could be interested in launching a conventional attack and blocking

[6]See the section "Hybrid Attacks" below for further information on the so-called "hybrid attacks".

all (apart from traditional media) access to independent information from the Internet, thereby raising the amount of panic and the feeling of helplessness within the population.

A second approach to attack IT infrastructure with conventional means could target the intercontinental connections. For example, many transcontinental data connections rely on transatlantic cable connections between Europe and the United States. Whereas European cable ends are widely spread between many different countries, they are often bundled on the American side and could therefore be an interesting target. The effects of such an attack could be observed when cables between the United States and China were damaged accidentally (Brunst 2008). According to a survey after this mishap, 97% of the Chinese users reported problems accessing foreign web pages; 57% claimed that their life and work was being affected by the damage (Persson 2006). If committed intentionally by terrorists, economic effects, in particular, could be the consequence. Furthermore, the psychological side within the population at large (terrorists being able to "shut down" the Internet) would be interesting.

Even though the structure of the Internet is spread widely and between many different systems, important connection points between different networks exist, so-called peeringpoints that could pose as possible targets for a third approach. The German peeringpoint DE-CIX in Frankfurt, for example, is said to handle 80% of the German and 35% of European Internet traffic (according to Force10 Networks 2007). The London Internet Exchange, LINX, is the world's largest Internet peeringpoint and was in the centre of a planned assault in the year 2006. However, Scotland Yard was able to arrest the suspects beforehand so that no damage was done. An MI5 website is reported to have said in this context that "without these services, the UK could suffer serious consequences, including severe economic damage, grave social disruption, or even large-scale loss of life" (Leppard 2007).

Hybrid Attacks

Although the attacks mentioned above are either pure electronic or pure conventional, many authors see a particular danger in hybrid attacks. Hybrid attacks are aggressions that use the advantages of both the virtual and the real world, e.g. to increase the number of casualties. This, for example, could be the case if perpetrators were able to manipulate the communication systems of police and ambulances to hinder an effective coordination of rescue teams in the event of a conventional bomb attack (Vatis 2001; Wilson 2005). Reality has already shown that such a scenario is not total science fiction. For example, a hacker from Toborg, Sweden was able to partially manipulate the "911" emergency call system in Florida, United States (Borland 1998; Cilluffo 2000). It is unknown, however, if this was the intention of the hacker or only a coincidence.

Apart from these attacks that are aimed at the lives of people, other hybrid attacks are being discussed that focus on severe economic consequences. These could occur if the perpetrators were able to launch a successful assault against

national financial networks (such as Fedwire or Fednet) or against transfer networks (such as SWIFT). It is estimated that such an attack could weak havoc on the entire global economy (Wilson 2005).

2.2.2.2 Attacks Against Human Lives

Even more dangerous than attacks that are targeted purely against other IT systems are those that target human lives. To understand the concept of such attacks, it is necessary to first describe the technical background for such attacks (see the following section "Technical Background"). Afterwards, a distinction is necessary between scenarios that target immediate death or bodily harm of the victims (see the section "Attacks with an Immediate Outcome") and those that try to achieve a long-term success (see the section "Attacks with a Long-Term Effect").

Technical Background

Often, attacks against computer systems are considered less dangerous than conventional attacks with bombs, because damages to computers are said to "only" lead to economic losses. At first glance, it seems almost impossible that human lives could be endangered by mere electronic attacks. However, the convergence between a "real", i.e. physical, and a "virtual", purely electronic, world is constantly rising. Therefore, computers are no longer exclusively used to "crunch numbers" and store huge amounts of data. Instead, a new type of computing services has quietly evolved without which production facilities for food, pharmaceutical products, electricity, traffic management systems (especially for trains and airplanes), and many other military and civil establishments would be unthinkable today. So-called supervisory control and data acquisition (SCADA) systems are used to measure and control other systems.

Often, SCADA systems are either directly connected to the Internet or they are connected to internal networks that are themselves connected to the Internet. According to informal sources, 17% of SCADA malfunctions are caused by a direct Internet access to the SCADA system (Sieber & Brunst 2008). The reason for this is often the wish that systems should be ubiquitously accessible so that data and systems can be controlled remotely (Collin 1997). In the long run, owners hope to save costs if they are able to reduce personnel on site and consolidate at a central location. As a result, many connection lines that carry sensitive data exist on the ground, in the air, or in the water. All of these could pose as targets for terrorist attacks. Furthermore, a successful attack against only one site can reveal access and possibilities for manipulations at many different localities. Because many of the control systems are based on standard Windows and UNIX operating systems (Bachfeld 2003), some hackers claim that it would take them only about a week to get into most of the existing control systems (Lenzner & Vardi 2004).

