Justitie

Ministerie van
Binnenlandse Zaken en
Koninkrijksrelaties

National Coordinator for Counterterrorism (NCTb)

Jihadis and the internet

PREFACE

Combating terrorism is one of the most important topics in international and national security policy. The Dutch National Coordinator for Counterterrorism (NCTb) is responsible for development of policy, analysis of (intelligence) information and direction of the security measures to be taken towards combating terrorism. It is extremely important, in order to face up to present-day threats of terrorism, to keep abreast with the most recent developments. After all, terrorists themselves are cunning in their use of the most modern technologies and communication media. Needless to say, the Internet plays a substantial part in this.

Jihadi terrorists and radicals (jihadis) make significant use of the Internet as a resource. One of the consequences is that the Internet is an important platform for radicalisation and can even serve as a virtual training camp. Jihadis not only use the Internet as a resource, however, but can also attack the Internet itself with terrorist activities (the Internet as a target) or use the Internet against other targets (the Internet as a weapon). It is essential to gain insight into these forms of Internet usage for the purpose of counter-strategies as well as security issues. This in-depth study "Jihadis and the Internet" provides that insight.

In its analytical role, the NCTb issues numerous products which, at the strategic level, are of great importance in combating terrorism. One of these products is the Terrorist Threat Assessment Netherlands (DTN), a national analysis which is issued four times each year. The NCTb also produces in-depth studies such as this one, comprising a more thorough investigation of a specific phenomenon. The present study has been realised on the basis of an investigation of the literature, interviews, monitoring of the Internet and an expert meeting on the topic of "The Internet as a target and a weapon". The results of this meeting - which brought together investigators, government services and private parties from the anti-terrorism, telecoms and Internet sectors - form an important cornerstone for this study.

I would express the hope that this study will provide other government organisations - and certainly private partners - with some starting points for averting the threat from this type of Internet usage by jihadis. The ways in which terrorism manifests itself and the nature of the Internet mean that this is not straightforward. At all events, the NCTb will be using the findings from this investigation in order to develop further measures, in conjunction with others, in order provide effective resistance to the terrorist threat.

The National Coordinator for Counterterrorism
T.H.J. Joustra

TABLE OF CONTENTS

SUMMARY

Jihadi terrorists and radicals (jihadis) make extensive use of the Internet. It is most important to understand this for counter-strategies and for security issues in the context of counter-terrorism. This in-depth study, which results from a global and wide-ranging orientation by the NCTb, attempts to provide such an understanding. A distinction is drawn between use of the Internet as a target and a weapon (Part A) and the Internet as a resource (Part B).

A The Internet as a target and a weapon

When the Internet is a target, terrorist activities are aimed at the Internet itself and its infrastructure. This might, for example, involve connection facilities (server parks), functionalities and connection lines for the Internet, or those organisations who provide services that are crucial to the operation of the Internet. An attack or strike against the Internet can take various forms:

- a cyber attack using computers via the Internet; in such a case, the Internet is both target and weapon: the Internet turns against itself;
- a physical attack using conventional weapons or sabotage campaigns as inside jobs;
- an electromagnetic attack using, for example, electromagnetic energy sources;
- indirect attacks or strikes, for example against the power supply or cooling facilities.

When the Internet is used as a weapon, attacks are committed against physical targets via the Internet. This might, for example, involve taking over air traffic control systems or management systems for vital installations in the chemical or power supply sectors.

The use of the Internet "as a target and a weapon" is a regularly recurring theme in the media, frequently being referred to as cyber-terrorism. Opinions vary markedly in the - largely international - media regarding the extent to which this amounts to a terrorist threat. Some reports appeared in early May 2006 concerning the simplicity with which a (terrorist) attack/strike could be mounted against the Internet in the Netherlands. These are all good reasons to devote some attention to this issue in the present in-depth study. Precisely because relatively little has been written on the Dutch situation, as knowledge about that situation is quite fragmentary, the NCTb organised an expert meeting with representatives from the intelligence services, academia, police, other government services and the telecoms and Internet sector. The threat has been assessed from a variety of angles of approach in this study, and this has led to three conclusions.

A1 Cyber attacks by jihadis *against the Internet* are unlikely

A cyber attack against the global or Dutch Internet itself[1] is not considered likely at this point. While a cyber attack involves a lower threshold than, for example, suicide attacks, so that there is a potential for larger numbers of jihadis being willing and able to undertake them, the most significant disadvantages for jihadis are that disrupting the Internet would also affect the jihadi infrastructure on the Internet, and it would not appeal to their sense of martyrdom. Also, a successful cyber attack is not a realistic possibility, primarily as a consequence of the measures already taken against this. If we were to expect a cyber attack, then it would be a small-scale attack for a limited period, or else a coordinated combination of small-scale cyber attacks.

A2 Other types of attacks by jihadis *against the Internet* are unlikely

Any other type of attack against the Internet, such as the physical attack mentioned above, is also considered unlikely at this point. Neither the Dutch nor the global Internet would actually be disrupted by such an attack. There may well be opportunities for small-scale attacks, but on the other hand steps have been taken to minimise the chances of this and to restrict the effect it would have. While this type of attack appears to be more probable than a cyber attack, it is certainly worth wondering whether terrorists would not prefer, for example, a bomb attack on a soft target instead of on an important Internet locale.

A3 Cyber attacks *via the Internet* are unlikely

An attack via the Internet, with the Internet operating as a weapon against other targets, may well be foreseeable, but is unlikely at this point. There are nevertheless opportunities for this, resulting from vulnerabilities in, for example, software for process management (SCADA) used by a variety of sectors. In addition, this has some attractive facets for jihadis, but such attacks require a great deal of (insider) knowledge as a rule. Classic attacks, such as bomb attacks or suicide attacks, can also be better exploited for publicity purposes. A combination of one or more classic attacks, deploying the Internet as a weapon, appears more probable. This would amplify the effect of such an attack.

B The Internet as a resource

Just like ordinary citizens, jihadis use the Internet for a variety of purposes and regard the Internet as being a crucial resource for jihad. Our in-depth study looked at various forms of Internet use, and at the Internet's influence on radicalisation, leading to the following conclusions.

B1 Propaganda via the Internet contributes towards radicalisation

Propaganda is disseminated professionally via the Internet, with great penetration and relatively little by way of contradiction. The propaganda is not restricted to one-way traffic: the jihadis actively attempt to enter into two-way communication with interested parties. When combined with the fact that it is primarily large groups of youngsters who have access to the Internet and use it intensively, it becomes clear that this ends up being a breeding ground for (further) radicalisation. This is certainly the case for young Muslim women, because of the attraction of the Internet for them (demand side) when combined with the active role of radical young Muslim women on the supply side.

1 Although the Internet is global, it is still possible to speak of the "Dutch Internet" to a certain extent. See, on this, paragraph 2.3.

B2 Acquisition of information via the Internet potentially contributes towards the commission of terrorist activities

The Internet forms an inexhaustible source of information for jihadis, as it does for everyone else. In particular, developments in the area of (real-time) satellite pictures, potentially combined with an Internet connection, as in the case of GoogleEarth, are making rapid progress. This further increases the opportunities for the acquisition of information by jihadis.

B3 Fundraising via the Internet by and for jihadis is still quite limited: a shift towards more covert fundraising can be expected

There are potentially many opportunities for fundraising by and for jihadis, and we are aware of some instances, but it is not yet a common phenomenon in practical terms. This form of fundraising is, after all, fairly conspicuous and therefore vulnerable to government intervention. As Internet banking becomes more and more straightforward and commonplace, use and abuse of this facility by jihadis will also undoubtedly increase. Combined with the increasing interest of hackers in online fraud, this may lead to a shift from more public to more covert fundraising. Fundraising via the Internet may also increase as a result of new digital and anonymous payment facilities.

B4 Use of the Internet results in more interactive forms of recruitment, which cannot yet be easily identified, and also in conscription and self-ignition

It is not really like that anyone from the Netherlands would allow himself or herself to be recruited directly by recruiters from international terrorist groups, on a one-to-one basis, via the Internet. This is not to ignore the fact that, for example, the core of Al Qaeda might have an inspirational impact, but it would be going too far to call this recruitment. A markedly *interactive* form of *recruitment* is, however, perceptible on the Internet, associated with the interactive methodologies of creating propaganda. Another characteristic of the Internet is that potential warriors, in particular, are willing to sign up for participation in a violent jihad *(conscription)*, which fits in ideally with the nature of the Internet. There can also be self-ignition in relation to the Internet, where someone might decide to embark on a jihad on his or her own initiative, and where it is impossible to distinguish between two different parties. If it is difficult in the physical world to distinguish between the transition from the radicalisation process to recruitment, on the one hand, and conscription on the other hand, then this is undoubtedly the case with Internet. The question perhaps ought to be whether the rise of the Internet means that the classic recruiter/recruit concept still persists, or

whether it is gradually being replaced by a permanent and interactive mix of top-down and bottom-up information provision and acquisition, mixed with online encouragement, steering or network formation.

B5 Use of the Internet for training purposes has the effect of weakening the threshold against the commission of attacks

Being prepared to carry out terrorist activities is one thing, but having the knowledge, skill and resources to do so is just as important. For "home grown terrorists" in particular, the readily available training material may contribute towards converting intentions into actions as regards carrying out terrorist attacks. Dissemination of training material via the Internet by jihadis also contributes towards a speedy dissemination of doctrine.

B6 Jihadis use the Internet for mutual communication and planning

There are sufficient indications that jihadis communicate among each other and plan terrorist activities via the Internet. In doing so, they make use of the opportunities for anonymous and secretive communication. As well as having benefits for jihadis, this usage of the Internet offers security and protection agencies the opportunity to intervene. The jihadis are very well aware of this.

B7 Virtual networks increase the force of the jihadi movement

An informal pool of those ready and willing to undertake the jihad is formed as a result of the formation of virtual networks, and they can develop violent activities either on their own or in varying combinations with each other. This allows local and international elements to become intertwined with each other.

B8 Use of the Internet sustains the entire process of radicalisation

Every phase of radicalisation requires an element of supply. Using the Internet, a potential jihadi can undergo processes of formulation and strengthening of ideology as well as ideological indoctrination. We would, however, like to see further academic investigation into group processes via the Internet, and the influence of Internet usage on radicalisation.

B9 From the perspective of radicalisation, the greatest threat arises from propaganda spread via the Internet, combined with the relatively large group of young Muslims looking for information

Propaganda is disseminated professionally and interactively, with great penetration and relatively little by way of contradiction. If we combine this with the potentially substantial target market of vulnerable young people, then it is clear that propaganda via the Internet makes the largest contribution to (further) radicalisation, more so than other forms of Internet usage.

B10 From the perspective of terrorism, the greatest threat arises largely from the (facilities for) creation of virtual networks and the use of the Internet for training purposes

If virtual networks primarily increase the force of the jihadi movement, then - for "home grown terrorists" in particular - the readily available training material may contribute towards a conversion of intentions into actions in relation to the perpetration of terrorist attacks.

1

1.1 BACKGROUND

The Internet can no longer be ignored in present-day society. It creates numerous opportunities for commercial life, the government and citizens, but it also has its dark side. The Internet is, after all, used to a large extent as a resource by jihadi terrorists and radicals, and has thus become an important platform for radicalisation, even serving as a virtual training camp. Jihadis not only use the Internet as a resource, but they can also direct terrorist activities against the Internet itself (the Internet as a target) or via the Internet against other targets (the Internet as a weapon). An understanding of these forms of Internet usage by jihadis is therefore of considerable importance for the formulation and evaluation of policy in relation to counter-terrorism. This in-depth study, which results from a global but wide-ranging orientation by the NCTb, attempts to provide such an understanding.

1.2 AIM, RESEARCH QUESTIONS AND LIMITATIONS

The primary aim of the study is to obtain an outline understanding of Internet usage by jihadis, along with the threat this poses, for an assessment of potential measures to avert the threat. The secondary aim is to identify topics requiring further analysis and/or research.

The research questions, derived from these aims, are:

1. How and to what extent are terrorist and radical jihadi networks, groups and individuals concentrating their efforts against the Internet and using the Internet?
   - How and to what extent do they choose the Internet as a target?
   - How and to what extent do they use the Internet as a weapon?
   - How and to what extent do they use the Internet as a resource?
2. How and to what extent does the Internet influence radicalisation?
3. To what extent do (any forms of) Internet usage pose a threat to Dutch society, and what does that threat consist of?

As is evident from the aims and research questions, the study focuses primarily on *jihadi terrorism* and *jihadi radicalisation*, sometimes also referred to as islamist terrorism and islamist radicalisation. Unless we indicate otherwise, no distinction is drawn between these and, for ease of reference, we employ the term “jihadis”. In some cases we shall also address the wider manifestation of terrorism, if only because this distinction is not always made in the literature. Definitions of expressions can be found in the table of definitions at the end of the study.

The broader use of the Internet by criminals of varying plumage (cyber crime) has been left out of consideration. There is accordingly no discussion of the presence and dissemination of depictions of child pornography on the Internet, the many manifestations of fraud and

swindling, the spreading of viruses, spyware and suchlike, unless they are specifically related to terrorism and radicalisation. Nor is there any discussion of use of the Internet for economic and industrial espionage, military purposes (cyber war) or its use by all manner of political activists.

The study also focuses on the Internet itself, and not on the broader areas of information communication technology (ICT) and new media. We do not, therefore, deal with the use of, for example, satellite and mobile telephones by jihadis or the use of satellite transmitters. While these topics are definitely related, the Internet itself is such a complex and comprehensive area of study that this was a conscious choice.

A further limitation is that the study focuses primarily on the Netherlands, although this is not always straightforward or sensible, bearing in mind the nature of the Internet. As a matter of principle, we paid no attention to the technical side of the Internet, for example the technical protocols employed, unless this was absolutely necessary to understand its use. Nor did we focus on specific criminal acts or offences. Our primary area of study has been the trinity of target, weapon and resource.

1.3 EXPLANATION OF WORKING METHODS

The phenomenon of Internet usage by jihadis is so large, dynamic and complex, that its study might involve work for many researchers over a number of years. As indicated above, we opted for a global, albeit wide-ranging orientation, based on which further follow-up research might be carried out. We accordingly opted for four research methods, namely: 1) interviews and background talks, 2) a study of literature, 3) an exploration of usage on some Dutch language websites and forums, and 4) an expert meeting.

Seven interviews were conducted with institutions in the Netherlands involved in the phenomenon of the Internet in a general sense. We also held some background discussions. Both the interviews and the background discussions were processed anonymously. The authors also took part in symposia and processed the findings from these.

Our study of literature was focused on academic literature and other public sources. An exhaustive exploration of the literature was made regarding Internet usage by terrorist groups and jihadis. This involved predominantly foreign literature written from an international perspective. Literature specifically tailored to the Dutch situation is relatively scarce. This is hardly surprising, bearing in mind that the Internet and Jihadism are primarily international in nature.

A meeting of experts was organised by the NCTb on 20 June 2006 in the context of the study, where researchers, government services and commercial representatives from the counter-terrorism, telecoms and Internet sectors were brought together to deal with the central issue of "The Internet as a target and a weapon". The results of this expert meeting are dealt with in chapter 2.

There are various ways of categorising Internet usage by jihadis from the perspective of the aims they are contemplating (see appendix 1). The NCTb opted for the following allocation at an early stage, taking account of aspects mentioned by others:

A the Internet as a target;
B the Internet as a weapon;
C the Internet as a resource, further subdivided into:
- Propaganda;
- Acquisition of information;
- Fundraising;
- Recruitment;
- Training;
- Mutual communication and planning; and
- Creation of virtual networks.

1.4 EXPLANATION OF THE STRUCTURE OF THE REPORT

Chapter 2 analyses the Internet as a target and a weapon, and chapter 3 analyses it as a resource. Chapter 4 presents our conclusions. The report concludes with a bibliography, terminology list and some appendices.

2

THE INTERNET AS A TARGET AND A WEAPON

2.1 INTRODUCTION

The Internet as a target and a weapon is frequently referred to using the term *cyber-terrorism*. While this may well be an expressive and popular term for the threat from "cyberspace", it is also at the very least ambiguous, with a number of potential definitions. It should not be so surprising that there are a variety of definitions for cyber-terrorism. The same applies to terrorism. If we want to use the term "cyber-terrorism", then the very least we have to do is to correlate it with the definition of terrorism commonly used in the Netherlands, i.e.:

> *The commission or threat of violence against at human life, or the commission of serious socially disruptive material damage, with the aim of causing social change or influencing political decision-making.*[1]

Intention is at the very heart of this definition, namely the aim of causing social change or influencing political decision-making. Serious consequences must also be involved. The authors are unaware of any definition of cyber-terrorism that adequately reflects this factor. These definitions are accordingly not suited to the Dutch situation on a one-for-one basis. There is also a further reason why the term "cyber-terrorism" causes problems for this study. Cyber is the prefix of the word "cybernetics", which means operation by means of automatons or computers. Cyber therefore actually means "through the use of computers". Since our study is focused specifically on the Internet and not on the wider use of computers, the term cyber terrorism is more confusing than enlightening. These are the two reasons why we have opted for "the Internet as a target" and "the Internet as a weapon", proceeding from the basic definition of terrorism indicated above. As far as the Internet as a target is concerned, what is involved is an attack against (the infrastructure of) the Internet, and for the Internet as a weapon this involves an attack via the Internet against physical targets, such as vital infrastructure or online service provision, such as Internet banking.

2.2 BACKGROUND

2.2.1 Explanation

In this section, we will first of all devote our attention to the history of the Internet and some of its aspects that are significant to what follows in this chapter. We will then explore some methods that the jihadis might employ for an attack against or via the Internet. An attack can take place by massively overloading the Internet or networks linked to it, with the underlying aim being the disruption or even the complete collapse of the operation of these computer networks. Another method is to take over or manipulate networks, databases and management systems by targeted hacking. Both of these methods, *mass overload attacks* and *targeted hacking*, will be explained separately. The application of either method requires hacking skills and/or familiarity with hacking, or access to the hacking community. In a short, separate section, we will deal briefly with

1 This is the AIVD definition, also used by the NCTb and based on the EU framework decision.

the issue of whether there are any indications that jihadis have already used or intend to use these methods.

2.2.2 The Internet

The Van Dale dictionary describes the Internet as "a worldwide network of computers by which information can be exchanged". It is probably better to describe the Internet as a worldwide network of computer networks. At its heart, the Internet is a communication environment or medium, and also an inexhaustible source of information. In addition to a technical dimension, namely the networks that are connected to each other across the world, the Internet has a separate dimension of all manner of communication services and resources, including the worldwide web (www) and e-mail. Internet also has a further social dimension: numerous social communities exist on the Internet, and governments, social groupings and obviously businesses make full use of these. There are some organisations whose only existence is online.