The effect that SCADA systems that are connected to the Internet can have on a population could be observed in 2003 when 21 power plants were brought down, and other critically important institutions in the United States (including Edwards Air Force Base, the test centre for B-2 and B-1 bombers) were also affected. Following the incident it was discussed whether these breakdowns were the result of the W32. Lovsan worm that was using the same port to exploit a weakness on individual personal computers being used by the plants to communicate with each other (Bachfeld 2003). The collision resulted in a large power-down in the United States and Eastern Canada. It is therefore an important task to determine which parts of a national infrastructure have to be regarded as "critical", i.e. a successful attack would have a serious impact on a nation. By the mid-1990s, the US *President's Commission on Critical Infrastructure Protection* determined eight areas of critical infrastructure that were considered as vulnerable and potential targets for attacks (Embar-Seddon 2002).

Attacks with an Immediate Outcome

Most of the attacks that are aimed at critical infrastructure have an effect that is immediately noticeable. Additionally, none of the scenarios that are described below have – as far as it is known to the public – taken place yet. Nevertheless, many authors see them as realistic possibilities that could be taken into consideration by terrorists, because their outcome is more direct and visible than most of the pure attacks on IT infrastructure described above. Furthermore, they almost guarantee what is important to generate fear within a population: extensive news coverage with impressive picture material. As such, mainly three scenarios are discussed in the literature: attacks on hydroelectric dams; tampering with control systems, especially for railways or air traffic; and taking over control of power plants.

Attacks on Hydroelectric Dams

Probably the most discussed scenario of cyberterrorism with an immediate danger for human lives is an attack on a hydroelectric dam. A perpetrator could gain access to a control system and remotely open the floodgates, thereby endangering the areas and inhabitants behind the gates. The consequences of (accidentally) damaged dams could be observed in the past, e.g. when, in 1975, the Banqiao and Shimantan dams on tributaries of Hang He (Yellow) river in China failed. Dozens of lower dams were damaged and at least 85,000 people died (Gleick 2006). Today, security measures at most dams probably would prevent such extreme results. However, if terrorists were able to control a dam, e.g. by hacking into the SCADA system controlling it, a deliberate opening of the floodgates could put hundreds or even thousands of people at risk.

The danger of dams connected to SCADA systems could be observed especially in two scenarios. In the first scenario, an individual was able to break into the computer system that runs Arizona's Roosevelt Dam. Although some details of the attack are being disputed (for details, see Brunst 2008), the fact alone that the

Roosevelt dam was compromised is sufficient to show the danger of a terrorist attack. The second case concerns a case that took place in the year 2000 in Queensland, Australia. There, the culprit was able to manipulate the control system of the sewage treatment facilities over a period of 2 months, letting hundreds of thousands of gallons of putrid sludge ooze into parks and rivers. According to an employee of the Australian Environmental Protection Agency "marine life died, the creek water turned black and the stench was unbearable for residents". In the concrete case, the motive of the perpetrator was not to generate fear in the public. The damage was caused "only" to bargain for a consulting contract to fix the problems he had caused (Gellman 2002; Giacomello 2004). However, the case also shows the potential a terrorist would have for bio-related terrorism, i.e. causing illness or death not only in people, but also in animals or plants (for further details on the threat of bioterrorism see Centers for Disease Control and Prevention 2007; Committee on Water Systems Security Research 2007; Leitenberg 2005).

Attacks on Traffic Control Systems

In the attacks of 9/11, the hijackers impressively and horrifically showed the amount of damage that they could do with airplanes under their control. It is easy to imagine the possibilities and the fear that would be created if terrorists were able to gain control over airplanes or airport control systems without actually being on board.

In 1997, for example, a juvenile was able to access the communication systems of Worcester, MA airport. The action disrupted the telephone service to the Federal Aviation Administration Tower at the airport, the Airport Fire Department, and other related services such as airport security, the weather service, and various private airfreight companies. Furthermore, the main radio transmitter and the circuit that enables aircraft to send an electronic signal to activate the runway lights on approach were disabled (Berinato 2002; Cilluffo 2000; Testimony of FBI Deputy Assistant Director Keith Lourdeau on "Virtual Threat, Real Terror: Cyberterrorism in the 21st Century" 2004). Fortunately, no accidents were caused by the attack.

The incident, however, shows the vulnerability of modern transportation systems. Therefore, not only airports and airplanes (which are usually quite well protected), but also train systems are the focus of the discussion. In a worst-case scenario, colliding trains or airplanes could possibly cost hundreds of lives (Giacomello 2004; Weimann 2005).

Attacks on Power Plants

The scenario that probably causes the most fear is a manipulation of power plants, especially of nuclear power plants. A similar danger is expected from intrusions into military missile control centres. Although these premises should count as areas with the highest protection and control density, authors still see a possibility for terrorist attempts (Foltz 2004). Furthermore, the massive breakdown of nuclear power plants in 2003 that was described above (see the section "Technical Background") clearly shows that even these systems are vulnerable to cyber attacks.

Attacks with a Long-Term Effect

Some scenarios that are discussed in the literature do not result in a one-time catastrophe. Instead, they aim at a long-lasting panic, fear within the population, and a continuing distrust in local economies. As such, they pose tempting targets for terrorist groups.

One of the cases that are being discussed as a theoretical threat is the manipulation of the production line for breakfast cereals or for baby food. If, for example, a terrorist was able to manipulate the production process and change to proportion of ingredients, this could prove dangerous for the customers, e.g. if the portion of iron in baby food was increased to a hazardous amount (Collin 1997). The same effect could be induced if terrorists changed the doses or composition of pharmaceutical products and medicine (Collin 1997).

Other areas that are being discussed concern the manipulation of weapons production processes, where a manipulation could lead to useless ammunition or attacks on the economical stability of a country by way of secret manipulations on bank, currency, and transfer systems (for further details, see Brunst 2008; Sieber & Brunst 2008).

2.2.3 Risk Assessment

The scenarios that are discussed last, i.e. attacks with a long-term effect are probably the ones that have to be feared the least. The production chain of a food company, for example, is usually constantly monitored. A manipulation would therefore often be detected already at an early stage. In addition, a sudden increase in the use of different ingredients would likely draw attention. Finally, a manipulation of the composition of certain food products will most likely alter the taste of the product so that again either quality control or customers will detect the change. Other areas that were mentioned (e.g. weapons or medication production sites) are often high-risk areas, where security measures are high, and production computers are seldom linked to public networks.

The same seems – at first glance – to be true for many of the attacks that would lead to an immediate outcome. Often, the sites affected by attacks – especially military ones – are "air-gapped", meaning that they are completely physically, electrically, and electromagnetically isolated (Brunst 2008). In these cases, a remote launch of, for example, a military missile would simply be impossible (Foltz 2004; Green 2002). Furthermore, many of the situations described rely on a failure of all accompanying security measures at the same time. Especially air traffic controllers and pilots are trained regarding "situational awareness", however, and use computers only as an aid. For a successful attack, it would therefore be necessary to manipulate not only the control system, but also pilots and/or controllers (Pollitt 1998).

There are, however, no grounds for a complete all-clear:

- One reason is that it is not reasonable or sufficient to distinguish exclusively between "computer-only" and "human-only" scenarios. Many organizations will, for example, have the funds to buy or otherwise introduce an insider. This can happen either in the form of active participation or in the form of gathering otherwise protected information. With such help, many security measures can be dangerously compromised. The cases of the Japanese Metropolitan Police Department or the company Ptech that were described above (see the section "Data Espionage") show that even vettings can be successfully circumvented.
- Another problematic area is the increasing use of connectivity and remote controlling even in high-risk areas. For example, new weapons are being developed by the military that rely on remote control, e.g. semi-autonomous military robots (see Brunst 2008 for further details). Many of these products rely on civilian technology and established operating systems, thereby opening additional loopholes for security risks.
- Finally, terrorists can use the fact that often, due to a lack of technical knowledge, members of the press or even politicians will draw wrong conclusions from facts that have become known to the public. For example, it is widely known that computers are used within missile launching premises. Computers have security weaknesses that can be exploited. Therefore, the deduction that missile centres are vulnerable to cyber attacks suggests itself. However, this conclusion might be wrong, if systems are in fact air-gapped as described above. This is, in turn, used by terrorists who do not necessarily rely on attacks being successful. An important aspect of terrorist attacks on the Internet is rather the creation of fear and uncertainty and the expectation that terrorists *could* at any time strike at any target they chose.

In this context, attacks against IT infrastructure can be of great help. The pure number of vulnerabilities that have become known and the number of targets that can be chosen offer a wide range of possible actions for cyber criminals as well as for terrorists. Any successful attack against "prominent" targets, e.g. government or intelligence websites, can be used to increase the level of anxiousness regarding more serious attacks.

The real danger that evolves from cybercrime attacks could be seen already in 1999, when the United States conducted an exercise named "Eligible Receiver". Hackers of the NSA acted as a so-called red team and attacked computer systems of the CIA, FBI, Defense Intelligence Agency, National Reconnaissance Office, Defense Information Systems Agency, Department of State, Department of Justice, and civilian establishments of relevant infrastructures during a 5-day period. Although many details of the exercise remained secret, it has become known that the red team relied solely on techniques and software that was freely available over the Internet. The group was able to enter protected networks, render systems inaccessible with the help of DoS and DDoS attacks, forge e-mails and gain root

level access to 36 government networks. Even the take-over of resources of the US Pacific Fleet, control of electric power systems, and the emergency number "911" in nine larger American cities was allegedly possible (Pike 2005; Weimann 2005).

Often, those who claim that cyberterrorism is not a real threat state also that terrorists lack the necessary skills for an electronic attack. The current generation of young terrorists, however, has – at least partly – grown up in a digital world. Computers seized from al-Qaeda, for example, show that they are becoming increasingly familiar with hacker tools that are freely available over the Internet (Wilson 2005). Furthermore, know-how, personnel, and outsourced services can be acquired on the free market, making it possible even for incapable groups to enter the new world of cyber attacks. The Islamic fundamentalist group "Harkat-ul-Ansar", for example, attempted to buy cyber attack software from hackers as early as late 1998 (Wilson 2005).

Finally, many nation states have started to invest into cyber forces to increase their powers also in this relatively new sector. This, in turn, opens new possibilities for state-sponsored terrorism (see Brunst 2008 for further details). The threat of future terrorist attacks that involve specific use of the Internet therefore has to be taken very seriously.