The history of the Internet goes back to the 1960s, at the height of the Cold War. A need arose at the time for a computer network to ensure that the American army command structure could not be disabled at a single stroke. What was required was a network of computers that would be immune to enemy attacks, and that in any event could not be completely disabled during a single attack or through sabotage at a single location. The American Ministry of Defence accordingly developed the experimental ARPANET (Advanced Research Projects Agency Network), which - unlike other computer networks - did not use a single master computer. This computer network had to be both flexible and reliable. The choice was therefore made for "packet switching".[2] A substantive message is contained in an electronic envelope (packet), which is sent from the issuing computer to the final destination(s) along a variety of routes. This does not involve a fixed route or a direct connection between the sending and receiving computers. Large messages are divided into several packets and provided with an address and a sequential number, so that the message can be reassembled at its final destination. Later developments, including the connection of more and more networks and the Ministry of Defence withdrawing as a sponsor, opened up the ARPANET for non-military and scientific purposes, with it also being renamed as "the Internet". The Internet is international; there are no national boundaries and there is no owner. This is all the result of the open architecture of the networks, meaning that anyone with suitable equipment and software can connect to it.[3]

2 There are 2 communications standards/protocols underlying the Internet, namely the Internet Protocol (IP) and the Transmission Control Protocol (TCP), collectively referred to as TCP/IP. The IP determines that: (1) every connection point on the Internet has an Internet address; (2) all messages are divided into information packets; (3) every message packet is sealed in an IP envelope; and (4) the outside of the envelope shows the address of the sending computer and addressee(s). The TCP and other protocols operate immediately above the Internet Protocol. TCP divides large messages into several packets, reassemble these at the final destination and has facilities for "repairing" damaged packets. Bang et al 1996, p. 13-19, information from TNO employee.

While the Internet can be categorised in various ways, the relevant distinction for this study is the various layers of Internet. These are:

- the application layer of the Internet services, such as surfing, e-mails, Internet telephone (Voice over Internet Protocol - VOIP), etc;
- the layer with essential services for the operation of Internet itself, including the conversion of a logical Internet address such as 'google.nl' into an IP address;
- the transmission layer underlying Internet traffic, such as various types of networks, cabling, et cetera.[4]

These layers are extensively interwoven.

It is likely that Dutch society's dependence on Internet will continue to increase. The opportunities are almost limitless, and new applications appear every day, so that the Internet and the physical world become more and more absorbed in each other as time passes. Thus the Dutch government, and certainly the Dutch Tax & Customs Authority, are actively involved in offering services via the Internet. Also, the infrastructures of the Internet, radio, telephone and television are growing closer together. Examples of this are the ability to telephone via the Internet, and the large-scale availability of television via the Internet. If one of the so-called "triple play" providers were to drop out of the picture, this would potentially have three times the number of consequences. Remote access to commercial information, management systems and the Internet itself is also likely to continue to increase. Illustrations of this, for example, include the facility for accessing the Internet at some Dutch railway stations and the facility of connecting to the Internet while on board aircraft.
New developments in the area of mobile telephony (UMTS) are also playing a part, as are the development of GPS, traffic information and control systems in road vehicles[5], and virtual medical consultations via webcams. There is a growing need for increased bandwidth among users, and suppliers are providing this. As a result of these developments, it is logical that the opportunities for abuse also increase, as well as the complexity of doing anything about this. The developments themselves appear to be outrunning attention to the vulnerability of the Internet.[6]

2.2.3 Mass overload attacks

Cyber attacks against or via the Internet are possible through an overload of the computer systems that facilitate the websites and other provisions on the Internet. This could be compared with the situation if everyone in the Netherlands were to call 112 at the same time. The telephone network would be overloaded and it would be impossible to reach the emergency services. A similar effect can be achieved on the Internet by having a large number of Internet-connected computers demanding access to a website or some other random online service at the same time. The most commonly used method for these mass demands is that individuals or organised groups of individuals gain unlawful access, in a fully computerised manner via the Internet, to many thousands (or even hundreds of thousands) of computers. This frequently happens without the knowledge of the owners of those computers, who in some cases may not

3 Weimann 2006, p. 16-20, Bang et.al. 1996, p. 13-36, Huizer 1998. For an extensive history of Internet, see for example http://www.isoc.org/internet/history/.
4 Thiele & Van Vliet 2005.
5 Luiijf 2006.
6 According to Thiele & Van Vliet 2005.

have made their own computers secure. The computers controlled in this way can then be deployed as a single weapon. It is called a "botnet", a network of hacked computers (robots).

Mass overload attacks are frequently referred to by the (collective name of) DoS attacks.[7] Such attacks have taken place and continue to take place regularly and they are sometimes successful. In February 2000, websites such as "Amazon.com", "eBay" and "Yahoo!" were disconnected for a few hours.[8] In the Netherlands, sites such as "regering.nl" were affected by this type of attack in October 2004. It is estimated that 4,000 overload attacks are undertaken every week.[9] There are many programs in circulation allowing a DoS attack to be undertaken, using the zombies or bots described above, which can cumulatively amount to a botnet. This type of botnet can also grow spontaneously by automatically localising and infecting other vulnerable computers. This has a larger impact, because more computers are looking to contact a particular server at the same time. It is also more difficult to trace the attacker, because the programme does not run directly from the attacker's computer. This does not preclude the attacker from being traced at the end of the day.

DoS attacks are aimed at affecting the availability of Internet. In addition to DoS attacks, viruses and worms can also ensure this type of disruption to Internet traffic. There have been fewer major outbreaks of viruses in recent times. This does not mean that there is no danger of this happening. The advanced viruses (and other pernicious software, or malware) appear to be aimed less at disruption of the entire Internet traffic and Internet availability, and more aimed at causing targeted damage or theft of information, affecting the reliability and integrity of the Internet and online (exchange of) information. The present threat of overload attacks appears to be principally related to DoS attacks.

2.2.4 Targeted hacking

Hacking is a broad term for breaking into computer systems or networks. Hacking can be effected by various techniques, including guessing passwords, exploitation of gaps in software security or the use of poorly configured computer systems.

A fundamentally thorough knowledge of existing systems and ICT security is required to succeed with a targeted and serious hacking attempt. A specific hacker tool will often have to be written in order to achieve the desired result, and this involves considerable prior reconnaissance, devotion and tenacity. It is certainly not the case that a secured system can be taken over at any old time. System managers also have the necessary windows of opportunity for discovery, because hackers still need time to roam around the system, leaving a trail behind them.

7 Various types can be distinguished: (1) the Denial of Service attack (DoS attack); (2) Distributed Denial of Service attack (DDoS attack); and (3) Distributed Reflection Denial of Service (DRDoS attack). Under a DRDoS attack, the network infrastructure servers (which manage world-wide Internet traffic) are involved in an attack. The servers are not taken over or infected like zombies, but used as a conduit for accumulation. This means that the enormous server complexes for search engines like Google and Yahoo become involved in this type of attack without being aware of it. This type of attacker is more difficult to localise and detect, as is discussed in Gibson, 2002.
8 Weimann 2006, p. 157.
9 Benschop 2006b.

2.2.5 Computer knowledge and skills on the part of jihadis

Looked at as a whole, jihadis are far from behind the West when it comes to the use of computers and the Internet. It is worth noting, for example, that Khalid Sheik Mohammed (one of the planners of the attacks on 11 September 2001) was involved in chats with those committing the attacks[10] and that Ramzi Yousef (responsible for the first attack on the World Trade Centre in 1993) was even then using advanced encryption.[11] The attackers of 11 September 2001 and Madrid in 2004 were quite clever in the use they made of the facilities offered by computers, for example working with the concept of the e-mail dead-letter box. By opening up a Hotmail account, where several users had the password, draft e-mail messages could be left behind in the "draft folder" and these could be looked at and changed by anyone with the password. This significantly reduced the risk of discovery. In addition, the jihadis have mastered the art of disseminating propaganda via the Internet more than anyone else. The general computer skills required for this are widely available. More than that, however, they use skills for these activities that could be classified as "basic" hacking: hijacking web space and websites in order to promote their own jihadi material.[12] All in all, it can certainly be said that terrorist groups and jihadis have sufficient knowledge concerning computer use, and they also have the resources. However, in addition to hacking aimed at propaganda, are there other examples to show that jihadis have the knowledge, resources and intention required for hacking?

We are aware of various examples of hacker groups that are enlightening in the context of the virtual jihad. For example there are hacker groups who have declared themselves to be associated with Al Qaeda or the worldwide jihad. These hacker groups have names such as the *Qaeda Alliance Online* - since 9/11 - the *OBL Crew*, the *Islamic Hackers* and the *Afghan Hackers*.[13] The *World's Fantabulous Defacers* (WFD) have 334 recorded defacements to their name between 20 November 2001 and 21 March 2002, from a pro-Palestinian perspective. Their primary target was the election campaign site of Ariel Sharon. Following a successful defacement, Sharon was presented as a criminal, and horrifying photographs of a scarred child were placed on the site.[14] There were also a great many hacking activities between pro-Israeli and pro-Palestinian hackers.[15] Various hackers were active following 9/11 in the name of Bin Laden.[16] Despite this example, and the warnings of cyber and hacking attacks after 9/11 and in the wake of the of Afghanistan, there was no evidence of an increase in hacking activities.[17]

Jihadi websites devote ample space to hacking. The *Muslim Hackers Club*, whose website was not, in fact, updated after 1999, contained a virus tutorial for hackers. It contained standard hacking tools that just happened to be available in a cyber-Islamic environment. One of the discussions on the site at the time did not indicate that there should be any aggressive hacking.[18] There is also ongoing discussion in other chat rooms concerning hacking. Is it appropriate within Islam? Is it criminal?

10 CRS 2005a, p. 18.
11 Benschop 2006b.
12 See on the question of propaganda, chapter 3, paragraph 3.4.
13 Weimann 2006, p. 170.
14 Bunt 2003, p. 45.
15 Bunt 2003, p. 48 et seq.
16 Bunt 2003, p. 54.
17 Bunt 2003, p. 55.
18 Bunt 2003, p. 38-39.

Visitors to the site and administrators were concerned about the criminal aspects and the risk of getting caught (with some examples of this being mentioned).[19] Many jihadi forums also contain a section entitled "electronic jihad", with discussion of hacking methods in addition to the waging of a propaganda war.[20] Specific targets discussed on Al Qaeda related web sites included the American Centers for Disease Control and Prevention in Atlanta, FedWire (electronic money transfer) and facilities governing the flow of information via the Internet.[21]

Figure 2.1 An example of attention for hacking

Islam Online produced an online fatwa indicating that hacking was only acceptable if you had suffered a personal attack by way of hacking.
Attacking web sites with content hostile to Islam is, however, permitted according to a different fatwa, discovered in 2002: "if [...] websites are hostile to Islam and you could [en]counter its evilness with goodness; And respond to it, refute its falsehood, and show its void content; that would be the option. But if you are unable to respond to it, and you wanted to destroy it and you have the ability to do so, it's ok to destroy it because it is an evil website."
Following this last-mentioned fatwa, FBI and Pentagon sites were attacked by Saudi hackers.[22]

The Global Islamic Media Front (GIMF) had in the meantime started to formalise and disseminate a 74 page compendium of hacking methods and opportunities. The new GIMF compendium (partly based on work by the jihadi hacker Irhabi007, who was arrested in the United Kingdom) also contains the compressed software files required to crack passwords and uncover security leaks. The compendium is actively distributed via jihadi forums and websites. The list of vulnerable sites contained in the compendium also includes a Dutch site.[23] We would like to make two comments concerning this compendium. Firstly, the material is out of date. This does not, however, alter the fact that some computers, networks and websites are still vulnerable to this type of technique. Secondly, and more importantly, the compendium is aimed at the exploitation of weaknesses in networks and websites so as to be able to publish and distribute material free of charge. All things considered, therefore, this compendium could well be described as "propaganda". This does not detract from the fact that the broad distribution of the material that would undoubtedly be achieved through the activities of the GIMF might well inspire other radical or jihadi individuals to go one step further than hacking for the purpose of distributing material. The same applies to the potential effect of specific parts of jihadi web forums.

If the jihadis were insufficiently skilled and resourced for hacking - although there is no reason to assume that this is the case - they would be able to hire hacking expertise. As far as collaboration with non-jihadi hackers is concerned, it is worthwhile mentioning an attempt in 1998 by the Pakistani Harkat-ul-Ansar organisation (considered by the US to be associated with Osama Bin Laden) to buy software from hackers.[24] There are highly

19 Bunt 2003, p. 45.
20 Rogan 2006.
21 Weimann 2006, p. 113.
22 Bunt 2003, p. 46, Weimann 2006, p.122.
23 Site Institute 2006b.
24 Benschop 2006b.

educated ICT specialists available to be hired, particularly in the former Soviet Union and on the Indian subcontinent, with some of the specialists having difficulty in obtaining any legal paid work.[25] These "hired hands" are frequently unaware of whom they have been hired by or indeed the purpose of their work. True hackers are concerned with the challenge, and not the background of those who challenge them to do something that should in fact be impossible. A digital break-in at a firm such as Boeing, combined with the pilfering of blueprints or other information about aircraft, might then be the ultimate challenge. The question of who is actually interested in them (and whether he is who he says he is) is much less interesting. Certainly for young hackers, it may be difficult to distinguish between the various individuals who are interested in their skills.[26] For the more criminally-minded hackers, it's also no more than a question of strictly "business".[27] It is also imaginable that hackers undertake activities for a terrorist organisation because they want to be accepted by that organisation since, in a general sense, they sympathise with the organisation's ideology (for example anti-American or anti-Western), or their activities might allow them the chance to take revenge on, for example, former employers or particular businesses. These hackers need not, by definition, fit any standard profile but may also have alternative sympathies.[28] The question remains as to whether the average hacker actually wants to contribute towards terrorist activities.
A report from 1999 alleges, in any event, that hackers are not "suited" to terrorism in a psychological or organisational sense[29] and one of the documented examples shows that, after September 2001, some hackers were very concerned that they might have unwittingly contributed towards the attacks in the USA, as they had risen to the challenge of gaining access to specific information from the aviation industry.[30]

Two FBI key figures have indicated that the technical competence of terrorists is on the increase. Terrorists also demonstrate that they have a greater knowledge of the critical role of information technology in the United States economy, and are fine-tuning their recruitment accordingly.[31] Al Qaeda and Hezbollah are becoming more and more confident in Internet and computer technology, and these groups apparently have the intention and desire of developing the skills required for a cyber attack.[32]
The next generation of terrorists is growing up in the digital world, but the same applies to system managers and government organisations. Who will ultimately benefit from this cannot yet be predicted, but it is likely that terrorists will be able to act more flexibly, as they do not have to deal with long lines of decision-making and can take their time to look for mistakes. Terrorist organisations also have modern equipment available.[33]

25 Wilson 2006, p. 84.
26 Mitnick 2006, p. 23-47.
27 Interview 2.
28 Interview 3.
29 Weimann 2006, p. 2006, p. 167, referring to Denning, Cyber-Terror: Prospects and Implications, 1999.
31 Mitnick 2006, p. 23-47.
30 Mitnick 2006, p. 23-47.
31 CRS 2005b.
32 Wilson 2006, p. 78, based on Dan Verton in Black Ice, who analyses a CIA brief to the US Senate Select Committee on Intelligence from April 2002.
33 Interviews 1 and 2.

2.3 THE INTERNET AS A TARGET

2.3.1 Explanation

Our society is becoming steadily more dependent on the Internet. This dependency, and its associated vulnerability, might persuade jihadis to regard the Internet itself as a target to be singled out for terrorist activities. These might take a variety of forms:

- a cyber attack using computers via the Internet. In such a case, the Internet is both target and weapon: the Internet turns against itself;
- a physical attack using conventional weapons or sabotage campaigns from within against (core) connection points, core functionalities and lines of connection, or the organisations providing services crucial to the operation of the Internet.
- an electromagnetic attack using, for example, electromagnetic energy (EMP) against (core) connection points, core functionalities and lines of connection.
- indirect attacks or strikes, for example against the electricity supply or cooling provisions, so that the Internet (or its infrastructure) can no longer function.[34]

Because this study is focused on Internet usage by jihadis, our focus is on cyber attacks with terrorist intent. This does requires further demarkation. We are excluding cyber attacks intended to make a political statement (so-called *"hacktivism"*). The definition of terrorism does not cover either the intention or the consequences of these. An appropriate term for these attacks might well be 'Weapons of Mass Annoyance'.[35]

Figuur 2.2 Examples of hacktivism

In 1997, the ETA service provider, based in San Francisco, was bombarded with e-mails designed to take the ETA web pages offline (which actually occurred a couple of days later).[36] *After what was described as the Danish cartoon issue, Danish websites were defaced, resulting in the Danish government sites also being inaccessible.*

2.3.2 Possible cyber attacks, vulnerabilities and defences

The Internet was originally developed as a network of computers that would be immune to enemy attacks, and that in any event could not be completely disabled during a single attack or through sabotage at a single location. Despite that, the Internet does, of course, have core junctions, connection points and functionalities, which undoubtedly make it vulnerable to a certain extent. One potential vulnerable point for cyber attacks is to be found in the *Domain Name Servers* (DNS-servers). These operate more or less as telephone directories in reverse: they search for the unique IP numbers belonging to computers, Internet and e-mail addresses. This is a layered structure with 13 root servers at the top, for what is termed the IPv4 protocol, and five for the newer IPv6 protocol, along with duplicates of them. A limited number of these are situated in the Netherlands.[37] There is also a DNS server for the Netherlands territory, and providers and major organisations have their own DNS servers within the Netherlands (as is the case in other countries). Another potentially vulnerable point consists of the so-called Exchanges. We may compare these with a major railway station. Many train lines converge at the station and passengers coming from different directions can change trains and choose a new direction. Destinations can also be reached by different routes, however. The station has facilities for regulating the flow of passengers, and traffic management arranges for actual transport movements.
One of the important exchanges in the Netherlands is the AMS-IX (Amsterdam Internet Exchange), which undoubtedly plays a European, but also a global role. There are also four other exchanges in the Netherlands.[38]
In addition, we should mention in this context the Internet service providers, KPN and other telecom and cable service providers whose telephone or cable infrastructure is used for Internet traffic.

These points of vulnerability affect primarily the availability of Internet, the layer of essential services we have already mentioned and the transmission layer (see paragraph 2.2.2). The application layer is supplied by so many professional players that a complete disconnection of it would be fairly unrealistic, although if these other two layers were disconnected, the application layer itself would no longer be able to operate.

The Internet could also be directly affected by undermining confidence in it. For example, if digital banking between one bank and another were to be disrupted for a few days, and if this were given the required publicity (jihadis have shown that they are quite adept at this), then confidence would be undermined. This element, however, is regarded as an aspect of the "Internet as a weapon" and will therefore be dealt with in the next section.

While it is possible to imagine other potential forms of attack, a cyber attack is most likely to take place through the use of the types of DoS attacks we mentioned earlier. As far as is known, there has been one DDoS attack, which had a profound impact on the infrastructure of Internet. This occurred on 21 October 2002, and was aimed against the DNS root servers that regulate worldwide Internet traffic. Seven out of the thirteen interchanges apaprently succumbed to the attack and two servers were apparently shut down. Technically speaking, the attack failed: the system would only be overloaded if eight or more of the DNS servers succumbed. This attack was carried out on a hitherto unprecedented scale. However, the fact that apparently only six per cent of the requests to the domain name servers were not answered[39] indicates that the robustness originally intended for the Internet, and the facilities for diverting data traffic, lived up to expectations.
In addition, there are no indications that this attack had any terrorist perspective. Wide-ranging measures have now also been adopted on an international basis, so that it is no longer possible to perpetrate this type of attack against the root servers.[40]

34 CRS 2005a, p. 3, Dasselaar 2006, Planet.nl 2006a, Planet.nl 2006b, Planet.nl 2006c, Nu.nl 2006b, Kwint 2004.
35 Lewis 2002, p. 4.
36 Benschop 2006b.
37 Source: TNO.
38 Source for summary of exchanges: TNO.
39 Benschop 2006b and http://www.cs.cornell.edu/people/egs/beehive/rootattack.html.
40 Expert meeting.

For example, in order to make a successful DDoS attack against the Internet, perhaps in order to largely isolate a country, an enormous army of bots would be required. Merely acquiring an army of bots via online trading would be relatively simple and inexpensive.[41] Let us give you an idea of the costs that would be involved: $250 to hire 5,000 (pre-infected) machines, or sometimes even greater numbers. Acquiring, adapting or even writing the required pernicious code for creating one's own zombie army is really quite straightforward. There are many tools available on Internet, with about 400,000 sites according to reports.[42] Attack armies are accordingly quite straightforward to create or hire, and also quite easily manageable by individuals with average skills.

How vulnerable is the Internet to cyber attacks? First of all, of course, the Internet was always intended to be able to withstand attacks. The Internet therefore responds flexibly to attacks: packets are quickly rerouted and computers can always continue to communicate via IP addresses if, for example, the DNS servers are down. A DDoS attack can be countered not only by quickly recognising it as such, using smart detection methods, but also by increasing server capacity and extending the number of junction points. Carrying out an attack against the Internet as a whole is a complex matter. At the time of writing this study, the Internet has never yet been completely disabled. The well-known examples of minor attacks against parts of the infrastructure have not been attributed to terrorists. An exercise imitating a mass attack on the information infrastructure of the Internet in the USA in July 2002, entitled Digital Pearl Harbor, had significantly reassuring results. According to a report on this exercise, a successful attack would require "a syndicate with significant resources, including $200 million, country-level intelligence and five years of preparation time".[43] There is accordingly a high threshold for any such attack.

But there are certainly still some vulnerabilities. Thus elements on the periphery of Internet might be brought down because of the lesser number of connections there and the lower levels of redundancy. A lack of transparency and understanding on the part of government, providers and users will increase the risk of an unanticipated lack of redundancy.[44] A global disconnection of the Internet does not, however, appear to be realistic. The Internet is too robust for this, and we have learned from earlier attacks.[45]

Is the "Dutch Internet" more or less vulnerable to cyber attacks? While the Internet is global by definition, making it difficult to take an isolated view of the Netherlands, it is still possible to speak of the Dutch element of the Internet to a certain extent. Thus the Internet in the Netherlands is partly dependent on the DNS server managing the '.nl' domain. By making all .nl domain names unavailable, all of the e-mail addresses, websites and services offered under the .nl suffix would be disconnected. Various experts conclude that there are now such a large number of clones of the DNS root servers, both worldwide and in the Netherlands, that there is a relatively small chance of disconnection of large parts of the DNS in the Netherlands (as regards both the availability of the .nl domains and the facility for Dutch surfers to access the Web).[46] In addition, websites and e-mail addresses with a different extension, for example .com, .org en .net, would continue to function normally. An isolating attack on the .nl domain would require preparation time of at least six months and also a significant amount of knowledge: the locations and systems would have to be reconnoitred in advance.[47] The routers would also have to be overloaded, but that would require a great deal of knowledge and there is built in redundancy. At the most, this would affect providers who did not have their houses in order. In the event of a cyber attack, there would be a gradual disconnection. The providers would therefore see any attacks as they happened. The Computer Emergency Response Teams (CERTs) keep in touch with each other and can speedily adopt counter-measures. On the one hand, the high degree of penetration of the Internet in Dutch households and organisations makes the Netherlands particularly vulnerable when compared with other countries. It has long been known that users do not take adequate security measures, so that they might end up being affected by a botnet. On the other hand, there are so many service providers in the Netherlands who are crucial to the operation of the Internet that the country is accordingly less vulnerable to successful cyber attacks. All things considered, taking down the Dutch section of the Internet seems unrealistic, albeit more realistic than switching off the entire Internet.[48]

41 CRS 2005a, p. 20.
42 Interview 2 and Bunt 2003.
43 Weimann 2006, p. 168, referring to a report from CNET.com.
44 Kwint 2004, p. 6, Thiele & Van Vliet 2005.
45 Expert meeting.

It is possible to imagine that a succession of pinpricks causing symbolic pain and adversely affecting confidence in the Internet. This might happen, for example, if terrorists were to impair the functioning of certain elements of the Internet on a few occasions. They would make the most of even a relatively small success, and regard it as a success nonetheless. This type of minor attack would therefore affect not so much the availability of Internet but primarily confidence in the Internet. It would have to be based on a targeted strategy (see also paragraph 2.3.7) and it is also debatable whether such an event would amount to terrorist activity. Perhaps it ought rather to be regarded as a non-terrorist weapon in an unequal struggle. It is, after all, entirely uncertain that society would be disrupted, which is the assumption underlying the definition of an event as terrorism. It is also imaginable that jihadis (perhaps from outside the Netherlands) would attempt to perpetrate cyber attacks on governments in the world's hot spots. In the Middle East, for example, there is a much lower level of redundancy in the Internet.[49]

Dependence on the Internet will increase in years to come as a result of new applications such as telephone and television, combined with greater bandwidth (see paragraph 2.2.2). This will also increase its vulnerability.

2.3.3 The intention behind jihadi cyber attacks

The intention on the part of jihadis to choose the Internet as a target is incorporated within the definition of terrorism, namely to promote social changes or to influence political decision-making. This is, of course,

46 Kwint 2004, p. 4-5, also interview 3.
47 Interview 2.
48 Expert meeting.
49 Expert meeting.

possible in many and varied ways, and the relevant question is therefore why they would want to target the Internet with a cyber attack. Why would this be attractive? It is, after all, frequently said that jihadi terrorists are primarily concerned with creating as many innocent victims as possible, and that their activities must by definition instil fear. Are there not better ways to do this than by opting for a cyber attack?

The principal arguments for the Internet being attractive as a target for jihadis, using a cyber attack, are:

1. This type of attack fits in with the general strategy of Al Qaeda. A cyber attack has the potential to result in major economic damage, and accordingly fits in with the strategy of Al Qaeda, which includes economic targets, as recently confirmed by al-Zawahiri.[50] In one of his many addresses, Bin Laden said: "America [...] needs further blows. The young men need to seek out the nodes of the American economy and strike the enemy's nodes".[51] Bearing in mind the current threat assessment, it is predictable that jihadis would also want to find economic targets elsewhere than in the United States. There are also signs that Al Qaeda strategists have discovered the Internet as a strategic battleground.
2. A cyber attack suits an uneven struggle quite well. DDoS attacks, for example, are implemented with limited resources against a large and advanced computer system. That is what is called an "asymmetrical attack", comparable in terms of strategy with the commission of a suicide attack against an oppressor with a large military power at its disposal.[52] In principle, a jihadi hacker might be in a position to throw a nation into chaos, temporarily or partially.
3. There is a major psychological effect, because of the unpredictability of a cyber attack. Bearing in mind the complexity of the Internet, the effects are not easily foreseeable or predictable, so that disruptive consequences cannot be completely excluded. The ultimate scale of a zombie network, for example, cannot always be projected.[53] There is always some uncertainty in advance as to whether sufficient measures have been taken against such an attack, and this unpredictability also has a psychological effect.
4. The combination of the unknown quantity of cyberspace with terrorism increases psychological fear. Lack of awareness of the (im)possibilities of committing attacks using computers and Internet, or disrupting society, is a factor that instils fear among many people. There is still some distrust of computers and Internet, and ghost stories are guaranteed to induce "cyber fear". For this reason even lightweight blows might have a disproportionately high impact.
5. Jihadis can use the multiplicity of reports concerning the vulnerability of the Internet. It is precisely these reports about the vulnerability of Internet that have put terrorists on the track of the (Western) economy as a potential target and have offered them a helping hand for an effective attack.[54]

50 NCTB 2006A.
51 Weimann 2006, p. 45.
52 Interview 6.
53 Interviews 2 and 6. This was also apparent in the case of the Dutch producers of this type of network for criminal purposes.
54 CRS 2005b, p. 4.

6. A cyber attack against the Internet has some operational advantages. There is, for example, no loss involved, as there would be with a suicide attack. Computers, Internet access and hacking tools are available to anyone, and much more readily available than weapons or explosives. The terrorists are also in a position to determine the time, location and circumstances themselves, as well as carrying out the attack from a distance: it is the equivalent of a smart bomb, which is difficult to detect and which can be detonated from a distance (even from another country), making detection and arrest more difficult. The (relatively) anonymous character of the attack makes it more difficult to detect and arrest the perpetrator. In many countries the chances of apprehending the attacker are relatively low, because of a lack of cybercrime legislation and sufficient knowledge on the part of the police.
7. A cyber attack has a lower threshold than an ordinary attack, certainly than a suicide attack. While terrorism is concerned with creating as many victims as possible, or wreaking as much havoc as possible, there is still a threshold involved. Research in the military sector, for example, shows that a large percentage would be unwilling to kill others if it came to the point. Internet swindling also has a lower threshold than swindling over the telephone or on the basis of physical contact. And while many jihadis strive for and approve of martyrdom verbally, there is a substantial gulf between words and deeds. In this context, a cyber attack is much easier to carry out than a suicide attack or some other type of attack where large numbers are killed or wounded as a result of the perpetrator's own actions.[55]

There are some arguments against cyber attacks as well as ones in favour:

1. The effects of a cyber attack are unpredictable. This unpredictability can also cause problems for the attacker, for example in relation to snowball or side effects. Thus, in 2000, Palestinian hackers successfully took down some Israeli ISPs. It subsequently transpired that the Palestinian Authority website was also put out of commission by this action.[56] While there is a potential for major economic damage, the actual damage cannot easily be predicted. This is partly because the Internet is robust and designed specifically to be able to take some hits.[57]
2. A cyber attack does not result in any spectacular photographs. There are no spectacular pictures of smoking heaps of rubble, dead bodies or wounded victims. This is in contrast, for example, with suicide attacks.
3. A cyber attack is not in the interests of terrorists. Terrorists would be shooting themselves in the foot, bearing in mind their own intensive use of Internet for other purposes. It is in their interest that the Internet should continue to operate properly. On the other hand, it should be borne in mind that terrorists probably do not care too much about this, and would be happy enough with such consequences in order to achieve a higher goal. Al Qaeda would also have taken account of the fact that the attacks in 2001 would have certain consequences for their own freedom of movement.
4. A cyber attack requires a long preparation period, is complex and is made all the more difficult by the dynamics of the Internet. A cyber attack requires a strategic vision, training and the availability of money and

55 Expert meeting.
56 Bunt 2003, p. 46.
57 Weimann 2006, p. 168.

resources. That said, it should be borne in mind that the attacks of 11 September 2001 also required a long preparation time as well as training. One important distinction, however, is that buildings are designed to stand for a long time, so that a lenghty preparation period is not a problem. The dynamics of the Internet, on the other hand, are such that preparations might well have been overtaken by developments in relation to the time when the attack was planned. This does not detract from the fact that terrorist organisations have generally demonstrated that they are extremely adaptable.

5. Using the Internet leaves tracks. While there are many possibilities for operating anonymously on the Internet, using the Internet still leaves tracks, so that this anonymity is only relative. For example, those who are actively involved in child pornography on the Internet use advanced techniques in order to remain anonymous. Fortunately for detection agencies, it is easy for them to make mistakes and it has been possible to trace them until now, partly as a result of intensive international collaboration in this area. There is no reason to assume that the same would not apply to terrorist use.
6. A cyber attack does not fit in with the quest for martyrdom on the part of jihadis. While this is certainly the case, we should still recollect the earlier argument against this, to the effect that a cyber attack has a lower threshold, and therefore there is the potential for greater numbers of (young and inexperienced) jihadis to feel called upon to convert their words into actions.
7. The high level of resistance does not make this an attractive area. Attacking something that was designed to overcome attacks is a challenge, but the high resilience of the Internet may also ensure that jihadis would prefer to opt for other targets at the end of the day.

2.3.4 Requisite and available knowledge and resources among jihadis for a cyber attack

We described two methods in paragraph 2.2, namely the mass overload attack and targeted hacking. The first of these is the more obvious for cyber attacks. We also indicated that examples of terrorist use of computers are known and that they have modern equipment. We also indicated that there are examples of jihadi hackers (in groups) and that knowledge about hacking is disseminated through jihadi websites. For the time being this appears to be focused on the optimal use of the Internet rather than on attacks against the Internet. We also mentioned possible collaboration between terrorists and hackers.

If jihadis were able to infiltrate the Internet industry, this would increase the chances of a cyber attack. To have the biggest impact, they would then have to infiltrate the major players. It appears unlikely that this would have any major chance of success, because the technicians with the required knowledge form a really close community and know each other well. Discovering the person who has done something wrong would not take much time.[58]

2.3.5 Consequences of a cyber attack

The chances of immediate fatalities or casualties as a result of a cyber attack against the Internet are small. No animals would be killed, nor would the environment

58 Expert meeting.

be affected.[59] What we're talking about, after all, is an attack against computers and computer networks. Indirectly speaking, of course, there might be fatalities or casualties if, for example, telephone traffic via the Internet were to be silenced, so that people could not make calls in emergencies, medics could no longer exchange information, or ambulance services could no longer communicate.[60] It is unlikely that this would involve large numbers of dead and wounded.

If the Internet were no longer to be operational, this would result in major economic loss. By putting all .nl domain names out of reach, for example, all of the e-mail addresses, websites and services offered under the .nl suffix would be disconnected. In the event of a sudden collapse, there would be immediate corporate production loss among service providers on the Internet amounting to about ff1 million per day (as at the end of 2003), resulting from the loss of traffic time and online advertising. The immediate requirement for many businesses and government institutions to look out for a different domain name (and to publicise such new names and e-mail addresses) in the event of an abrupt disconnection has financial consequences amounting to ff490 million.[61] GOVCERT.nl, however, states that these (actually indirect) costs cannot easily be estimated.[62]

GOVCERT anticipates that the intangible consequences of a cyber attack would affect more than 40% and perhaps as much as 75% of the Dutch population.[63] The nature of the consequences and the extent to which they manifest themselves depend partly, of course, on the period of time for which the Internet is non-operational. If jihadis actually succeeded in silencing the Internet, it is anticipated that little time would be required to restore it.[64] That would, of course, depend on the situation and the extent to which the jihadis would manage to sustain their attack.

2.3.6 Assessment of the threat of cyber attacks

All things considered, the NCTb regards the threat of cyber attacks against the Internet as minor. Attacks against the global or Dutch Internet itself are not considered likely. The most important reasons for this are that the advantages do not substantially outweigh the disadvantages, and that a successful cyber attack is not really within the realms of possibility, particularly because of the Internet's significant resilience and redundancy.

While a cyber attack involves a lower threshold than, for example, suicide attacks, so that potentially larger numbers of jihadis would be willing and able to undertake them, the most important counter-argument is that disrupting the Internet would also disrupt the jihadi infrastructure on the Internet. Other arguments we have considered include that different types of attack - such as bomb attacks on public transport - have a greater impact, whereas the consequences of a cyber attack may well be significant, but cannot be guaranteed (from the terrorists' perspective). There might be

59 This conclusion is partly derived from Thiele & Van Vliet 2005.
60 See, for the indirect consequences, Planet.nl 2006b, for example.
61 Stratix 2004, p. 1, Planet.nl 2006a, Planet.nl 2006b.
62 Thiele & Van Vliet 2005, p. 16-17.
63 Thiele & Van Vliet 2005, p. 18.
64 Expert meeting.

major consequences if an attack were to be successful, particularly in relation to economic factors, but it is unlikely that the Internet would be inoperable for a lengthy period.
There are opportunities for cyber attacks and there are vulnerabilities that could be used, but far-reaching steps can be and have been taken to make Internet less vulnerable. Also, a successful cyber attack is a gradual business. Once launched, a cyber attack spreads through the Internet. This offers sufficient opportunities for detection, and there are collaborative arrangements in place in order to take appropriate steps. We are only aware of a single example of a cyber attack as defined here, but there are no indications that this was committed with terrorist intent. If we were to expect a cyber attack, then it would be a small-scale attack for a limited period, or else a coordinated combination of small-scale cyber attacks. This might affect confidence in the Internet, certainly if it was combined with a publicity campaign, but we find it difficult to foresee serious consequences for the operation of Internet.

2.3.7 Other types of assaults and attacks against Internet

Other types of assaults and attacks against the Internet, in addition to cyber attacks, are also possible; these include a physical assault, an electromagnetic assault and indirect attacks resulting in the failure of the Internet (or its infrastructure). Which are the vulnerable places and elements in the Netherlands for this type of attack? There are core junctions, core functionalities and connection lines in the Netherlands that are important for the Internet in this country, but also sometimes for the European or even the global Internet. Earlier on we referred to the (duplicate) root servers situated in the Netherlands, the DNS server managing the ".nl domain" and exchanges in the Netherlands such as AMS-IX, whose role is a global one. We should also mention the Internet service providers, KPN and other telecoms and cable service providers whose telephone or cable infrastructure is used for Internet traffic.
There are numerous optic fibre and other cables within the Netherlands for data transport, but there are also cables for access to the Internet by Dutch users, and the telephone or cable infrastructure we have already mentioned is frequently used for this. Because of the geographical position of the Netherlands, many transatlantic cable connections arrive in the Netherlands, where there are also cable connections with other European countries.
Some of the data is transported via microwave radio link or satellites. The equipment used at the "core" junctions by the various organisations for the core functionalities depends on electrical current; it cannot readily resist water or electromagnetic radiation and it requires cooling facilities. While these organisations are spread throughout the country, there is a concentration of businesses, junctions, servers and cables in the western part of the Netherlands.[65] To summarise, there are: a) the various types of organisations, b) servers and server parks, c) cables, and d) connection resources, all vulnerable to this type of attack and with a concentration in the western part of the country. In addition, the equipment and cables that run the Internet are also dependent on other equipment and service provision, thus creating an extra vulnerability.