2.3 Dissemination of Terrorist Contents

With the establishment of the WWW, the Internet has created the possibility for everyone to disseminate information without costs – and largely without any control regarding the content. Terrorists are using the Internet therefore not only to launch attacks, but also to fight a "war of ideas" (Giacomello 2004).

2.3.1 Terrorist Websites

For a terrorist organization, it is extremely important to communicate their views, aims, and ambitions. Although in former times this was extremely difficult, the Internet now offers possibilities to easily communicate and possibly influence the media and the public at large (Brunst 2008). Therefore, it is no wonder that today almost every underground organization has its own website (Weimann 2004b, 2006) and the number is still steadily rising. In 1999, only a few of the 30, according to the US Department of State, deemed foreign terrorist organizations were able to operate a website (Conway 2002; Desouza & Hensgen 2003). By 2005, this number had increased to more than 4,500 terrorist-related websites (Coll & Glassner 2005; Conway 2002). The number of Internet-related items that carry terrorist contents (i.e. including forums, blogs, etc.) is even higher. According to some sources, in 2007, there were approximately 50,000 sites with extremist and terrorist content (Chen & Larson 2007).

Terrorist websites can be used for a number of purposes. For example, it is possible to target special audiences, e.g. the media, followers, or – with cartoon-style design and children stories – even young kids (Tsfati & Weimann 2002; Weimann 2004b, 2006). Contents can be presented as mere text-written viewpoints or – often with the help of fresh graphics, sound, or video files – as a glorification of recent acts or as an incitement to future acts (Brunst 2008). Although it is difficult to assess how many people are paying attention to these websites, it is said that the most popular terrorist sites are able to attract tens of thousands of visitors every month (Conway 2002). The difficulty of judging an organization only by its website (often as its only "official" organ) can also be abused. For example, a terrorist organization with an impressive website can easily claim to be bigger and to have more followers than it actually has (Embar-Seddon 2002).

Another issue of popular terrorist websites is that governments will often try to shut them down when they becomes too popular. However, the censorship resistance of the Internet in many cases prohibits these efforts. For this reason, many websites are not stored in the country of their organization. Instead, they are hosted on servers in countries that have a more liberal freedom-of-speech approach. Several websites of al-Qaeda, for example, were physically stored in the United States and Canada (Brunst 2008). The same is true also for other organizations that chose to be hosted outside of their country (Desouza & Hensgen 2003).

2.3.2 Threats and Propaganda

As already mentioned above, terrorist websites are not restricted to presenting only their own viewpoints. Instead, they can also be used to threaten the enemy or to spread propaganda. Especially if threats are presented with the help of multimedia technology, this gets the attention of the press and the public. For this reason, computer games have been developed, e.g. one named "Quest for Bush" that lets followers kill US President Bush (Vargas 2006). Other multimedia threats can literally burn images into the memories of the viewing audience. The assassination of Daniel Pearl, for example, showed the impact of psychological warfare that was conducted by these new means. Since then, the use of multimedia has rapidly increased. Whereas the al-Qaeda media arm As-Sahab issued only six audio or video web messages in 2002, this number increased to an impressive 97 multimedia messages in 2007 (Sedarat 2008).

To improve the presentation of their viewpoints, threats, propaganda, or incitements to terrorism, terrorists have even begun to record their attacks. For the best results, they are often filmed simultaneously from different angles so that the material can be better used for the distribution to the media, websites, and the production of DVDs (Kristof 2005). This kind of material is often used to (directly or indirectly) influence public opinion.

In the past, only a few well-established organizations were able to produce newspapers, magazines, or TV shows. The Internet makes it now possible for virtually

anyone to launch their own periodicals. Al-Qaeda therefore was able, for example, to start its own TV program "voice of the caliphate", which is available on the Internet. In the program, a hooded newsreader with a gun and a copy of the Koran on his desk, reads the latest headlines from the world of the Islamist jihad (La Guardia 2005; Musharbash 2005). Additional multimedia items were often sent out by the "Global Islamic Media Front" (GIMF). This kind of information can normally be easily recognized as terrorist material. Other information, however, might be disguised as seemingly neutral material in the hope that less critical members of the press take up the news and report about them. Because the Internet has become a major source for stories, background information, and also for photographic and similar material, this hope cannot be dismissed. By attractively presenting viewpoints and opinions, terrorist organizations can at least increase their chances of introducing these opinions into mass media products.

2.3.3 Financing

Online advertising and similar ways of gaining monetary income with Internet services has become a profitable business model for many. For terrorists and terrorists groups, this is not as easy, especially if explicit terrorist content is contained on a website. Nevertheless, some organizations have started to use their site not only to disseminate information, but also to use their site as a source of income for financing and fundraising.[7] Some websites, for example, are used – apart from their original purpose – to sell CDs, DVDs, T-shirts, badges, flags, or books (Conway 2002; Weimann 2004b).

Another way to finance terrorist activities is to give instructions on how to donate money. This can be done, for example, by giving necessary information (e.g. bank account details for transfers) or by implementing possibilities to enter credit card information for automatic withdrawals (Weimann 2004b).

Since the websites terrorist organizations are often at the center of surveillance by security agencies, hundreds of support websites commonly appear and disappear. Each website provides links to other supporter websites so that a visitor who once has found an entry point into the terrorist web can easily find other and similar sites. In some cases, even specialized web rings are founded. Yahoo!, for example, hosted dozens of sites in the "Jihad Web Ring", a coalition of 55 Jihad-related sites (Buettner 2001; Conway 2002; Reuters 2001).

If, at any point, users give personal information, terrorists are also able to gather user demographics. This can happen, for example, if a user fills out online questionnaires, order forms, or enters relevant e-mail lists. Users that are identified as potential sympathizers can then be e-mailed and asked to make donations over other (e.g. more secret) channels (Weimann 2006). Because this

[7]For other aspects of terrorist financing, see Chap. 16.

first contact is made electronically and over a distance, users might engage more easily into this "clean" form of terrorist support, which also can function as a gateway into closer ties between terrorist organizations and their future supporters.

2.4 Conventional Use of the Internet

A commonly underestimated threat is the conventional use of the Internet. While the access to "dangerous" sources, e.g. terrorist websites or relevant message boards, could – at least potentially – be constantly monitored and taken as an initial point for action, this is not possible with everyday services such as search engines, common websites, or e-mail traffic. However, a closer look reveals that even seemingly harmless sites offer information that is, on the one hand, valuable and important for terrorists and, on the other hand, uncontrollable. By way of example, the use of individual communication between terrorists and the planning and supporting of conventional attacks will be highlighted below.

2.4.1 Individual Communication

Although conventional methods for individual communication are still widely available, e.g. telephone or letters, they have individual disadvantages over the possibilities that the Internet offers. A telephone conversation, for example, requires both parties to be present simultaneously at their point of communication. Additionally, contents are transmitted unencrypted so that government agencies can listen if the parties are already under surveillance (or if they are affected by strategic large-scale surveillance measures). A letter, on the other hand, offers the possibility for asynchronous communication and easy encryption, but it takes longer to transmit. Additionally, like the telephone, it requires both parties to be present at certain points, e.g. at a mailbox for the sender or at the destination address for the recipient.

The Internet, however, allows both parties to communicate asynchronously, e.g. by e-mail. This service does not require much bandwidth, making it possible to send and retrieve information even over older mobile phones or in areas where Internet connections are limited. Additionally, messages can be stored and retrieved at any given point in time; terrorists neither have to be online all the time, nor do they have to entrust third parties with the task of accepting personal messages for them. Therefore, e-mail allows terrorists to communicate independently of a specific and pre-determined place. Furthermore, many companies offer e-mail services free of charge so that several different e-mail accounts can be used simultaneously. The organizers of the 9/11 attacks, for example, had operated in such a way and opened multiple accounts on largely anonymous e-mail services, such as "Hotmail" (Conway 2002).

If, for any reason, a synchronous communication is preferred, the Internet offers many different opportunities as well. Internet Relay Chat (IRC), for example, allows for a conversation between two or more persons who are online at the same time. The service is text-based, fast – and largely unsupervised. Even voice-based systems, like Skype, can be used (Weimann 2004b; Wilson 2005).

The biggest advantage of Internet-based communication, however, is that all messages are digital right from the start. Therefore, many publicly available encryption programs can be used (see Brunst 2008; 2009 for further details). These are accessible as open source so that terrorists can check themselves for hidden backdoors or other unwanted "features". Nevertheless, terrorist groups have started to compile their own software products for encrypted communication. The software "Secrets of the Mujahideen" – currently available as version 2.0 – is advertised as "the first Islamic program for secure communications through networks with the highest technical level of encoding" (Sedarat 2008). The use of such specialized and often easy-to-use applications drastically increases the protection of terrorist's messages between each other. This, in turn, makes it hard or – if used correctly – impossible for government agencies to successfully monitor communication, resulting in a lack of information.

2.4.2 Planning and Supporting

It seems surprising that most of the information needed for a conventional attack is not protected, but freely available. This can, for example, be a picture of an important manager that is available on a company's website or the favourite nightclub of his teenage daughter that can be taken from her profile on facebook.com. According to a terrorist manual, public sources can therefore provide up to 80% of all required information on an opponent (Weimann 2004b).

An example that is often cited is the satellite maps that are provided, for example by Google, Microsoft, or NASA. In former times, images of that quality were available only to experts, now they are a common good and accessible to anybody. It is therefore of no surprise that terrorists have started to use these services for their own purposes. According to UK army intelligence sources, for example, during a raid in 2007, printouts from Google Earth were found. They showed buildings inside the British bases in Basra in detail and vulnerable areas "such as tented accommodation, lavatory blocks and where lightly armoured Land Rovers are parked" (Harding 2007). Due to some additional evidence, officials believed that this information was used to prepare attacks on the premises.