The organisations with a crucial part to play in the operation of Internet are of course aware of these vulnerabilities. For example they operate from various co-locations, have extra safeguards built in for an uninterrupted power supply, have emergency generators and the requisite fuel supplies, redundant equipment and, to some extent, reserve equipment.[66]
There are still, however, some risk factors. Thus on 29 May 2006, the AMS-IX in Amsterdam had trouble with a power cut. Everything slowly started up again after eight minutes. This meant that a number of people were excluded from the Internet, with a slight increase in the traffic via other networks. The other exchanges also dealt with slightly more traffic.[67]
That showed, on the one hand, that there could be quite a small-scale event but also, on the other hand, that even if the AMS-IX were to disappear completely from the face of the Earth (which is fairly unlikely) the Internet would still continue, albeit with some delays here and there and slightly reduced performance. Those connected to the AMS-IX did in fact have alternatives for dealing with Internet traffic. The participants at the expert meeting also considered that the other parties, and certainly the major players, had taken sufficient precautionary measures. One other vulnerability is that the physical cables might be sabotaged, smashed up et cetera. There are, however, many cables in the Netherlands and re-routing would be a speedy affair. This does not alter the fact that there could be single points of failure in the Netherlands. The extent of the impact of this is, of course, partly dependent on the capacity of the cable in question, and the extent to which that cable has a unique part to play, or is at least difficult to replace. A point of concern is whether the various government authorities are sufficiently aware of the importance of those service providers who are crucial to the operation of the Internet. If there is a disaster in the vicinity of a crucial location, for example a bomb attack or a quarantine area in connection with bird flu, the employees still need access to that location. That it is certainly the case if the service provider itself were to be affected. Emergency generators need to be refuelled every so often, for example.
In addition, an adequate fenced enclosure is often desirable, but one of the participants at the expert meeting indicated that local government authorities sometimes cause difficulties with the building permits required for them.[68]

This type of attack has certain attractions, which we mentioned earlier in connection with cyber attacks (paragraph 2.3.3). These attacks or assaults a) fit in with jihadi strategy, b) combine fear of the unknown (cyberspace) with terrorism, and c) there is also a lot known about the vulnerabilities of the Internet. Other advantages we mentioned at that point are not really relevant to this category (relatively simple and inexpensive, asymmetrical battle, unpredictability, operational advantages and lower threshold). An extra attraction for this type of attack, as opposed to cyber attacks, is that it is possible to imagine really spectacular pictures, which would fit in with the jihadi propaganda strategy. Also, this type of attack can affect confidence in the medium of the Internet because of its visibility, and because essential services or information can be destroyed. Therefore it acts as a means by which terrorists can instill fear.

65 Expert meeting, Dasselaar 2006, Planet.nl 2006a, Planet.nl 2006b, Planet.nl 2006c, Nu.nl 2006b, Kwint 2004.

66 Expert meeting, Planet.nl 2006a.
67 Computable 2006. Shortly thereafter - on 11 June - the AMS-IX carried out a blackout test, after which the problems with the backup system were resolved.
68 Expertmeeting, Dasselaar 2006, Planet.nl 2006a, Planet.nl 2006b, Planet.nl 2006c, Nu.nl 2006b, Kwint 2004.

Two less attractive aspects of a cyber attack also have to be considered here, namely the unpredictability of the effects and also that an attack would not be in the interests of terrorists. The other negative points (no spectacular pictures, long preparation time/ complexity and leaving tracks) do not apply. An extra disadvantage, however, is that silencing the Dutch Internet in this way, let alone the global Internet, would almost certainly be unsuccessful. This would require a huge number of simultaneous successful attacks. This type of attack accordingly has a lesser impact, in principle, than a cyber attack with regards to affecting the availability of Internet. While we also consider this to be unlikely, it would be possible for an individual using a cyber attack to bring the Dutch Internet to a standstill. This result would require a great deal of effort to achieve, even for a group, with the other types of attacks. Also, for this type of attack, a significant amount of physical preparation would be required, making the terrorist vulnerable and leaving tracks.

The attraction is also for large part determined by the extent to which there is a conscious strategy. What do they want to achieve and to what extent can they exploit their attack in terms of publicity? Do the terrorist groups who embark on such attacks view them as complementary to other types of attack (force multiplier) or as an independent attack? We are aware that the jihadis take account of the propaganda effects and psychological impact when choosing their type of attack. The bottom line is that a single attack with one aeroplane in the USA would have had a major impact, but they opted for four simultaneous attacks. The same occurred with the attacks in Madrid and London. Viewed in this way, it seems appropriate to presume a strategy whereby several attacks of varying types would be committed, including one or more against the Internet. We are also aware that they would want to hit economic targets. This type of attack would certainly fit in with jihadi strategy, bearing in mind the dependence of the economy on the Internet.[69]

As regards the knowledge and resources required, and the extent to which jihadis have access to these, the position is that no special knowledge and resources are required - apart from knowledge about vulnerable points in the infrastructure - beyond those required for comparable attacks against other targets, such as train stations. We may therefore assume that terrorists have, in principle, adequate knowledge and resources for this type of attack. Those participating in the expert meeting pointed out that it is not very difficult to find out about vulnerable and critical locations in the Netherlands. There is also sufficient training material available on the Internet on how to carry out such attacks. This is also true for electromagnetic attacks and equipment. We can find indications on jihadi websites that they are interested in this type of attack. None have yet been committed by terrorists, however, as far as we are aware. The participants at the expert meeting also pointed out that a significant body of knowledge and resources would be required for a properly targeted, large-scale electromagnetic attack, so that such an attack - and certainly a successful one - is (as yet) unlikely. The consequences are comparable with those of cyber attacks, subject to the proviso that it is more likely that this type of attack would result in fatalities and casualties. The time required to restore the situation would also be longer. After all, if a location were to be subject to a real strike, it would not be rebuilt immediately, and there is not a great quantity of reserve equipment available at very short notice. On the other hand, the service providers are now working from co-locations, so that even in the event of disconnection, the effects might still work out acceptably for that specific service provider. It is also the case that there is a large degree of redundancy on the Internet. This type of attack would therefore have lesser impact than one assisted by a cyber attack.

69 Partly based on expert meeting.

2.3.8 Assessment of the threat of other types of attacks

The NCTb considers that there is not a high likelihood of other types of attacks. There may well be opportunities but, steps have been taken to minimise the opportunities and restrict the impact. It is impossible, in principle, to switch off the Internet with these other types of attack; the operational consequences are more limited than for a successful, large-scale cyber attack, but the effects may be more visible, they would impact the availability of (stored) data and the repair time for buildings and equipment would be longer. The impact would also be more easily exploited via propaganda. It is conceivable that there would be victims in the event of an explosion, but the damage would principally affect equipment. Jihadis have access to the required knowledge and resources, particularly in relation to bomb attacks.
While one of these other sorts of attack against the infrastructure of Internet appears more likely than a cyber attack, and has its own attractions for jihadis, we are justified in asking whether - bearing in mind particularly the limited impact it would have on the operation of Internet - terrorists would not prefer to perpetrate a bomb attack against a soft target instead of an important Internet location.

2.4 THE INTERNET AS A WEAPON

2.4.1 Explanation

The Internet is becoming more and more interwoven with all manner of activities in the physical world and all manner of sectors, organisations and individuals are linked to the Internet. This means that they, too, are vulnerable to attacks via the Internet. Frequently heard theoretical scenarios include taking over management systems for vital installations, such as those in the chemical sector, in order to cause catastrophes. Disruption of communication systems, public transport, the logistical sector, the financial sector and power supplies are also mentioned as opportune examples, along with attacks on the reliability of virtual services such as Internet banks. Mention has also recently been made of the possibility of infiltrating hospital systems via the Internet. The manipulation of blood groups in patient files, for example, could have potentially dramatic consequences.[70] Another familiar scenario is the disconnection of alarm control centres or emergency centres, for example by *hacking* or causing overloads, thus increasing the effects of conventional attacks such as a bomb attack (*force multiplier*).

70 Interview 3 and Planet.nl 2005.

Use of the Internet as a weapon is particularly susceptible to overreaction and exaggeration. Accordingly there are regular reports of hacking into websites. These often involve public web sites belonging to organisations rather than their internal networks.[71] This is fundamental to the element of threat, because there is no contingent risk for example of electricity supplies being brought to a standstill. On the other hand, it is not always necessary to have "traditionally" disastrous (or visible) consequences of terrorist activities, and the multiple simultaneous hacking of websites for virtual services (principally electronic banking) and the (continued) manipulation of sensitive information can have a real terrorist impact, as can rendering such information unobtainable or unreliable. Hacking the homepage of an Internet bank and defacing it with jihadi slogans should only be regarded as a nuisance, however, or activism at the most. That is why it is important to have good demarkations. It is also important, when considering the Internet as a weapon, that cyber attacks designed to make a political statement ("hacktivism") are not included, because neither the intention nor the consequences fall within the definition of terrorism. This can also lead to confusion with use of Internet as a resource. One example of the application of the Internet as a resource is the collection of information on a nuclear power station via the Internet, with the aim of committing a terrorist attack against it. Another example is publicising a threat via the Internet, with the attack as a form of instilling fear. In this study, we have preferred to regard these forms of Internet usage as a separate category. It does, after all, involve other activities, for which different knowledge and resources are required, and which also involve different action points in terms of policy (see chapter 3).

Figure 2.3 Examples outside the scope of "The Internet as a weapon".

Imagine that a jihadi infiltrates a power station as an IT specialist, and either has or obtains access to the computerised control systems and manages to achieve a "blackout" of part of the Netherlands on Monday morning at 7 a.m., with all of the consequences involved. Dutch society is - at least temporarily - disrupted, and if the disconnection persists then backup systems such as those in hospitals might also fail.
Despite the fact that the gravity of the threat is significant, and that ICT has been used, this is not an attack via the Internet. This example would not therefore fall within the definition of "the Internet as a weapon" as used in this study.

According to a report dated 29 June 2006, a group of Moroccan hackers hacked into more than 750 Israeli websites after the Israeli army invaded the south of the Gaza Strip with dozens of tanks, bulldozers and armoured vehicles. The targets included websites for banks, car factories and hospitals. The group, called Team Evil, supported opposition to the Israeli occupation. [....] The hackers left the following message on the sites they had hacked into: "Hacked By Team-Evil Arab hackers u Kill Palestine people we Kill Israel servers" It was the largest attack against Israel websites to date.[72] This is a typical example of hacktivism, rather than use of the Internet as a weapon.

2.4.2 Internet possibilities as a weapon; vulnerabilities and defences

Attacks via the Internet can take various forms, including the overload by a DDoS attack, which we mentioned earlier. The impact of disrupting or overloading a specific network is limited, however, and would be very unlikely to have a major influence on the operation of a vital sector. Targeted hacking in order to manipulate or disconnect systems is more likely (see paragraph 2.2.4).

There are no concrete cases known about, anywhere in the world, where targeted attacks against physical targets have occurred via the Internet with adverse consequences that could actually be categorised as terrorist, [73] although there have been a number of unpleasant incidents that could have ended up with serious consequences. Thus a young hacker apparently obtained access to the control system of a dam in the USA and was in the position where he could have opened the floodgates. This tale transpired at the end of the day to be slightly exaggerated. The hacker apparently did obtain access to the management network, but was not in a position to actually "control" anything.[74] But there have also been incidents involving hackers in the EU and in the Netherlands, for example in the energy sector.[75] Leaving aside for a moment the actual consequences of hacking attempts so far, what these show is that really good and devoted hackers can always uncover vulnerabilities, whether or not they get help from infiltrators or frustrated former employees. Many incidents also go unacknowledged or unreported for fears of damage to the corporate image.

Apart from the critical infrastructure, services (including financial services) may also be affected. While it is reasonable to ask whether this has any "traditional" terrorist impact, it can certainly jeopardise the reliability of data and services. It can also serve a double purpose: the commission of fraud can in the first place be used to acquire funds, for example for future campaigns. Secondly, the wealth of publicity given to large-scale (credit card) fraud campaigns can adversely affect public confidence in electronic payment traffic, general data traffic and perhaps even the Internet itself. When this type of campaign is combined (through phishing, pharming or otherwise, as experience with cybercrime shows) with a physical attack on a storage provider, so that backup information on accounts and transactions is lost, it makes citizens extremely uneasy. While the effect is more subtle than manipulation of a power station, resulting in large-scale supply disruptions, the psychological impact can be substantial, certainly bearing in mind our increasing dependence on the Internet. Jihadis can also profit from this type of campaign from a propaganda perspective, by demonstrating publicly that they have succeeded in striking at the heart (its finances) of the West.[76]

As we indicated earlier, it is not possible to take over control of an entire system or network at the drop of a hat. No such attack has yet taken place in the Netherlands (or at least none has been publicised), and it would be a complex business, but there are examples from abroad that might also be

71 Weimann 2006, p. 158. The NASA website was hacked, giving rise to the idea that hackers had been "in control".
72 Nu.nl 2006a.
73 Weimann 2006, Green 2002.
74 Weimann 2006, p. 166.
75 Luiijf 2006, p.52-53.
76 Expert meeting.

applicable to the Dutch situation. It is therefore important to determine where the Dutch vulnerabilities are, certainly in relation to vital infrastructure. The following aspects are involved: (a) SCADA, (b) standardisation of systems and software, (c) false security, (d) social engineering, (e) complacency and human error, and (f) the dynamics of the Internet, software and networks.

A SCADA

SCADA *(Supervisory Control And Data Acquisition)* is a generic term for process control systems used by many business sectors including water and energy businesses, the transport sector and the chemical industry. A SCADA system frequently monitors and manages entire installations. SCADA is subject to vulnerabilities related to its layout, complacency and human error. This means that SCADA is vulnerable to targeted hacking, which ultimately means that buttons might be pushed within an installation. It is worth asking, however, who apart from in-house staff would have the specific technical knowledge to be able to use a SCADA system. Hacking is one thing, but actual management is quite another.[77] The SCADA software may well be standard, but individual configurations vary from one business to another. It would seem that infiltration or inside information would be required to take over a system. Without this type of specific knowledge, any attack would be no more than a lottery. We are aware of more than 40 actual cases of hacking attacks against SCADA.

Figure 2.4 Examples of vulnerability to the Internet as a weapon.[78]

The Slammer worm, dating from 2003, nestled itself inside the network of a telecommunication provider. This made communication with a SCADA system at an electricity supply substation no longer possible, and the SCADA system became unusable for between six and eight hours. In August 2005, a worm disabled 23 factories in the USA. A factory in Belgium was infected from that network. A factory in Australia was also out of business for a few hours, with production loss estimated at $6 million.

Figure 2.5 Example of vulnerability via SCADA

A well-known example of unauthorised access to a SCADA system was the disruption of a drinking water and sewage treatment plant in 2000 by a former contractor. He disengaged warning systems, disrupted communications, prevented pumps from starting on time, and released an estimated 1,000,000 litres of untreated waste water.

B Standardisation of systems and software

On the one hand there is much to be said for the extensive standardisation of systems and their security by means of software enhanced by fixed protocols. This prevents any element of amateurism, for example. On the other hand, standardisation offers opportunities to individuals with suspect intentions. Companies are more and more frequently buying Commercial Off-The-Shelf (COTS) software. In principle, anyone can buy this software and study it as part of the reconnaissance for a cyber attack. Once errors or vulnerabilities are discovered, every system using the same software can, in principle, be exploited. This is also the reason why a virus like the "I Love you" virus was so successful: on a global basis, as almost everyone uses the same e-mail program.[79]

Setting up a network and its associated security to one's own specification accordingly has advantages in addition to the obvious disadvantages. In this context, people talk about *security by obscurity*. A lot of software is specially written for specific companies and is then managed by one or more system managers. Depending on the quality of the software and the personal working methods of the system managers, this can result in a proverbial maze. Thus we are aware of an example where an organisation's network was broken into, but then a wrong turn was taken and no critical elements were reached, far less manipulated.[80]

It is expected that standardisation in automation and network management will continue to expand. The security of systems may well increase, but if a hacker succeeds in obtaining access, he will quickly find his way around more and more systems. Security by obscurity will come to an end through good housekeeping and uniformity in software and management.

C False security

Companies often only make paper checks as to whether or not their systems are secure. This is quite different from actually testing whether all of those measures on paper actually work in practice. Thus, for example, air-gapping is applied in order to prevent attacks from outside: this means that critical systems and networks are not linked either with each other or with the Internet. In 2004, however, computer systems belonging to the Army Space and Missile Defense Command, secured by means of an air gap, were twice infiltrated by a virus. Apparently no anti-virus software had been installed on that system. As soon as such a system is linked to a different network, even though doing so might be against the protocols, contamination is then only a question of time. Air-gapping is also completely ineffective if WiFi equipment is incorporated into an air-gapped network.[81] This instantly cancels the security measures taken on paper.

In addition, a great deal of investment will probably have been made in the relevant sector following privatisation, but perhaps not in the ICT infrastructure. There should be more tests and drills in the vital sectors. Finally, physical security and IT security - two quite different things - are regularly confused with each other.

77 See on this last point, Green 2002.
78 xamples taken from Luiijf, 2006.
79 Thiele & Van Vliet 2005, p.21.
80 Interview 2.
81 Based on Interview 3, Weimann 2006, p. 166 and Expert meeting.

D Social engineering

Social engineering means manipulating individuals within a business in order to acquire sensitive information. This topic is, in fact, outside the scope of this study. Social engineering can, however, be an essential resource in the preparatory hacking phase for a successful cyber attack. There are documented examples of this.[82] An exercise by NSA in 1997 in the USA showed that pretending to be a technician or a senior officer could convince others to surrender particular passwords.[83]

E Complacency and human error

Human complacency is a major risk. An investigation from April 2005 in the USA demonstrated that *Service Pack 2* for the Windows XP management system, essential for the security of systems, had only been installed on 9% of all PCs in the 251 investigated companies.[84] In the Netherlands, too, the position is undoubtedly that many system managers are not concerned in the first instance with security but rather with their core business: keeping the system in operation (sometimes 24/7), and therefore keeping the client or employer happy.[85] An investigation in the Netherlands showed that three quarters of the businesses investigated had a firewall, and had installed software against viruses and worms, and that 60% owned software to counter spyware.[86] The extent to which the installed firewalls were correctly configured, and the virus scanners were updated, is not known. It is also worth mentioning the analogy here that installing a firewall is the same as fitting a lock to a door: once you've gained access, for example because of a faulty lock, you can often get your hands on anything, unless the valuables are shut away in a safe.[87] Firewalls therefore have to be properly configured, and the accounts and files should preferably be protected by passwords.

Human error can also offer terrorists the opportunity of mounting a cyber attack. As we have indicated, many networks and management systems are not linked with the Internet. An ostensibly stand-alone system at, for example, a power station can still be attacked through any unforeseen connection with a network, which in turn is connected to the Internet. Thus the shared use by two separate networks of a single modern printer with its own memory capacity may be enough to pose a serious security risk. An ostensibly stand-alone network would then end up being connected to the Internet, and would be vulnerable without being noticed. This might also happen for example in a hospital, with the result that patient information could be manipulated.[88] There is also a risk inherent in the combination of office applications (where new vulnerabilities are discovered regularly) and monitoring and management systems, such as SCADA mentioned above.

82 Mitnick 2006.
83 Weimann 2006, p. 160 on the exercise 'Eligible Receiver'.
84 CRS 2005b, p. 5 en Wilson 2006, p. 75.
85 Interview 3.
86 EZ 2005.
87 Mitnick 2006.
88 Interview 2.

F Dynamics of the Internet, software and networks

Software and systems always contain vulnerabilities that can be exploited. A serious error was discovered in 2002, as a result of which Internet routers could easily have been taken over.[89] Another discovery of a vulnerability was demonstrated during a conference on computer security in July 2005 (Black Hat): there was a security gap in the heavily utilised Internet routers belonging to Cisco Systems. This vulnerability was so serious that even a well-known critic of cyber terrorism had to admit that there was a serious risk of attacks and data theft from networks, using a very speedy hack. While Cisco Systems had already issued a patch (repair software) for this gap, not all of its customers were apparently aware of this.[90] Other vulnerabilities have recently been discovered in office applications such as Word 2003 and Excel. This emphasises the risk of combining office applications and process control systems within a single network.