According to some authors, terrorist organizations have even started to use databases to gather, sort, and evaluate the details of potential targets in the United States (Weimann 2004b). Actual findings on terrorists' computers have shown that publicly available information of all kinds are indeed being downloaded and used for planning purposes (Harding 2007; Weimann 2004b). It can therefore be assumed

that information that is freely available on the Internet is indeed significantly strengthening the operational capabilities of terrorist groups.

Terrorists, however, are not only taking information from the Internet. They use the net also to store information and make it available for others. Some authors therefore claim that the Web has become "an open university for jihad" (Coll & Glassner 2005). This "university" offers information such as the "Mujahadeens Poisons Handbook" that contains various "recipes" for homemade poisons and poisonous gases (Weimann 2004b, 2006). Similar information is compiled in other collections, such as the "Terrorist's Handbook", the "Anarchist Cookbook", the "Encyclopedia of Jihad", the "Sabotage Handbook", and the famous "How to Make Bombs". Today, many collections are amended by extra information, e.g. on hostage taking, guerrilla tactics, or special kinds of bombs (Brunst 2008).

2.5 Conclusions

In this chapter, different risks of terrorists using the Internet have been assessed. Although a large cyber attack that was verifiably committed by terrorists has – up until now – not taken place, this is no reason to underestimate the risks and potential of future scenarios. Already the brief outline of the conventional use of the Internet by terrorists has shown that terrorists are not unfamiliar with the Internet. On the contrary, it is known that the Internet is constantly used for their purposes already today, e.g. to prepare conventional attacks, to communicate, or to disseminate their respective contents.

The general characteristics of the Internet indicate furthermore that digital attacks are a likely scenario. Chances are high that such incidents will be directed against other IT systems, especially if connected to real-world machinery, and result in an immediate outcome rather than long-term effects. The attacks and aggressions that have been launched in the past by common cyber criminals, state-sponsored, or (presumably) governmental groups have partly demonstrated the potential of such assaults. Especially the two last-mentioned groups have to be considered as extremely dangerous, because they have the ability to use monetary and technical resources to which common criminals seldom have access.

The actions that have been taken on a political and legal level to counter cyberterrorism have, for a long time, been rather reluctant.[8] In the end, it was probably the attacks on Estonia in 2007 that showed governments around the world and the public at large what knowledgeable aggressors can do to a whole nation solely by digital means. International organizations such as NATO therefore now take cyber attacks "as seriously as the risk of a missile strike" and see cyberterrorism as a chief threat (Johnson 2008). Especially if a nation with offensive cyber capabilities is

[8]For legal responses that have been taken to conquer cyberterrorism see Sieber, this volume.

willing to support perpetrators, the risks and potential damages will additionally increase. The convergence of terrorism and the cyber world therefore creates a new threat that has to be taken very seriously.

References

AFP News Agency. (2005). Hacker Attacks in US Linked to Chinese Military [Electronic Version]. *Breitbart.com*, *12.12.2005*. Retrieved April 2008 from http://www.breitbart.com/article.php?id=051212224756.jwmkvntb&show_article=1.

Bachfeld, D. (2003). War der Wurm drin? *c't, 2003*(18), 34.

Berinato, S. (2002). Cybersecurity – The Truth About Cyberterrorism [Electronic Version]. *CIO Magazine*. Retrieved April 2008 from http://www.cio.com/article/30933/CYBERSECURITY_The_Truth_About_Cyberterrorism.

Borland, J. (1998). Analyzing the Threat of Cyberterrorism [Electronic Version]. *Techweb.* From http://www.techweb.com/showArticle.jhtml?articleID=29102707.

Brunst, P. W. (2008). Use of the Internet by Terrorists – A Threat Analysis. In Centre of Excellence – Defence Against Terrorism (Ed.), *Responses to Cyber Terrorism* (pp. 34–60). Amsterdam: IOS Press.

Brunst, P. W. (2009). Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen. Berlin: Duncker & Humblot.

Buettner, R. (2001). Web of Terror Thrivin on Net. Retrieved April 2008 from http://www.nydailynews.com/archives/news/2001/09/18/2001–09–18_web_of_terror_thriving_on_net.html

Centers for Disease Control and Prevention. (2007). Bioterrorism Overview. From http://www.bt.cdc.gov/bioterrorism/overview.asp

Chen, H., & Larson, C. (2007). Dark Web Terrorism Research. Retrieved April 2008 from http://www.ai.arizona.edu/research/terror/index.htm

Cilluffo, F. J. (2000). Cyber Attack: The National Protection Plan and Its Privacy Implications. Testimony of Frank J. Cilluffo Before the Subcommittee on Technology, Terrorism, and Government Information Committee on the Judiciary on 1 February 2000 [Electronic Version]. From http://www.csis.org/media/csis/congress/ts000201cilluffo.pdf.

Coll, S., & Glassner, S. (2005, 7 August). Terrorists Turn to the Web as Base of Operations. *The Washington Post*, p. A01.

Collin, B. C. (1997). The Future of Cyberterrorism. *Crime and Justice International*, 13(2), 15–18.

Committee on Water Systems Security Research. (2007). *Improving the Nation's Water Security*. Washington, DC: The National Academies Press.