Numerous steps have been taken to reduce vulnerabilities. Networks are made more robust, and the infrastructures in fact already take natural disasters, user error and lightning strikes into account. Any disruptions caused by these circumstances can be quickly repaired,[91] and this should also be the position in relation to disruptions caused by an attack via the Internet. In addition, systems at power stations, for example, have built-in redundancy and are often equipped with emergency generators.[92]

Nor should we ignore the fact that the virtual world is not always a completely separate world, but rather it is a part of our own physical world: disruptions will be discovered, corrected or dealt with by people. Take a poisoning scenario as an example, where hacking into the production system results in the iron content of a breakfast cereal being increased to such an extent that children become sick and die;[93] the fact is probably being overlooked that the taste will also change (and this will be discovered by testers and others), or that the ingredient in question will suddenly have to be topped up much more - and more often - at the factory, and so on. The human factor and other factors should not immediately be disregarded in the case of an attack via the Internet. The same applies to disconnection of air-traffic control or onboard computers. Pilots are trained to be able to navigate and land without these aids.[94]

Are we particularly vulnerable in the Netherlands? Broadband and Internet penetration in the Netherlands is enormous. More and more businesses are using the Internet to offer their services or to operate systems, and our dependence on the Internet will undoubtedly continue to increase in future. And where there is no deliberate, direct link, there can still be an unknown connection to the Internet via a back door (see above under "Complacency").

All things considered, we can draw the following conclusion. There are opportunities for deploying the Internet as a weapon, and physical targets and virtual services are vulnerable to a certain extent. For physical and essential targets, control would have to be taken over, which would require

89 CRS 2005a, p. 9. It concerned an error in the Simple Network Management Protocol.
90 Wilson 2006, p. 75.
91 Lewis 2002, p. 11 en Green 2002.
92 Interview 2.
93 Colin 1997, p. 15-18.
94 Denning 1999.

extensive study or inside information. Experience in the area of cyber-crime seems to show that virtual services can be disrupted more easily. Steps can be and have been taken against this, however. The security of process control systems, such as SCADA, still lags behind the times to some extent. Vulnerabilities do not always relate directly to computers or the Internet, but rather to human factors. An attack via the Internet, such as we describe here, is a complex matter. There are no known examples of large-scale attacks via the Internet with serious consequences, although the incident with the untreated waste water (see Figure 2.5) is an example of what can go wrong if someone who knows the system wants to manipulate it from a distance.

2.4.3 Intention and the Internet as a weapon

Just as is the case with Internet as a target, there are also advantages and disadvantages concerning the Internet as a weapon, which will determine the question of whether and to what extent jihadis might want to use the Internet as a weapon. The advantages outlined in section 2.3.3 also apply in broad terms to the Internet as a weapon. The *unpredictability* of an attack, and therefore the psychological impact, is greater, however. For the defender, it is virtually impossible to foresee every consequence of a cyber attack, because it has not yet happened; it is also difficult to simulate and not all of the interdependencies can be predicted. This means that all manner of unexpected effects might occur.[95] It is also not a pleasant idea that a terrorist can break into the internal network of some element of a vital infrastructure or a hospital from a distance. For example, closing or opening a sluice or a dam through manipulation of the relevant SCADA system would not necessarily cause a flood disaster, but it might seriously interfere with shipping transport, result in accidents and instil fear in the population.

The *great variety and large numbers of combinations* available for attacks might be described as an extra advantage. There appear to be endless scenarios for attacks, and the number will only increase with the growth of Internet usage and dependency on the Internet. In addition, computers, software and networks will always be vulnerable, there will always be undetected inadequacies, and the complexity of vital infrastructures will inevitably result in mistakes and gaps.[96]

As with the advantages, the *disadvantages* specified in section 2.3.3 also apply to the Internet as a weapon. One important difference is that jihadis would not be shooting themselves in the foot with any such attack, because the Internet would still continue to operate. An attack and the damage it might cause would also be less predictable. Such damage might be greater because it involved direct targets, frequently part of vital infrastructure.
The damage - if for example the floodgates of a dam were opened as a result of a cyber attack - would be relatively limited when compared with a bomb attack (caused by flying an aircraft into the dam or otherwise) resulting in actual serious damage to the dam.[97]

95 Support for the extra unpredictability is based on Interview 6.
96 Weimann 2006, p. 166.
97 Lewis 2002, p. 4.

Bearing in mind the limited impact, or the unpredictability of the effects or their duration, terrorists would also have to attack several targets over a lengthy period in order to achieve a truly "terrorist effect".[98] Looked at from the jihadi's point of view, an extra disadvantage is that the human factor cannot be underestimated here. People may notice irregularities and take action, or they may be trained to act in emergency situations (see section 2.3.2).

Perhaps committing this type of attack is the last resort when conventional terrorism is being combated more effectively. If the physical security of vital property is increased, attacks via the Internet might well increase in proportion.[99]The question, however, is whether better security means that other physical targets would be subject to physical attacks before the terrorists attempted to take their pound of flesh via the Internet. The increase in virtual services certainly means that jihadis have extra targets available to them if they are not looking for martyrdom. Discussion *(chatter)* about SCADA on jihadi web forums is also apparently on the increase.[100]

2.4.4 Knowledge and resources

We indicated, in section 2.2, that we are aware of examples of terrorist use of computers and of the fact that they have modern equipment. We also indicated that we are aware of some jihadi hackers (in groups) and that knowledge about hacking is disseminated through jihadi websites, and we alluded to possible collaboration between terrorists and hackers. For attacks via the Internet, targeted hacking is the most readily available method, as DDoS attacks can only be deployed for overload disruption, except perhaps in the case of SCADA systems.
A serious hacking attempt cannot be carried out at the drop of a hat. Terrorists need to cope with a lengthy preparation period, and also attack several targets at the same time in order to achieve a true "terrorist effect". This type of strategic planning is not easy in a dynamic environment such as the Internet, with its many new applications and developments.
Even then, the results are unpredictable. An attack via the Internet, as described here, requires not only a great deal of knowledge but also effort and devotion. True hackers who have the capacity to cause actual damage are few and far between, but any such hacker of a jihadi persuasion, or who has been hired in (perhaps unwittingly), will do his utmost to succeed in his plan. This will also involve resources other than merely technical ones.
It might, for example, involve social engineering, infiltration or undercover work.

It is a fact, however, that there are no known examples of use of the Internet as a weapon by jihadis, and certainly not against any vital sectors. There are, however, indications that jihadis are interested in this type of attack. There are also known examples of criminals abusing or extorting virtual services, or rendering them unreliable. To date, greater attention has been paid to this variant of the use of the Internet as a weapon, because of the financial gain involved, and jihadis are more likely to be knowledgeable about this variant than about manipulation of a process control system in one of the Dutch sectors.

98 CRS 2005a, p. 11.
99 Weimann 2006, p. 171, Interview 1.
100 On this, see Independent 2006a.

2.4.5 Consequences

Jihadis may attack vital infrastructural elements via the Internet. Some of the sectors are therefore covered by the Counterterrorism Alert System, and for good reason. Terrorist activities against those sectors would have major and serious social consequences. It makes no difference here whether the attack is perpetrated via the Internet or otherwise.

While we can imagine innumerable scenarios, it would be difficult to imagine a cyber attack actually resulting in large numbers of fatalities or casualties. Hospitals might form an exception to this, with manipulation of patient data having potentially fatal consequences in some cases, as well as public transport, where disruption of railway interchanges might in principle have serious consequences. The reliability of the Internet, along with virtual services such as Internet banking, could well be affected, and this might ultimately have an influence on the continued existence and development of these types of services.

If cyber attacks caused long-term disruption in several sectors of the economy or society at the same time, people would actually start to feel the damaging consequences, and it is feasible that panic might break out in some segment of the population. People might start hoarding, the stock exchange might be disrupted or at least negatively affected, and at the end of the day there might be an element of disruptive damage to society. However, not every social and vital function is so dependent on the Internet that an attack via the Internet would actually be perceived as a blow. People recover from shocks quite quickly, for instance, and they are accustomed to breakdowns in power supplies and computers. The human factor is also significant in another sense: disruptions and changes are picked up by our senses or otherwise. If, for example, a chemical factory is manipulated via the Internet and starts to pump out poisonous gas, this will quickly be noticed in the surrounding area. We are not saying that there would be no casualties, but the cause of the problem would undoubtedly be traced quite quickly. This does not, of course, alter the fact that there might be more subtle consequences.

2.4.6 Assessment of the threat

The NCTb does not consider an attack via the Internet to be particularly likely at this point. The most significant considered reasons for this are that the advantages do not substantially outweigh the disadvantages (intent), that other types of attack would have a greater impact, and that while the consequences might be significant, there are no guarantees of this from the terrorist's perspective). There might be major consequences if an attack were to take place, but it is unlikely that the targets would be inoperable for a lengthy period. The confidence of the man in the street might well be affected by multiple disruptions in vital sectors, for example, or if virtual services and their associated privacy-sensitive data (banks and hospitals) became unreliable. It is difficult to assess how long such an impact on confidence might last, but it might be easier to cause this via the Internet than to cause a major disaster in the vital sectors. Steps can be and have been taken in order to reduce the vulnerability of the targets

to attacks via the Internet, but it is clear that process control systems like SCADA are still an exception to this rule. An attack via the Internet combined with a physical attack, operating as a force multiplier, is more likely than a cyber attack on its own.

The question of why terrorists have not as yet committed a cyber attack is also an interesting one. The knowledge, resources and preparation time are on hand and additional expertise can be hired in. The consequences of a cyber attack may well be less predictable than those of a bomb attack, but they can still be significant, and the jihadis would then be able to exact the maximum exploitation of the outbreak of "cyber fear", which could be anticipated, in their propaganda. The fact that this has not yet happened is probably a result of the fact that jihadis are not yet fully aware of the possibilities, or prefer to opt for more traditional targets.

2.5 FINAL ASSESSMENT

In this chapter, we have looked at the threat emanating from the Internet as a target and weapon from a variety of angles. We have distinguished a range of possible attacks and assaults. We have also looked at the separate dimensions of possibilities and vulnerabilities, how attractive such attacks might be, the extent to which jihadis have the knowledge and resources on hand, and the consequences. Finally, we have also looked at several points at other types of attacks within the terrorist repertoire.

If we can start of the last point first, we are still convinced that other types of attacks, including bomb attacks, are more likely in the foreseeable future than the attacks and assaults we have described in this chapter. We can imagine suicide and bomb attacks aimed at disrupting the Internet, but it is more likely that terrorists will prefer to commit these attacks against other targets, such as soft targets. The bottom line is that the Arena in Amsterdam, for example, has a much higher public profile than one of the Internet exchanges in Amsterdam, and also a much higher national and international publicity value. Also, although jihadis are very sensitive to the psychological message behind attacks, these more classic types of attack would seem to offer better opportunities for publicity than cyber attacks, as well as having more predictable results. Suicide attacks are particularly attractive to jihadis because of their glorification of martyrdom. Martyrdom cannot be achieved through the forms of attack and assault mentioned in this chapter. This might, of course, be an advantage in itself for Dutch jihadis: the gulf between words and deeds is, after all, smaller with this type of attack than with a suicide attack. A combination of one or more classic attacks, deploying the Internet as a weapon, appears more likely. This would amplify the effect of the classic attack.

The Internet as a target and a weapon may well pose little by way of threat at the moment in the Netherlands, but the opportunities for abuse continue to increase, as does the complexity of doing anything to counter that abuse. Jihadis are interested in cyber attacks and they have the knowledge and resources to undertake them, as well as the intent of striking at Western economies. The fact that this might not involve martyrdom may attract jihadis as well as

putting them off, but we need to bear in mind that this may in fact be quite attractive to Dutch jihadis. The scale of the threat will depend primarily on: (a) the extent to which terrorism continues to develop throughout the world, (b) whether there are any effective measures to be taken against other types of attack, leading to a possible shift of emphasis, and (c) the measures that can be taken to deal with the Internet's vulnerabilities as well as those of the physical and virtual targets associated with Internet.

3

3.1 CONTEXT AND FORMS OF INTERNET USAGE

Despite the fact that jihadis advocate a return to the days of the glory of Islam, and complain about the pernicious influences of the West, they use the Internet as a resource for a range of purposes, just like ordinary citizens. Jihadis regard the Internet itself as a crucial resource for jihad, which it also propagates. *"This is the Internet that Allah has taken over to serve the jihad and the Mujahideen, that has come to serve your interests - as half of the Mujahideen battle is fought out on the Internet pages - the sole channel for Mujahideen media".*[1]
The fact that the Internet is regarded as a crucial resource is also perfectly obvious from a speech by a well-known Syrian Islamic spiritual preacher and former leader of Al Muhajiroun, in these terms: *"We have no problems with technology. Other people use the Web for stupid reasons, to waste time. We use it for serious things."*[2]

While this study is aimed specifically at jihadis, we cannot avoid also looking at Salafism at some points. Salafism can be described as an orientation within Sunni Islam. Within Salafism, the central issue is the reversion of Muslims to what is called the "pure Islam". What the Salafis understand by this is a practice of the faith as formulated by the Salafs, literally meaning ancestors. The term Salafs refers to the Prophet Mohammed, his disciples and his immediate followers. Most present-day Salafis interpret this return to pure Islam in an ultra-orthodox, puritan manner. They assert that true believers must focus on the Koran and the Sunna literally in every aspect of their lives. Salafism consists of a variety of factions. For the purposes of this study, we will make do with mentioning the two most important of these: the non-jihadi and the jihadi (violent) forms of Salafism. The non-jihadi form of Salafism wants to ban "heretic" influences from Islam and to bring Muslims back to the "pure Islamic way of living". The jihadi form of Salafism asserts that pure Islam will not be safeguarded merely by banning heretic influences from the personal lives of every Muslim. Armed conflict also needs to be waged against the enemies of pure Islam. When we mention Salafism in this study, what we mean by this is the non-jihadi form of Salafism, with "Salafi" referring to the supporters of this variant. This is in contrast to the jihadi form, which we refer to using the expression "jihadis".

To some extent, jihadis' use of Internet is plain to see for anyone who logs on to the Internet. Sometimes it takes a little more effort to trace jihadi use of the Internet, but it is still possible. It might, for example, involve using a username and password. Some of the jihadi Internet usage, however, goes on behind closed doors on the Internet. These are the secretive activities, which would remain unspotted without the application of special powers available to investigation and security agencies. Obviously we know more about the visible activities than the secretive ones, so that this study focuses primarily on the visible element.

1 Benschop 2006a, referring to S. Ulph, 'Mujahideen to Pledge Allegiance on the Web', in Terrorism Focus, 2, 22 (29 November 2005).
2 Higgins et al. 2002.

This chapter opens with some general background relating to jihadi Internet usage (section 3.2) and an analysis of the Dutch situation (section 3.3). Sections 3.4 to 3.10 then go on to explore the following forms of Internet usage in depth: propaganda, acquisition of information, fundraising, recruitment, training, mutual communication and planning, and the creation of virtual networks. Each section concludes with an assessment of the threat of the particular form of Internet usage for the Netherlands, albeit viewed in an international context. Section 3.11 goes on to analyse the extent to which Internet usage influences radicalisation, and how it does so. The chapter concludes with a final assessment.

3.2 BACKGROUND

3.2.1 Introduction

This section outlines a general picture of jihadi Internet usage. We will deal with (a) the advantages of the Internet for jihadis, (b) their modus operandi and the extent to which they are conscious of their own security on the Internet, and (c) the rise of the virtual jihadi community.

It is of considerable importance to appreciate that we cannot study jihadi Internet usage in isolation from general developments in society, on the Internet and in Jihadism. Thus Internet usage in our society has increased significantly in recent years, as has the bandwidth of the Internet. Where an ADSL connection was too advanced for many private individuals a few years ago, a large proportion of households now have a permanent fast link with the Internet. Another factor is that jihadis in the Netherlands are often in the younger age group, and they are often the first to use new information technology. Where the creation of a website might still be shrouded in mystery for those over the age of 40, it poses no problem whatsoever for many younger people. Youth culture encompasses Internet usage, as well as challenging the established order and provocative behaviour; this is a culture by which young jihadis can at the very least be influenced, and one which they can also take part in. Within the international jihadi movement, there is more by way of inspiration and imitative behaviour than direction from the centre. It is hardly surprising in this context that jihadi usage of the Internet is continually developing, that Dutch "virtual" jihadis are being inspired by foreign jihadis and that they are adopting similar behaviour without there being any direction from outside.

3.2.2 Advantages of the Internet for jihadis

The Internet as a new medium has some unique characteristics. New, and opposed to telephone, television and radio, is that the eyes, ears and lips have a part to play, as well as the interactive nature across the whole spectrum ranging from one-to-one communication to communication by many people with many others, and with no restrictions as regards place and time. The multimedia characteristic is also new: text, video, audio and photographs. Another aspect is that the separate technologies and infrastructures such as those pertaining to television, radio and data communication are becoming more and more integrated.

The advantages of the separate media are therefore available in combined form. While those wishing to issue a message via newspapers, television or radio are still dependent on editors and journalists, along with the characteristics of the specific medium, anyone can, as it were, create his own newspaper, television or radio station for next to no cost via the Internet. Individuals and organisations are both consumer and producer, and they are in a position to determine for themselves what they receive and what they send. As either consumers or producers, they can also remain anonymous to a certain extent. Yet another attractive point is the limited amount or absence of regulation, censorship or other forms of government control.[3]

This chapter will show that jihadis exploit these advantages. Thus they make full use of the multimedia nature, focusing on several target groups. They do so in the form of, for example, video broadcasts via the Internet, digital magazines, animations, cartoons and one-off messages, and by making extensive use of banners, logos and music (battle songs) with a jihadi background.

3.2.3 National & international modus operandi and security consciousness

Abu Musab as-Suri, strategist and ideologist of the jihadi movement and Al Qaeda, has developed a model for what he terms 'virtual jihadi resistance brigades'. This model operates as a source of inspiration for the modus operandi of the jihadi movement on the Internet, and can be summarised as follows.

Muslim youngsters who are interested in joining the jihadi battle must set up their own completely independent jihad brigades. These brigades operate without any functional connection with the central leadership. The only connection maintained is the communal ideology and aim. These resistance brigades can be divided into three types. The first are the *initiating* and *setup brigades*, who arrange for the recrutment and initial training of new members in all sorts of areas, including ideological, security and military techniques.

The second type comprises *operational brigades*, directly involved at the front line. The third type is made up of the *clandestine mobilisation brigades*.

These jihad brigades are made up of individuals who are outstandingly equipped in areas of Islamic knowledge, as well as politics, intellectual and media matters. They are people who are also well versed in the use of the Internet and IT networks. According to as-Suri, knowledge about the Internet and computer technology is part of the jihad warrior's basic equipment. The initiating and setup brigades are, as it were, "information brigades", whose duty it is to spread the jihadi message by means of literature, research, publications and particularly by covert communication media such as the Internet. They translate articles, publications and news reports concerning the resistance into all Muslim and world languages. These brigades are supposed to deal with security surrounding the dissemination of materials. They develop their own working methods and adapt to the local circumstances of the countries where they work.[4]

3 Kortekaas 2005, p. 98-99, Castells 1998, p. 60-65, Weimann 2006, p. 23-31.
4 Translation from the Arabic of as-Suri, p. 1336 en 1408-1410.