Conway, M. (2002). Reality Bites: Cyberterrorism and Terrorist 'Use' of the Internet (Publication. Retrieved 01.12.2005): http://www.firstmonday.org/Issues/issue7_11/conway/index.html

Davis, J. (2007). Hackers Take Down the Most Wired Country in Europe [Electronic Version]. *Wired Magazine*. Retrieved April 2008 from http://www.wired.com/politics/security/magazine/15–09/ff_estonia.

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In Arquilla, J. & Ronfeldt, D. (Eds.), Networks and Netwars (pp. 239–288). Santa Monica, CA: Rand Corp.

Desouza, K. C., & Hensgen, T. (2003). Semiotic Emergent Framework to Address the Reality of Cyberterrorism. *Technological Forecasting & Social Change*, *70*, 385–396.

Drogin, B. (1999). Russians seem to be Hacking into Pentagon [Electronic Version]. *San Francisco Chronicle Online*, *07.10.1999*. Retrieved April 2008 from http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1999/10/07/MN58558.DTL.

Embar-Seddon, A. (2002). Cyberterrorism – Are We Under Siege? *American Behavioral Scientist*, *45*(6), 1033–1043.

Espiner, T. (2005). Security Experts Lift Lid on Chinese Hack Attacks [Electronic Version]. *ZDNet News*, *23.11.2005*. Retrieved April 2008 from http://news.zdnet.com/2100–1009_22–5969516.html.

FCW Staff. (1999). Russia Hacking Stories Refuted [Electronic Version]. *Federal Computer Week*, *27.09.1999*. Retrieved April 2008 from http://www.fcw.com/print/5_188/news/68553–1.html.

Foltz, B. (2004). Cyberterrorism, Computer Crime, and Reality. *Information Management & Computer Security, 12*(2), 270–295.

Force10 Networks. (2007). Customer Profile: DE-CIX. Retrieved April 2008 from https://www.force10networks.com/company/customer_profiles/profiles-de-cix.asp

Gellman, B. (2002, 27 June). Cyber-Attacks by Al Qaeda Feared. *The Washington Post*, p. A01.

Giacomello, G. (2004). Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism. *Studies in Conflict & Terrorism*, *27*(5), 387–408.

Gleick, P. H. (2006). Water and Terrorism. *Water Policy*, *8*, 481–503.

Graham, B. (2005). Hackers Attack Via Chinese Web Sites [Electronic Version]. *The Washington Post Online*, *25.08.2005*, A01. Retrieved April 2008 from http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html.

Green, J. (2002). The Myth of Cyberterrorism [Electronic Version]. *Washington Monthly*. Retrieved April 2008 from http://www.washingtonmonthly.com/features/2001/0211.green.html.

Harding, T. (2007). Terrorists 'Use Google Maps to Hit UK Troops' [Electronic Version]. *The Telegraph Online*. From http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/01/13/wgoogle13.xml.

ICANN. (2007). Factsheet: Root Server Attack on 6 February 2007. Retrieved April 2008 from http://icann.org/announcements/factsheet-dns-attack-08mar07.pdf

Janczewski, L. J., & Colarik, A. M. (2005). *Managerial Guide for Handling Cyber-Terrorism and Information Warfare*. Hershey, PA: Idea Group Publishing.

Johnson, B. (2008). Nato Says Cyber Warfare Poses as Great a Threat as a Missile Attack [Electronic Version]. *The Guardian Online*. Retrieved April 2008 from http://www.guardian.co.uk/technology/2008/mar/06/hitechcrime.uksecurity.

Kristof, N. D. (2005, 20 December 2005). Terrorists in Cyberspace. *The New York Times*, p. 31.

La Guardia, A. (2005). Al-Qa'eda Launches Voice of the Caliphate Internet News Bulletins [Electronic Version]. *The Telegraph Online*. Retrieved April 2008 from http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/09/28/wirq128.xml&sSheet=/news/2005/09/28/ixnewstop.html.

Leitenberg, M. (2005). *Assessing the biological weapons and bioterrorism threat*. Strategic Studies Institute of the U.S. Army War College.

Lenzner, R., & Vardi, N. (2004). The Next Threat [Electronic Version]. *Forbes Magazine*. From http://www.forbes.com/forbes/2004/0920/070_print.html.

Leppard, D. (2007). Al-Qaeda Plot to Bring Down UK Internet [Electronic Version]. *The Times Online*. From http://www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece.

Leyden, J. (2001). Mass Hack Takes Out Govt Sites [Electronic Version]. *The Register*. Retrieved April 2008 from http://www.theregister.co.uk/2001/01/22/mass_hack_takes_out_govt/.

Miniwatts Marketing Group. (2007). Internet Usage Statistics. Retrieved April 2008 from http://www.internetworldstats.com/

Musharbash, Y. (2004). US-Firmen-Website für Qaida-Botschaft gehackt. *Spiegel Online*, *17.06.2004*.

Musharbash, Y. (2005). Al-Qaida Launches a Weekly News Show [Electronic Version]. *Spiegel Online*. Retrieved April 2008 from http://www.spiegel.de/international/0,1518,378633,00.html.