The virtual jihadis operate in a professional manner and are back online very quickly - under a different name and using a different provider somewhere abroad - if they are removed as a result of official judicial intervention. They also shift locations spontaneously quite frequently. Sites that have used the same name for a while gradually acquire fewer visitors, because users start to worry that the security services are keeping an eye on them, or perhaps are even running them. It should also be noted that most jihadi websites contain a great deal of up-to-date information, for example in the form of high-quality multimedia files or commentaries on current events. The sites are very actively managed, with any undesirable content being removed and with counters to record site visits.

Most of the Islamic sites openly supporting the jihadi battle operate from American servers.[5] In 2004, out of 21 Hezbollah sites promoting martyrdom and terrorist activities, 19 of them were using the services of American companies.[6] The popularity of American servers is also evident from other sources. This is partly attributable to the reliability, accessibility and technical advance of the servers, along with the fact that they can deal with many visitors at one time, and partly because of the constitutional freedom of expression. American servers accordingly contain a great deal of anti-American material.[7] European and Asiatic service providers (web hosting businesses) are also used, including some in Malaysia.

Organisations sometimes abuse the free space on servers that they do not own (see section 3.2.3.2), and jihadi websites appear to be making more frequent use of service providers to offer web space for free (or at minimal rates), the 'third party file-hosting services'. The primary use is to make audio and video material available. The use of this type of service gives rise to greater continuity in the enormous supply of material, and also creates a shadow address, since the jihadi material is hidden behind an unsuspected and unquestioned Internet address. The space available also offers facilities for providing downloadable files in various formats. Thus, at the start of 2006, al-Zawahiri recordings were available in three formats via a file-hosting service: mp3 (audio), RealMedia (standard media player) and mpg (a format suitable for burning video CDs).[8]

The suppliers of jihadi websites and materials, together with any customers seeking information, all appreciate that the Internet may well be a sanctuary, but at the same time it is not a completely anonymous sanctuary. The reason is that many companies and software applications collect information on users, their interests and their surfing behaviour. Police and security services also use the facilities offered by the Internet in this context. Whenever someone connects to the Internet, he can in principle be traced using the unique IP address of his computer. Jihadis accordingly do their very best to remain anonymous and use various facilities for this, including working from Internet cafes. It would be going too far to deal with these facilities at any great length here. The fact is, however, that these facilities are discussed on jihadi sites, and there are pointers as to how they can be used.

5 Bunt 2003, p. 207.
6 Weimann 2006, p. 231.
7 Benschop 2006a.
8 SITE-Institute 2006a

Jihadis also do their best to keep any spies out of their camp. Some jihadi websites are protected by passwords, although this is often not much of a barrier. A more extensive form of protection is that new users have to be introduced by one or more respected users. They also set up barriers by challenging each other intellectually, so that anyone with a limited knowledge of Arabic and Jihadism will quickly be sifted out. If a user is just looking around and not playing an active part, or if he voices contrary opinions, he will be removed. Another trend is that an ever-expanding registration form has to be completed (including reasons for participation, and often in Arabic) and passwords are only valid for a brief period.

Jihadi security consciousness is also apparent from several reports containing tips and warnings, which appeared in 2006. They related, for example, to the use of Google, Google-Toolbar[9] and the potential risk of this application being deployed as spyware.[10] Some attention was also paid to the way in which the Saudi authorities, for example, monitor and trace users of web forums, and there is an indication that e-mail addresses ending in .sa can never be safe, because the Saudi security services would always be able to have access to them.[11] Jihadis are also conscious of "enemy" cyber attacks against their own sites, and they exchange tips on how to deal with these. Jihadis also warn each other if there is a presence on the part of the investigation or security services on the discussion forums.[12] A recent phenomenon is the setting of honeypot traps for those who fight terrorism. This might, for example, involve the use of a tactic such as dissemination of previously arranged passwords, so that the investigation and security services are recognisable when they connect with web forums, but it may also involve physical meetings. This would mean false information being passed over, so that the recipients became susceptible to detection.[13] The victims of this type of campaign might also include others such as investigative journalists.
None of the publications by jihadi groups and spiritual leaders contain any copyright details. On the contrary, many publications are provided with the following recommendation: "Copyright does not apply to this publication. Use it in accordance with the wishes of God and the Prophet". Training manuals for preparing and carrying out jihadi campaigns do, however, impose a restriction on their use. The user is asked to swear an oath that "the knowledge acquired will not be used against Muslims".

3.2.4 The structure of the virtual jihadi community, with examples

3.2.4.1 The structure in general terms

The virtual jihadi community consists of a large number of web sites, web forums and weblogs put together by terrorist groups and sympathisers. While there may be several different ways to categorise these, we shall describe them using the following subdivisions:

1. Official sites of jihadi organisations;
2. Sites of jihadi scholars;
3. Other websites, forums and weblogs;
4. Distribution channels.

9 SITE-Institute 2006q.
10 Washington Post 2006.
11 SITE-Institute 2006r.
12 Our own experience on a forum on 04.01.06.
13 Newsbytes 2006.

It should be borne in mind that the boundaries between these categories are not always clearly defined. Some sites playing an important part in the distribution of material, for example, also operate as web forums. This is certainly the case for those websites described by some as "mother sites". They operate as stable, authorised and primary sources of information, particularly for theological questions, ideological debates, strategic issues and official doctrines and press releases.[14] The mother sites often have "mirrors", copies that are ready to be put on line if necessary. Uploading mirror sites may be necessary following intervention on the part of a (government) organisation to take the website offline, or if they become victim to some private "Internet avenger".[15] It may also be the case that the website is a *"parasite"* (see section 3.2.3), which is caught and then removed from the server in question.

3.2.4.2 Official sites of jihadi organisations

Many jihadi organisations have a presence on the Internet. Some of these are mentioned below. The core of Al Qaeda is represented as well, of course. The original and official alneda.com website of Al Qaeda was registered in Singapore at the end of the 1990s and could be found on the Web servers of various providers in Malaysia and the USA (Texas).[16] Al Neda ("The Call") contained editorial articles written by the important leaders of Al Qaeda. These called for the commission of terrorist activities and contained extensive legitimation for attacks that had been carried out. The site's discussion forum contained a number of relatively innocent messages, which were presumed to contain coded signals. The multimedia section included photographs, audio files and videos of Osama bin Laden.[17] The site wandered around after being removed at the request of United States. The domain name registration expired at the end of 2002 and then went into private ownership. The result of this was that the Al Qaeda site became what is termed a "parasite", using a Web server software error in order to abuse the space of an existing legal site: it is a type of technique mentioned in the GIMF hacker compendium (see section 2.2.5). This parasitic activity was discovered on a regular basis, so that the parasite wandered around between September 2002 and April 2003. The site then returned independently under the name of faroq.com, carrying an Al Neda banner. This site initially focused on the war in Iraq, but the original content of alneda.com slowly reappeared on the site.[18]

Another Al Qaeda website was the *Center for Islamic Studies and Relief*. This website had contributions from Abu Gaith en al-Zawahiri, who published his declaration of war against the USA there. The site was also the source of the bi-monthly magazine *Sawat al-Jihad* or *The Voice of Jihad*. Its initial edition was primarily devoted to Internet propaganda, and the magazine provided some insight into one of Al Qaeda's principal aims, the generation of support from the public at large and legitimation among Muslims.[19]

While the official Al Qaeda website is not accessible at the moment, Al Qaeda is still represented on about 50 sites[20] used for propaganda and distribution purposes. These sites form part of the major distribution and communication network for this organisation, which is hunted in the real world but which manages to retain its elusiveness in cyberspace. The jihadis in Iraq are also actively involved on the Internet. The best-known of these are *Islamic Army in Iraq* and *The Islamic front of Iraqi resistance*. The Islamic Army in Iraq website offers communiques, articles, books, information on operations and two online magazines, al-Fursan (The Knights) en al-Kata'ib (The Battalions). There is also a section entitled "Fight with us", where visitors are urged to take part in the jihad.[21]

14 Lia 2006.
15 Benschop 2004.
16 Weimann 2006, p. 67.
17 Benschop 2004.
18 Weimann 2006, p. 68.
19 Weimann 2006, p. 44, 68.
20 Weimann 2006, p. 65.

3.2.4.3 Sites of jihadi scholars

Jihadi scholars publish their ideologies in texts, pictures and sound, set up hyperlinks (electronic references) to what they consider to be other influential sites, and can communicate directly with interested parties via e-mail and chat programs such as Paltalk or Instant Messenger. As-Suri is particularly popular among jihadis. He has a very large body of work to his name, amounting to about 1600 pages (see also sections 3.2.3 and 3.8). The work originally appeared in Arabic but some parts have now been translated into English. Bearing in mind the increase of material translated into Dutch (see section 3.3.4), it is only be a matter of time until translations of the work of as-Suri appear in the Netherlands and start to be used there.[22] Abu Basir al Tartousi is also an influential jihadi scholar offering a large amount of information and knowledge, including commentary on recent developments in the Middle East, the West and particularly in the United Kingdom. We should mention that these sites are regularly offline and that they often change their location. This does not detract from the fact that this type of site is very popular and that the material from these sites is being spread on an increasingly wider basis.[23]

3.2.4.4 Other websites, forums and weblogs

A more interactive variant of jihadi Internet news can be found on the web forums and weblogs. The web forums operate in the first instance as discussion platforms for a variety of matters, from current affairs through to preparation for the jihadi battle. Many of these forums have heavy visitor numbers. Apart from the discussion element, they provide hyperlinks to important websites, materials and treatises.

In addition to the popular web forums, there are also jihadi weblogs or "blogs". These are frequently not concerned with the original function of a blog, which is the circulation and discussion of current opinions. In such cases they operate more as a distribution channel providing hyperlinks to the most popular jihadi sites, a type of electronic bulletin board. The advantage of these blogs is that they suffer no interference from fake and disruptive postings, but this also means that they are much less interactive. This is exactly why their popularity might well increase. The ideology can be circulated quickly, currently and without disruption.[24]

All in all, many jihadi blogs are a cross between interactive sites and distribution sites (see following page).

21 Rogan 2006, p. 19.
22 Interview 5.
23 Rogan 2006, p. 32.
24 Rogan 2006, p. 22.

3.2.4.5 Distribution channels

The distribution channels can be subdivided even further into those of directory sites, fan sites or support sites, and production companies. Professional *directory sites* contain very extensive and up-to-date HYPERLINKS to jihadi websites, such as locations for downloading files, forums, news sites, sites of Sheiks, sites with lists of martyrs, and so on. An example of a professional and stable directory is Dalil Meshawir, which is available in English and French versions.[25] The distribution channels lack a well-defined structure, as is usual on the Internet. There is accordingly no hidden central steering or direction.

Some distribution channels are formed by *fansites* or *support sites* set up by amateurs (and computer experts). The sites look well-designed from a technical perspective, but they are also sometimes obviously set up by amateurs and are therefore not always stable or up-to-date. The primary duties of fansites and support sites appears to concern the distribution of material as widely as possible, which has been derived from mother sites and other locations such as the online Al Qaeda magazines *Sawat al-Jihad* en *al-Battar*. Sometimes they may only function as a "portal", which means that they principally offer hyperlinks to other web sites or download locations. Others may offer a sort of encyclopaedia of specific files or hyperlinks to this type of file, focusing for example on training or weapons. Some of the fansites or support sites accordingly operate as directories.

Figure 3.1 Examples of support sites

al-Muhajiroun (UK). This website has sections on Ramadan and conferences but looking past this information it is possible to trace a piece on 'Aqd Al Amaan', or 'The Convenant of Security'. This covenant is to the effect that Muslims in the West may not attack the country where they live. Other Muslims, however, are allowed to attack these same unbelievers. The website talks at various points about "the magnificent contemporary Mujahideen and Martyrs", "the magnificent 19 of 9/11", "the domination and influence of the kufr states" and "This book.... gives an Islamic solution to the Cancer known as America".

Supporters of Shareeah, the site of Abu Hamza al Masri. This is a really modern site using flash technology and multimedia. It is strongly propagandist in nature and appears to support or glorify suicide attacks.[26]

Tajdeed.org.uk, a support site for the Saudi dissident Mohammed al-Masari, registered in London. The sect called the bomb attacks on the London underground a "victory for fundamentalists".[27]

A third variant of distribution channels comprises the *production companies* or media groups, such as the Global Islamic Media Front (GIMF) and as-Sahab, the (alleged) Al Qaeda media company. They circulate the material from the mother sites but also put together media productions themselves, frequently based on authorised material, for example in the form of compilations or compendiums, such as the hacker compendium.

The GIMF is one of the most important mouthpieces of Al Qaeda and is responsible, among other matters, for the professionally produced jihadi Internet journal *"Voice of the Caliphate"*. The status of the GIMF can partly be inferred from the fact that Al Qaeda has apparently indicated that sympathisers should only take information seriously if it has been tested, approved and confirmed by the GIMF on Yahoogroups.com.[28] In any event, the GIMF presents itself as the focus (they use the word "Qa'ida", or base) for jihadi, anti-Jewish propaganda on the Internet. The fact that they take their work seriously is apparent from the fact that the GIMF called on people who were experienced in the area of video production and editing websites (such as IT and communication experts, film producers and photographers) to make contributions.[29] The GIMF frequently translates its productions into English and French, but has also recently translated particular statements from the *Mujahideen Shura Council* and video productions from as-Sahab into German, with these t hen being placed on a website.[30]

The media group as-Sahab is responsible for the video entitled *"A letter to the people of the West, in occasion of the four year anniversary of the attacks of New York and Washington"*, which is a 45 minute long interview with al-Zawahiri made in September 2005 and issued in December of that year. All eight of the video messages by al-Zawahiri broadcast in 2005 bore the as-Sahab logo. The recordings have become more and more professional, using logos and English subtitles. In the first half of 2006 alone, three audio recordings by Bin Laden and six recordings from al-Zawahiri have already appeared via as-Sahab.[31] A video marking the anniversary of the attacks in London on 7 July 2005 was issued at the start of July.[32]

3.3 JIHADISM ON THE DUTCH INTERNET

3.3.1 Introduction

Like many other Western countries, the Netherlands has had to cope with virtual Jihadism on the Dutch Internet for some years. We can use the term 'Dutch Internet' if a website, forum or similar (1) is in Dutch, (2) is oriented towards the Netherlands in one way or another, or (3) is facilitated either physically or virtually from the Netherlands or operates in the Netherlands. The criteria for a jihadi website are incorporated in appendix 2.

Information in this section is based primarily on findings while monitoring the Internet, and a content analysis of the material found on sites on line (until at least May 2006) and in open sources. Our overview of jihadi websites is not complete. The sites we discuss have been authoritative ones over the last four years, as they are or have been widely known and

25 Rogan 2006, p. 22, 'Dalil' means 'my index'.
26 Both examples taken from Weimann 2006.
27 Cops@Cyberspace 2006a.
28 Weimann 2006, p. 228.
29 Benschop 2004.
30 SITE-Institute 2006e.
31 NRC-Next 2006.
32 SITE-Institute 2006k.

have attracted media or political attention at certain times. In addition, a website is only mentioned by name and designation if it is no longer in existence, in order to avoid current sites suddenly registering a lot of extra visitors.

First of all, we indicate the typical characteristics of a Dutch Salafi website. We go on to describe the jihadi sites on the Dutch Internet and then the Dutch virtual jihadis. We conclude with a summary of our findings.

3.3.2 Salafi sites in the Netherlands

The Dutch Internet has a large number of sites with an Islamic identity and character. While there are some neutral sites, the lion's share are Salafi. In general terms, Salafi websites can be subdivided into three categories. First of all we have the sites principally aimed at Salafi teaching of dogma, worship and ethics. These are, as it were, apolitical sites, conscientiously attempting to avoid political issues and therefore topics dealing with the jihadi battle.
The second category consists of a limited number of Salafi sites, which avoid open criticism of the regimes in the Middle East, and which are probably encouraged by the Saudi state. The majority of these are dominated by the Dawa, the promulgation of the Islamic faith and the conversion of native Dutch citizens. One important function of the sites is the creation of a Salafi community of faith. To the extent that these sites deal with current affairs, their attention is devoted to the Palestinian question, the war in Iraq and Afghanistan. This involves incorporation of news reporting by the Western media without any commentary.
The third category could be described as comprising "hybrid" sites. These sites propagate the Salafi ideology, but by implication they approve of, or at least do not explicitly distance themselves from, the jihadi battle.

The jihadi Internet sites in the Netherlands can be distinguished from the Salafi ones because of the explicit politicisation of their theological, dogmatic, liturgical and ethnic principles and a call to the (armed) jihadi battle.

3.3.3 Jihadi sites in the Netherlands

3.3.3.1. Three periods

The earliest manifestation of jihadi terrorist movements in the Netherlands occurred around 2000. The terrorist threat to the Netherlands was inferred from the international threat.[33]
In 2002, the terrorist threat was converted from an external one to an internal one.
In 2003, the jihadi warriors explicitly turned their sights on the Netherlands as a target.
The development of jihadi websites followed this pattern in broad terms.

The first jihadi websites that the Netherlands had to deal with were either established abroad or aimed at events abroad. Arabic was the primary language used. The position changed in the course of 2001, however. Sites appeared that were focused specifically

33 AIVD 2002a, p. 21.

against the Netherlands or that had been set up by Dutch jihadis, albeit still with a foreign orientation. Later still, around 2003, some Dutch jihadi sites appeared, which were focused on the jihadi battle in the Netherlands. There are accordingly three, sometimes overlapping, categories to be distinguished, and these can also be viewed in terms of periods:
1. jihadi sites in the Netherlands focusing on events abroad;
2. Dutch jihadi sites with a foreign orientation;
3. Dutch jihadi sites focusing on the Netherlands.

3.3.3.2. Jihadi sites in the Netherlands focusing on events abroad

There were no jihadi websites prior to 2001 focusing specifically on the Netherlands in terms of language, content and orientation. As far as we know, this category includes three sites bearing some distinct relationship with the Netherlands, namely:

- *www.qoqaz.com*, a site in Arabic, supporting the jihadi battle in Chechnya. In 2002, certain jihadi-oriented individuals from the Netherlands placed postings on this website, and in June 2002 two individuals from the Netherlands made brief contributions to the discussion forum.
- One site hosted by a Dutch company;
- *www.alneda.com*, an Al Qaeda site, which at one point used hacked web space owned by a Dutch football club. One of the documents on this was an address by Bin Laden.

3.3.3.3. Dutch jihadi sites with a foreign orientation

The jihadi players behind these websites operated from the Netherlands, developed various Dutch language Internet environments, focused on the Dutch population and explicitly called on Dutch youths to take part in the jihadi battle. We shall deal with two sites from this category.

The site *www.qoqaz.nl* was the first fully-fledged jihadi site with a full range of appropriate functionalities: audio-visual content, news headlines and interactive applications (e-mail and forum). This site originally focused on the jihadi battle in Chechnya and published articles, photos and videos on this. But in March 2001, it published an article in which Muslim youths in the Netherlands were called on to participate in military training as a preparation for the jihadi battle. Interested youngsters were referred, for example, to the recruitment offices of the Royal Netherlands Army, and lots of advice was given. The website was closed in April 2001, but surfaced again in 2003 and in April 2004.