National Conference of State Legislatures. (2002). Cyberterrorism. Retrieved April 2008 from http://www.ncsl.org/programs/lis/cip/cyberterrorism.htm.

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G. (1999). *Cyberterror: Prospects and Implications*. From http://www.nps.edu/Academics/Centers/CTIW/files/Cyberterror%20Prospects%20and%20Implications.pdf.

OLG Frankfurt a.M. (2006). Lufthansa Online Demonstration. *Multimedia und Recht* 2006, 547–552.

Persson, C. (2006). "Rückfall ins Telefonzeitalter" nach Erdbeben. Retrieved April 2008 from http://www.heise.de/newsticker/Rueckfall-ins-Telefonzeitalter-nach-Erdbeben--/meldung/83007

Pike, J. (2005, 27.04.2005). Eligible Receiver. Retrieved April 2008 from http://www.globalsecurity.org/military/ops/eligible-receiver.htm

Pollitt, M. M. (1998). Cyberterrorism – Fact or Fancy? *Computer Fraud & Security* (February 1998), 8–10.

Record, J. (2003). *Bounding the Global War on Terrorism*. University Press of the Pacific.

Reuters. (2001). This Jihad WEb Site Brought to You by… Visa? Retrieved April 2008 from http://www.usatoday.com/tech/news/2001/09/19/jihad-sites.htm

Rolski, T. (2007). Estonia: Ground Zero for World's First Cyber War? [Electronic Version]. *ABC News*. From http://abcnews.go.com/International/Technology/Story?id=3184122&page=1.

Sedarat, F. (2008). Jihadi Software Promises Secure Web Contacts [Electronic Version]. *Reuters Online*, *2008*. From http://www.reuters.com/article/internetNews/idUSL1885793320080118.

Sieber, U. (2004). The Threat of Cybercrime. In Council of Europe (Ed.), *Organized Crime in Europe: The Threat of Cybercrime* (pp. 81–217). Strasbourg: Council of Europe.

Sieber, U., & Brunst, P. W. (2008). Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions. In Council of Europe (Ed.), *Cyberterrorism – The Use of the Internet for Terrorist Purposes* (pp. 9–105). Strasbourg: Council of Europe Publishing.

Sliva, J., & Ritter, K. (2006). Estonia's Defense Minister Says Kremlin Involvement Possible in Cyberattacks [Electronic Version]. *The Sydney Morning Herald Online*. Retrieved April 2008 from http://www.smh.com.au/news/Technology/Estonia39s-defense-minister-says-Kremlin-involvement-possible-in-cyberattacks/2007/05/18/1178995335698.html.

Testimony of FBI Deputy Assistant Director Keith Lourdeau on "Virtual Threat, Real Terror: Cyberterrorism in the 21st Century", Subcommittee on terrorism, technology and homeland security of the committee on the judiciary United States Senate, 24 February Sess. (2004).

Testimony of James Adams, Chief Executive Officer, Infrastructure Defense, Inc., United States Senate, Committee on Governmental Affairs (2000).

Thornburgh, N. (2005a). Inside the Chinese Hack Attack [Electronic Version]. *Time Online*, *25.08.2005*. Retrieved April 2008 from http://www.time.com/time/nation/article/0,8599,1098371,00.html.

Thornburgh, N. (2005b). The Invasion of the Chinese Cyberspies [Electronic Version]. *Time Online*, *29.08.2005* from http://www.time.com/time/magazine/article/0,9171,1098961–1,00.html.

Traynor, I. (2007). Russia Accused of Unleashing Cyberwar to Disable Estonia [Electronic Version]. *The Guardian Online*, *17.05.2007* from http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

Tsfati, Y., & Weimann, G. (2002). www.terrorism.com: Terror on the Internet. *Studies in Conflict & Terrorism*, *2002*(25), 317–332.

Vargas, J. A. (2006). Way Radical, Dude [Electronic Version]. *The Washington Post Online.* From http://www.washingtonpost.com/wp-dyn/content/article/2006/10/08/AR2006100800931.html.

Vatis, M. A. (2001). *Cyber Attacks During the War On Terrorism: A Predictive Analysis*. Retrieved April 2008 from http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf.

Weimann, G. (2004a). Cyberterrorism: How Real is the Threat? [Electronic Version]. *Special Report (United States Institute of Peace)*, *119*.

Weimann, G. (2004b). www.terror.net. How Modern Terrorism Uses the Internet [Electronic Version]. *Special Report (United States Institute of Peace)*, *116*.

Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism*, *28*, 129–149.

Weimann, G. (2006). *Terror on the Internet*. Washington, DC.

White, J. R. (1990). *Terrorism – an Introduction*. Pacific Grove, CA: Brooks/Cole Publishing Co.

Wilson, C. (2005). *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (Vol. RL32114). Washington, DC

http://www.springer.com/978-0-387-89290-0

A War on Terror?
The European Stance on a New Threat, Changing Laws and Human Rights Implications
Wade, M.; Maljevic, A. (Eds.)
2010, XV, 554 p., Hardcover
ISBN: 978-0-387-89290-0