The site *www.geocities.com/sluitjeaan* is thought to have started in the spring of 2003. The name 'sluit je aan' ["join up"] refers to a publication by Abdullah Azzam, a pre-eminent jihadi and co-founder of Al Qaeda. This web site focused clearly on the jihadi battle in Afghanistan, Chechnya and Palestine. The site opened with a general ideological and political treatise in Dutch and English. It was, in fact, a Dutch version of the jihadi website already established in Great Britain, *www.azzam.com*. The focus gradually shifted towards targeted calls to prepare

for participation in the jihadi battle. A call to Muslim youngsters to participate in the jihadi battle appeared in September 2003. The site did not have its own independent domain on the Internet, but rather used subsidiary space offered by an Internet company. Interactive functionalities were limited, but the site specifically invited visitors to make a contribution and encouraged their input. It disappeared following some commotion in the media and politics about the publications on these sites, only to reappear at a later date at a different Internet location. The website was then immediately taken off the air again.

3.3.3.4. Dutch jihadi sites focused on the Netherlands

A number of jihadis were active on the Internet in the course of 2003. They were particularly active in MSN groups. A new MSN group surfaced in the spring of 2004, with two websites of an outspokenly jihadi nature (MuwahhidinDeWareMoslims, 5434_, Tawheed_wal_Jihaad) and other static Internet pages of limited size.

The content of the various MSN groups and sites was focused on the theoretical and dogmatic aspects and also on the practical and operational aspects of the jihadi battle. They appeared in many respects to be similar to each other. The proliferation of jihadi MSN groups in 2004, along with the extensive use that was made of them, can perhaps be explained by the simplicity of the application of this facility and extensive use of MSN among young people. The MSN groups were born and designated with explicitly jihadi names. They would disappear for a brief period, only to reappear elsewhere under a new name and new outward appearance. The MSN groups provided an indication of the level of development, Internet skills and also strategic orientation of the Dutch virtual jihadis at that point. They allowed experience to be gained in the design and content of a jihadi website.

Figure 3.2 Summary of jihadi MSN groups (except for two still on air)

Name	Period
De Basis	*January 2003-March 2004*
De Basis2	*March 2004-July 2004*
MuwahhidinDeWareMoslims	*July 2003-January 2004*
	July 2004-September 2004
ElKhatab	*August 2003-September 2004*
al-ansaar	*March 2004-July 2004*
Shareeah	*April 2004-September 2004*
*5434_*	*March 2004-October 2004*
Tawheedwaljihad	*August 2004-October 2004*
Tawheedwalqitaal	*August 2004-October 2004*
Nlboeken	*December 2004-February 2005*
Ahloetawheed	*October 2004-February 2005*

The jihadis underwent self-development, used new Internet functionalities and graduated in 2004 to using the free .tk domains and Freewebs in order to set up their own web sites. The .tk domain can be associated with any other website, web page, homepage, web profile, weblog, blog or web gallery. Registration is a straightforward matter. Use is free, although the web pages carry advertising. On Freewebs, private individuals, companies and institutions can enjoy free hosting including a domain name. This has no associated obligations or costs, and there is no compulsory advertising. It is really straightforward for anyone to obtain a website online via Freewebs.

The use of the free .tk domains and Freewebs by jihadi groups in the Netherlands offers a financial advantage, needless to say, but also advantages in terms of security. Maintaining one's own paid site, after all, requires registration, administration and protection, whereas a free hosting provider does not often ask for (accurate) registration, and the user benefits from the professionality of the hosting company as regards protection, technical know-how and the stability of the service provision. Figure 3.3 summarises some of the .tk domains and Freewebs.

Figure 3.3 Jihadi .tk domains and Freewebs (except for two still on air)

Name	Period
www.twaheedwaljihaad.tk	*June 2004-September 2005*
www.tawheedwalqitaal.tk	*September 2004-May 2005*
www.ahloetawheed.tk/	*May 2004-November 2004*
www.freewebs.com/aqeeda	*January 2005-April 2006*
www.freewebs.com/poldermujahideen/	*February 2005-November 2005*
www.freewebs.com/overigeinfo	*September 2004-February 2005*

The first independent Dutch jihadi website opened in the second half of 2005, and was thereafter expanded and diversified as regards its subject matter and areas of interest. The site was no longer operational at the start of 2006, and it was announced some time later that the website would definitely be staying offline. This site outdid its predecessors in every respect and focused both on the jihadi battle and on the dissemination of Salafi ideology in the Netherlands. This site clearly preached and promoted the jihadi battle while refraining from being guilty of incitement to violence or explicitly stirring up hatred, and it offered a good overview of Salafi activities in the Netherlands at the time. One of the sections in the forum distributed the literature of the Hofstad group, particularly the translations and writings of Mohammed B., but also newly translated literature. The site was professionally set up as regards form and content. The quality of the Dutch could be described as being good to very good. The development, operation and maintenance of this type of site presumes the existence of a dedicated, supported and professional grouping.

Weblogs and the use of Paltalk together form yet another phenomenon in the Dutch jihadi context. The first weblog with an explicitly jihadi orientation dates from mid-2005, but disappeared from the web in December 2005. It contained a number of publications and statements by the 'Leeuwen van Tawhied' ["Lions of Tawheed"]. There are also a number of weblogs whose content is not specifically focused on the jihad, but which include articles relating to current topics in jihadi ideology. They also contains songs relating to the jihad in Arabic. Salafi and jihadi groups are also making increasing use of Paltalk. This is a free chat program, supporting direct speech. It allows people to participate in discussions or to listen to them anonymously. Arabic is often spoken in a number of so-called Paltalk rooms, while Paltalk also makes it possible to speak in many other languages. By communicating in Arabic, anyone who does not speak Arabic can be knowingly or unknowingly excluded from the discussions.

In addition to setting up their own web sites, it is noticeable that Dutch jihadis also aim at neutral websites and forums that might be popular with their potential target groups. Some examples of this include postings in features where the public can respond to allegations or news items, and on random websites. Virtual jihadis also take part in the discussions on a regular basis. On some of the forums, any deviant ideas or suggestions of Salafism meet with a fierce counter-reaction from some of the "forum controllers". There is a notable dissemination of Al Qaeda literature on political, ideological and strategic matters, recently translated into Dutch, through discussion forums. These are first published on various discussion forums as individual postings or articles. The intention behind this is to promote discussion among the site visitors. The publications are then circulated widely via other forums and Internet sites. The translated literature will later appear as a publication, issued by a virtual publisher or individual/group. Once the publications are translated, they are published repeatedly on various forums and sites. In this way, the Hofstad group documents keep appearing on the Internet either as a text file or in a new layout and format. A trend has been apparent since the start of 2006 with regard to the mass placement of hyperlinks to Arabic language jihadi audiovisual productions on neutral websites. Operating on neutral sites offers certain benefits, namely:

- preventing the detection of individuals and structures underpinning the website;
- avoiding losses resulting from removal and campaigns by police and security services;
- acquiring legitimacy and legality without exposure to public condemnation;
- increasing awareness among a broader public;
- maintaining contacts and communicating with the broader public.

We can deduce that this tactic may well be necessary in order to reach a wider audience from an investigation showing that Moroccan and Turkish youths in the Netherlands specifically visit general Dutch sites, as well as sites for Turks and Moroccans living in the Netherlands. Only 5% of their surfing consists of visits to Turkish, Moroccan or other international sites.[34] While this abuse of neutral websites and forums does not provide a

34 Holst 2006, p. 12.

distinct image on the Internet, it is nonetheless a crafty method for propaganda and recruitment. The jihadi message reaches a much wider audience, with new possibilities for growth, but with a more limited risk of intervention by government authorities.

3.3.3.5 Classification of Dutch jihadi sites

We indicated at an earlier stage that it is very important to realise that jihadi Internet usage cannot be viewed in isolation from general developments in society, on the Internet and in Jihadism. We referred specifically to the fact that Internet usage by young jihadis in particular cannot be viewed separately from youth culture, and that the international jihadi movement is characterised more by inspiration and imitation than by central leadership.

Until now, Dutch jihadis have focused primarily on compiling, offering and disseminating information and materials from jihadi spiritual, strategic and operational leaders, as well as referring to that material on English and Arabic sites. In so doing, they operate primarily as intermediaries between the original producers of the material and end users, although they may of course be end users themselves. This transfer of information coincides with the language, culture, mentality and perceptions of Moroccan youths in particular. It ensures an effective transfer of the jihadi message. The sites are increasingly offering translated materials, simplifying the transfer to a specific Dutch target group. This information primarily serves a propaganda purpose, but is to some extent also focused on training, and we shall refer to these aspects in greater detail at a later point in this chapter. These sites should be viewed principally as distribution channels (see section 3.2.4.5).

In addition to being distribution channels, many sites offer the facility of interaction between jihadis and a wide and varied audience of interested parties, as well as between jihadis themselves. Input from visitors, participants and members is actively stimulated. This allows a completely targeted and customised exchange of information with interested parties, dealing with specific issues or current events. It also allows the creation of virtual networks of Muslims and non-Muslims (potential converts) who are interested in the jihadi battle. At the end of the day this even offers the facility for recruitment of those individuals who are truly interested in the jihadi battle (see also sections 3.8 and 3.7).

We should draw attention to a clear development, in terms of which the jihadis are now increasingly using the Internet's multimedia potential to support their activities in the Netherlands. Examples include a Dutch version of one of the video film clips of Al Qaeda in Iraq and a short film clip about Dutch MP Wilders. There are not yet any genuine, independent production companies (section 3.2.4.5).

When setting up the Dutch sites, therefore, the Dutch virtual jihadis have been inspired by the model developed by as-Suri for the virtual jihadi information brigades (see section 3.2.3). The production of audiovisual materials also coincides with the modus operandi of Al Qaeda

in Iraq and Saudi Arabia. This consists of the parent organization - which prepares, plans and implements terrorist campaigns - also setting up a parallel media organisation at the same time. The media organisation focuses on providing information to its supporters and recruiting new members. We cannot rule out this working method being imitated in the Netherlands as well. It is precisely on the basis of these (foreign) sources of information for Dutch jihadis that we can anticipate what to expect on the Dutch Internet.

There are indications that many individuals who are active in existing jihadi networks in the real world are also active Internet users. In any case, the study by Peters of the Hofstad group literature, and the analysis of how these documents have spread through the Internet, show that the Hofstad group also operated as a virtual organisation by providing foreign productions, arranging for translations/subtitles and even developing productions, frequently in the form of imitations. This virtual manifestation was complementary to the physical group. They also made clever use of the facilities of the Internet and information technology, such as setting up their own web sites, circulating information to public web sites and applying encryption. A virtual jihadi organisation can therefore be an indicator of a real-life jihadi organisation.

3.3.4 Dutch virtual jihadis

There are, of course, individuals, groups or networks hidden behind the substantial jihadi corpus on the Internet, of which the Hofstad group was one of the most important. A few members of the Hofstad group set up and maintained a number of MSN groups. In this way they made their own web pages with MSN groups, for example under the names "5343", the "tawheedwaljihad" and the MSN group Muwahidin/dewaremoslims. Based on Peters' analysis of the literature from members of the Hofstad group, which we mentioned above, and the analysis of the dissemination pattern of a number of documents from this literature, we can state that many of the MSN groups and sites we have already described as being active between 2002 and 2004 were clearly influenced directly or indirectly by the Hofstad group. The information produced by members of the Hofstad group was not only placed on their "own" sites, but also circulated by them in various discussion forums.[35] A number of moderate Salafi sites were also used to publish texts with a jihadi tendency. The Hofstad group's ideological literature was posted on various discussion forums of existing moderate Salafi sites and published in various innocent MSN groups in the course of 2003, and remains available even now. In addition to the theoretical articles on the jihadi battle in general, messages were also placed on these sites concerning the jihad in Iraq and Afghanistan, along with speeches by Bin Laden, al-Zawahiri and al-Zarqawi. Two other MSN groups, al-ansaar en shareeah, were maintained by Bilal L., who issued threats against the Dutch MP Wilders.

Monitoring of the Internet has also shown that what amounted to a virtual international translation network of jihadi literature from Arabic, English and French came into being in the course of 2005, and that it made intensive use of the Internet. The Dutch virtual jihadis found a point of contact here. On the one hand, the Dutch sites offer hyperlinks to these translations, and on the other hand the Dutch virtual jihadis get involved themselves in the translation of jihadi literature into Dutch. This shows that the Dutch virtual jihadis are being inspired in the formulation of their ideas by others based abroad, who take the initiative for a translation program. These others are looking for current information and are well-acquainted with the location of information on Arabic language jihadi websites. The selection of the pieces to be translated displays the presence of specialist knowledge. An analysis of the texts also shows that there is, as yet, no autonomy in terms of ideological know-how and production among Dutch jihadis. The level of conceptualisation and abstraction, along with the ability to apply knowledge and understanding to the Dutch situation, are not yet fully developed. Nearly all of the items translated into Dutch have already been translated into English and subsequently from English into Dutch. The English-language sites have already made a selection of the translated material on offer. The works translated from Arabic are also originally by others, rather than being prepared by the Dutch jihadis. This seems to show to a large extent that the majority do not have a good command of Arabic.

When compared with other European countries such as Great Britain, France and Belgium, the Dutch virtual jihadis can be distinguished by the active part played by women. Young Muslim women first became involved as members of the networks surrounding the Hofstad group. They also contributed to the development of Dutch language jihadi literature. They carried out documentary research on the English language jihadi-oriented websites and then translated this material into Dutch. Most of the currently available jihadi literature translated into Dutch was prepared by women.[36] These young Muslim women also play a prominent part in both the substantive development of the MSN groups/sites and in relationships with the public. Young Muslim women participate in discussions, pose questions and lodge messages on more general Islamic websites, but certainly also on Salafi and jihadi ones. During the hearing of Soumaya S., who was detained at the same time as Nouredine el F. and Martine van der O. in Amsterdam, she allegedly stated that she regularly visited Internet cafes in Amsterdam and The Hague, using Hotmail addresses. She also stated that she used nicknames and visited web sites to acquire information concerning her faith. She went on to state that she regularly chatted with Nouredine via MSN.[37] In their contributions, the young Muslim women romanticised their role in history and in the violent jihadi battle. This to some extent indicated their need for emancipation. They also tried to organise (discussion) meetings either on the Internet or elsewhere.[38]

As explained earlier, Internet usage by Dutch jihadis has to be viewed in the broader context of Internet use by young people. By placing postings and taking part in discussions, "would-be" jihadis are also trying to gain

35 Benschop 2004, p. 17, 27.

36 Source on this point, Volkskrant 2005.

37 KRO Reporter, 18 juli 2005, reported in Cops@Cyberspace 2006b.

38 Partly based on Nationaal 2006 and Nieuwsblad 2006. On the role of women, see also AIVD 2006, p. 40 and 48.

acknowledgement and respect. This means that what they say might be much more radical than how they actually are. Another point worth noting is the exchange of roles. Anyone can put himself forward as an expert using a nickname on one forum, while using a different nickname on another forum to ask questions of other "experts", so as to be able to "peddle" the knowledge acquired in this way. After all, the nature of the Internet is such that it is very easy to build up some credibility quite quickly, even at a young age and without years of study. This means that not everyone who expresses radical viewpoints will by definition pose a threat. Security and detection agencies have the difficult task of separating the wheat from the chaff.

3.3.5 Findings

The analysis in this section leads us to the following conclusions:

1. Dutch jihadis have hitherto focused primarily on organising, offering and circulating jihadi information and materials. This information is primarily for propaganda purposes, but is also to some extent focused on training.
2. Many sites offer the facility of interaction between jihadis and a wide and varied audience of interested parties, as well as between jihadis themselves. It is not just information, fully targeted and customised, that can be exchanged with interested parties, based on specific issues or current events, but this can also lead to the formation of virtual networks, or else the recruitment of those who are truly interested in the jihadi battle.
3. Virtual Jihadism on the Dutch Internet may be a pointer towards real-life jihadis in the Netherlands.
4. Dutch virtual jihadis take inspiration from an international, virtual translation program, and they mainly translate material taken from the range of "preselected" material made available by others.
5. Young Muslim women are very active as translators, in the development of sites and in dealing with the public.
6. Dutch virtual jihadis operate either on a structural basis or sporadically on a variety of neutral discussion forums of a non-jihadi nature. The jihadi message reaches a much wider audience, with new possibilities for growth, but with a more limited risk of intervention by government.

3.4 PROPAGANDA

3.4.1 Explanation

Terrorist groups try to achieve a political aim with their activities. They do so, for example, by carrying out attacks resulting in deaths and casualties. But they certainly also try to reach a wider and more general public, over the heads of their victims, in order to instil terror, influence decision-making, put their group on the map and recruit and mobilise sympathisers. In the notorious recordings issued in November 2001, where Bin Laden spoke about the attacks of 11 September 2001, he indicated that the perpetrators of the attacks had not so much committed an act as made a speech overshadowing other speeches, and one that would be understood the whole world over ("Arabs, non-Arabs and even Chinese"). We should note here that Bin Laden appears to regard terrorism primarily as a means of communication.[39] Propaganda accordingly forms a significant aspect of terrorism, because it substantially amplifies the impact of the attacks themselves.[40] Jihadis also regard propaganda as being a significant element of their strategy.

A distinction is frequently drawn between propaganda and psychological warfare. Jihadi propaganda might be understood to include selling anti-western, jihadi ideology to various target groups. It is clear here who is spreading material, which, additionally, is being handed to interested parties on a plate. On the other hand, people sometimes have to download something, for example, so that the propaganda is more subtle. Psychological warfare is the term used for instilling terror in order to influence the enemy and the enemy public. What this means in jihadi terms is instilling terror in the hearts of unbelievers. Propaganda is therefore primarily targeted at winning over souls and indoctrinating the support base and backers, whereas psychological warfare is aimed primarily at instilling terror in order to promote the desired political changes. Because propaganda and psychological warfare are so closely related, and because 'psychological warfare' is such an emotionally charged term, we will not make any distinction between them in this study. Some forms of propaganda are dwelt upon in our further discussion:

A the acquisition or retention of direct support and (larger-scale) backing (see section 3.4.3);
B influencing international public opinion (see section 3.4.4);
C influencing the enemy and the enemy public (see section 3.4.5);
D instilling terror (section 3.4.6);
E hacktivism (section 3.4.7).

There is not always a clear distinction between these various forms of propaganda, because a single message may serve a range of purposes and may be aimed at a variety of target groups. These are sometimes described as 'multi-target messages'. Instilling fear can also, for example, have some impact on recruitment. Sometimes terrorist organisations will specifically issue a peaceable, diplomatic message in order to wrongfoot the opposition and then foster legitimacy when the enemy subsequently refuses to negotiate, despite the peaceable proposals.[41] Thus Osama bin Laden issued an ultimatum on a number of occasions, and offered a form of negotiating perspective on 19 January 2006 and other dates. Various reactions showed that this method can be effective, as it appeared to be quite conceivable that the West might open up negotiations with Al Qaeda.[42] The pictures on jihadi websites of Abu Ghraib, the Iraqi prison where prisoners were abused by American soldiers, were also an example of multi-target messages, addressing friend and foe in a single message.[43] For the brothers, the pictures were even further proof of the depravity of the West, and proof that the West hated Muslims and regarded them as being of no value. The pictures might have the effect of raising some doubts

39 Weimann 2006, p. 40, referring to a report to Nacos, Terrorist Calculus.
40 Muller et al. 2004, p. 57-70, Weimann 2006.
41 Weimann 2006, p. 59.
42 Volkskrant 2006 and Zerkin 2006.
43 Weimann 2006, p. 61-64.

among the enemy. For a neutral public, this can mean that they develop sympathy for the position and/or struggle of the jihadis, who present themselves as victims. We might expect that, when planning their attacks, jihadis will take increasing account of the propaganda value of their actions, whether or not they are broadcast 'live' via the Internet.

The following section outlines the advantages of propaganda via the Internet. In subsequent sections we will then explore the various forms of propaganda. We will close with an assessment of the threat.

3.4.2 Advantages of the Internet for propaganda

The advantages of the Internet are discussed in section 3.2.2. There are some additional benefits, in comparison with traditional media, particularly in relation to propaganda. In most countries, the media in the form of television broadcasts and newspapers make the choice as to whether and in what form terrorist messages will reach the public, for example by way of television broadcasting. The material broadcast via the regular media is accordingly subject to framing, editing and possibly also censorship in many cases.

Framing is the selection of particular parts of a real experience, and making these more salient in the text in such a way that any particular problem definition, causal link or moral evaluation and solution are promoted in relation to the relevant subject matter.[44] In the case of the NOS journal, for example, there is widespread adaptation of Al Qaeda videos to a Western frame. One example of this is the video from December 2001, in which Bin Laden indicated that the attack on the World Trade Center had delivered everything he could have hoped for. The focus of the journal (and its host/specialist) is almost fully aimed at the authenticity of the recording on the one hand and the reliability of the translation on the other hand. The reason for this was the desire on the part of the West at the time for proof that Bin Laden was behind the attacks.[45] Internet broadcasts are not troubled by framing.

Another phenomenon with the regular media is editing, or editorial processing of the message. As-Sahab, one of Al Qaeda's production companies, issued a 52 minute audio message from Bin Laden on 26 April 2006. Al-Jazeera only broadcast 5:45 minutes of this and provided a commentary on those parts of the speech that were not broadcast.[46] Jihadis counter the editing process creatively by circulating short, pre-fragmented messages, so that these snippets of messages end up effectively being broadcast as a whole. Internet broadcasts are not troubled by editing, since they are fully under the control of the jihadis.

In addition, (government) censorship or control of Internet broadcasts is difficult, although it does happen in countries such as Singapore, China and Saudi Arabia. In Singapore, for example, all Internet traffic is monitored under the pretext of preventing cyber attacks, the government controls the three ISPs and all websites are screened for objectionable or insurrectionist content. In China, every Internet user must register at a local security office, which means that the government can check up on which Internet pages have been visited.[47]

44 Van Yperen 2005, and the reference to the definition by Entman, 1953 - translation from English.
45 Van Yperen 2005.
46 SITE Institute 2006d.

A further advantage of the Internet is that content of the messages can easily be tailored to various target groups in order to build up a profile, which is as powerful as possible. Jihadis have a fine understanding of this craft, which is also referred to as *narrowcasting*. They focus on children, Muslim women or the general public in specific Western countries, for example.

Finally there is the facility for repeating sermons, messages and videos. Repetition is important for hammering home the messages. The jihadis are particularly proficient at this. Forthcoming repeats and retrospectives are even announced, as in the case of the announcement of the retrospective on the attacks in London on 7 July 2005.[48] The use of such announcements *(teasers)* is also extended to announcing new items, statements or publications.[49]

Al Qaeda has come out openly in favour of the use of the Internet as a propaganda resource, as in an online Al Qaeda magazine in 2004, which included a promotion of Internet usage for that purpose.[50] As far as known, Al Qaeda has been pointing out to Muslims their "sacred duty" to circulate news and other items concerning the jihad as quickly as possible in other newsgroups, forums and sites since 2000. There has even been a threat of religious sanctions: Muslims must answer to Allah if a website containing Al Qaeda material is suddenly closed down before they have made the effort to effect a wider circulation of its contents.[51]

3.4.3 Acquisition or retention of support and backing

When we are talking about this form of propaganda, we have to refrain from merely looking at jihadis. Salafis (also frequently referred to as Islamists) actively attempt to win over souls to their ideology and to indoctrinate Muslims and unbelievers. This might be termed a "digital dawa", and in the Dutch context this means a sort of Dutch variant of radical Islam. We should point out that this does not automatically lead to an orientation towards religiously legitimated violence, but it does reduce the barrier towards propagating the jihad.[52] This *digital dawa* is not therefore really concerned with jihadi propaganda, but it can make individuals receptive to the jihad and operate to reduce resistance (see also section 3.11).

47 Weimann 2006, p. 180.
48 SITE-Institute 2006k.
49 SITE-Institute 2006o.
50 Weimann 2006, p. 105 on the Sawt al-Jihad magazine of February 2004.
51 Weimann 2006, p. 66.
52 AIVD 2006, p. 29-30.

The jihadis' intentions behind the propaganda aimed at acquiring and maintaining support and backing are as follows: 1) to give heart to former warriors and current supporters in a general sense and to confirm their existing perceptions of the depraved West, 2) to inspire young new (potential) jihadis, and 3) to convince the broader backing of the need for the organisation's existence and activities.

This form of propaganda manifests itself in a variety of ways, some of which are:

1. Official sites in local languages; these sites contain detailed information on internal politics and relationships with other groups.
2. Islamic sermons, speeches and video images of the jihad's successes, and evils perpetrated by Western, Zionist and Christian enemies.
3. Training material or manuals; these may operate as propaganda because they can give someone the feeling of being craftier than the enemy and the feeling that they can succeed against the odds: people can contribute something and feel "superior". This is something that many Muslims - especially young ones - are looking for. Later on, we will be looking at this type of training material again from a different perspective.
4. Materiaal gericht op interne disciplinering en versterking van de moraal van de (potentiële) 'harde kern', teneinde twijfel of afwijkende meningen te voorkomen.[53]
5. Material legitimating aspects of the jihadi battle. There is a lot of this material in many texts attempting to justify suicide attacks and the killing of Muslims as "collateral damage".
6. Material aimed at specific target groups, including young Muslim women and children.

In recent years, a disproportionately large amount of propaganda material has emanated from Iraq, a goldmine in propaganda terms for the jihadis. A lot of propaganda material has recently originated from the Mujahideen in Afghanistan.

Figure 3.4 Examples of propaganda aimed at supporters and backers

In one of Osama bin Laden's recordings dating from December 2001, he indicated that the United States had almost been forced to its knees. The message was intended to boost the morale of the Afghani warriors, who were at that point being routed from Afghanistan.[54]

In January 2004, members of the Hofstad group made the following announcement: "Dear brothers and sisters, as you may already know, the Mujahideen have altered their battle tactics. If we start to attack the unbelievers on Iraqi or Afghan soil, it will be mainly Muslim citizens who are victimised here; this is also the reason for the Taliban's withdrawal from the major cities in 2002. Our efforts are aimed at beating the unbelievers on their own ground [...]. Just as in America, England and other European countries, we now have the resources here, inshallah [God willing], to embark on large-scale bomb attacks, liquidations and guerrilla campaigns. [...] God willing it not be long before the first blows fall and the ground trembles beneath the feet of the unbelievers".[55]

The jihadis placed political statements on various discussion forums on the Internet, in which they adopted positions on current affairs, with a view to mobilising Muslims against the Dutch government and society as being "unbelievers". The communiques that were published were explicitly aimed at Muslims in Dutch society. Recent examples from 2006 include:

- *a pamphlet aimed against participation in the municipal elections of 4 March 2006,*
- *a statement from the "Lions of Tawheid" on the morning when the Court pronounced its sentence against the Hofstad group, and*
- *a pamphlet entitled 'Muslims in the Netherlands to boycott the Dutch courts'.*[56]

3.4.4 Influencing international public opinion

The jihadis intend to apply this influence in order to engender sympathy among the public at large for the jihad and jihadis. This form of propaganda also manifests itself in a variety of ways.

Unlike supporters and backers, the international public is not actively looking for such information. A number of terrorist groups provide basic information on their own organisations in a range of languages for this public. Various terrorist groups also issue general press releases and video messages, targeted at the press in other countries. Certain video messages are also designed to "launder" information,[57] by sending it out into the mainstream press, which then transmits it to the general public as its own reporting.
Many terrorist groups make extensive use of the expressions such as "freedom of speech", "political prisoners" and "human rights and women's rights", because the western public is particularly sensitive to this sort of subject matter. The terrorists present themselves as victims, and while doing so exaggerate the actions of the enemy. All this can serve to increase the degree of acceptance and provide a general ground of justification for political action.[58]
It can take the form of shifting responsibility (we are the victims, so we have to do something, but it is not our fault or responsibility), de-humanising targets (describing them as dogs, apes, pigs), favourable comparisons (the West is committing greater atrocities than we are) and altering the temporal sequence of facts and circumstances (9/11 was a response to US aggression in the Middle East and Africa).[59] In fact this tactic is also used to some extent in other forms of propaganda.

Figure 3.5 Example of propaganda aimed at international public opinion

There is a great deal of repetition of atrocities on the part of the West. Images of the attacks in the United States on 11 September 2001 and photographs of abuse at the Abu Ghraib prison are ever-present on the Internet. This was also the case during the so-called "cartoon crisis" at the start of 2006. The video that appeared on a number of hacked Danish websites also showed photos of Abu Ghraib.

3.4.5 Influencing the enemy (and the enemy public)

The jihadi intention behind this form of propaganda, aimed at the enemy and enemy public, is to weaken support for government policy through demoralisation, challenging the media (its credibility), the government and government personnel.[60] There is also an effort to encourage (military) staff to be less enthusiastic about continuing the battle. This can be achieved by spreading disinformation, or by actively correcting any wrongly presented images. We should also take account of infiltration of ordinary western web forums by individuals or groups of individuals, who try to

53 Hoffman 2006, p. 3, and Interview 6.
54 Hoffman 2006, p. 7.
55 Foxtrot 2004.
56 Our own investigations.
57 Hoffman 2006, p. 4.
58 Weimann 2006 p. 53.
59 Weimann 2006, p. 55, referring to a theory of Bandura.
60 Weimann 2006, p. 61-64.

argue their way towards reducing the support base among the western population. The GIMF called for action of this sort. The groups should have been made up of "Internet jihadis" who are fluent in English, Spanish, French or German. These individuals have to be good debaters and have their own "method for convincing people".[61] Dutch jihadis employee this tactic of abusing neutral sites a great deal (see section 3.3.3.4).

Figure 3.6 Example of propaganda aimed at the enemy (and its public)

When Chechnyan rebels shot down a Russian SU-24, the Russian authorities tried to deny the situation. They were overtaken, however, by the rebels' publicity campaign showing pictures of the wreckage of the aircraft in question.[62]

The Taliban issued a final warning via the Internet to Afghanis collaborating with coalition troops: if they didn't repent, there would be no way back for them during a forthcoming Taliban offensive against the coalition troops.[63]

A 42 minute video, issued by the GIMF, was a compilation of, on the one hand, an existing American HBO documentary entitled "Baghdad ER", concerning American soldiers in Iraq and the medical treatment they had to undergo, and on the other hand image and sound material from al-Zarqawi, al-Zawahiri and others. The introduction was: "They [American soldiers] are injured...taken by ambulances, then to the emergency room and at last...they die like dogs".[64]

3.4.6 Instilling fear

It is possible to instill fear, for example, by issuing threats via the mass media, by pretending to be larger and more dangerous than you actually are, or by making extreme, violent videos available and making extreme pronouncements, perhaps in the form of suicide testaments. The GIMF, which we have already mentioned as an important player in the dissemination of jihadi material, has stated that it is its right to instill fear in the enemy.[65]

Figure 3.7 Examples of instilling fear

The Abu Hafs Brigade claimed responsibility for the major power cuts in the summer of 2003 in parts of the United States. While there may be some doubts as to the actual existence of Abu Hafs as an entity, and certainly as to the claims they made, it was definitely an attempt to manifest themselves to the public at large and to instill fear in that public in relation to possible further attacks. The claim by Abu Hafs also contained some spectacular titles. The "attack" that allegedly caused the power cut was entitled "Operation Quick Lightning in the Land of the Tyrants of this generation".[66]

An article appeared at the end of 2005, describing how Muslims ("blonde or black") could easily murder of thousands of Americans by striking during the Superbowl: by causing a few explosions in the stadium, there would be such panic that people would trample each other under foot and the stands would collapse, with final consequences that would be worse than the drama at the Heysel Stadium in Belgium.[67]

A Candid Camera / Funniest Home Videos type of compilation appeared at the start of September 2005, with the subtitle: Bloody comedy. It was a compilation of recordings edited, one following quickly after another, of attacks against American soldiers, backed by recorded laughter and "amusing" (animal) noises.[68]

A video by Bilal L. dating from January 2005 threatened the Dutch MP Wilders. This professional video message started with a pledge of support for Mohammed B., who murdered Theo van Gogh, and ended with the following message: "And finally. A small present for Geert Wilders. We have already sharpened our swords, dog." The sound of knives being sharpened could be heard in the background. The end credits for the message read: "This is a production of the Leeuwen van de Tawhied (the polder Mujahideen) (better known as the Hofstad network.)".[69]

The fact that instilling fear actually affects the public at large can be assessed from the interest in what is perhaps the best-known example of this, the videos of Nick Berg and Paul Johnson being beheaded, placed on the Internet by the Iraqi Ansar as-Islam. In May 2004 'Nick Berg' was - after *'American Idol'* - the most popular search term on Google, and in June 2004 it was 'Paul Johnson'.[70]

3.4.7 Hacktivism

Hacktivism involves cyber attacks designed to make a political statement. It may take the form of carrying out cyber attacks on websites belonging to the enemy or "organisations linked with the enemy", showing them up in a bad light or silencing them.

Apart from attacks on websites, it is also possible to make a political statement by way of a Google-bomb. A Google bomb is an attempt to influence the Google search results, in order to get a particular page to a prominent position on the results list of the search engine. The programme indexes pages by "grazing" through them. One of the features looked for is the number of hyperlinks to other sites. This is how George Bush became the victim of a Google-bomb. If you entered the words "miserable" and "failure", the first search result you would receive would be Bush's web site.[71] We are not yet aware of any cases of a jihadi Google-bomb.

61 SITE-Institute 2006g.
62 Weimann 2006, p. 61-64.
63 SITE-Institute 2006n.
64 SITE-Institute 2006p.
65 SITE-Institute 2005b.
66 Weimann 2006, p. 55.
67 SITE-Institute 2006l.
68 SITE-Institute 2005a.
69 The TV programme Zembla dealt with this video on 10 February 2005.
70 Weimann 2006, p. 110.
71 Nu.nl 2006d.

We cannot yet predict how far the known forms of jihadi hacktivism, including the hacking attacks during the cartoon riots and against Israel (see section 2.2.5), might have been the precursors of larger attacks in the future. It seems in any event that computer skills among jihadis are on the increase, and there certainly seems to be an intention to commit this type of attack.

Figure 3.8 Examples of hacktivism

The private initiative, Internet Haganah, in the United States, which aims at getting jihadi websites offline, became the victim of Denial of Service attacks so that its own site was no longer accessible.

The website of the Dutch MP Wilders was hacked for the second time by Islamic hackers in July 2006. They left a message behind on his website.[72]

During the Danish cartoon disturbances, there were not only heated discussions on the issue, but many Danish websites were also hacked, resulting in defacements: the content of the Internet pages in question was replaced by jihadi images, videos and slogans. Generally speaking, these defacements have little effect. Much worse was that the Danish government was inundated with e-mails, which interfered with regular e-mail traffic to and from the Danish government.

3.4.8 Assessment of the threat of propaganda

The Internet offers multifarious opportunities for propaganda. Salafis and jihadis make extensive use of the Internet for this purpose. There are many known examples of propaganda via the Internet. This is done professionally, with them aiming their message at a wide and varied public audience and specific target groups within that audience, for which they use a range of languages. There are some documented examples of people becoming radicals under the influence of the Internet. Imam Samudra, for example, who was condemned as the field coordinator of the attacks in Bali on 12 October 2002, stated that he had formed his convictions by reading a number of standard works and articles on radical websites. And the autobiographical sketches of Samir A., that the Dutch National Criminal Investigation Team [Nationale Recherche] discovered on his home computer under the title 'Deurwaarders' [Bailiffs], contain an extensive description of his searching procedures on the Internet and the part played by the Internet in his radicalisation process.[73] Jihadis also regard propaganda itself as useful in achieving their aims. Too many repetitions in the messages and compilations of older videos and sermons are, on the one hand, an indispensable and necessary characteristic of propaganda, but - at least to outsiders - they also show some element of intellectual poverty. All things considered, we can therefore state that propaganda via the Internet makes a contribution towards radicalisation.

72 Nu.nl 2006c.
73 AIVD 2006, p. 46.

3.5 ACQUISITION OF INFORMATION

The Internet is a virtual library with an almost endless supply of information, most of which is also openly accessible. Governments, companies and individuals place large quantities of information on the Internet, such as street maps, arrival and departure times for aircraft and address details. This information can be helpful in the commission of attacks on buildings and for all sorts of preparatory activities.

The jihadis are well aware of the facilities offered by the Internet for the acquisition of information and use the Internet as a virtual library and source of information for their preparatory activities.

> *"AIVD research has clearly shown that jihadis in the Netherlands actively search for this operational knowledge on the Internet. In a number of cases, during searches of premises and arrests, home-made explosives were found, whose manufacture was presumably (partly) based on knowledge acquired via the Internet."*[74]

Thus, after the detention of Samir A., photos, sketches and street maps of the Borssele nuclear power plant, the buildings of the Dutch House of Representatives, the Binnenhof and the AIVD building were found, and he had assembled these largely via the Internet. Samir A. followed up his virtual reconnaissance of the AIVD building by a physical reconnaissance of the premises.[75] Also, for example, architectural drawings of a dam were found on computers seized from Al Qaeda.[76] Shortly after a call to jihadis by al-Zawahiri to attack oil installations, it was possible to find Arabic language jihadi websites providing information on the locations and sizes of oilfields and oil installations, with the appropriate hyperlinks to other sources of information. Uploading and searching for information does leave traces, however, and this can be a hindrance to terrorists. As we indicated earlier, they are well aware of this and take counter-measures.

It is clear that the Internet is outstandingly suitable for acquiring a great deal of information legally. Airlines, for example, contribute to this intentionally by providing departure times. But organisations also place information on the Internet without appreciating that it might be abused for a number of purposes. The American Minister of Defense warned his staff in January 2003 that the Defense websites contained too much unclassified material that might potentially be used by terrorists. He reminded his staff of the contents of an Al Qaeda handbook discovered in Afghanistan, to the effect that 80% of the information required about the enemy was available via public sources.[77] The American Department of Defence was clearly also aware of the risks in 2005: "The enemy is actively searching the unclassified networks for information, especially sensitive photos, in order to obtain targeting data, weapons systems vulnerabilities and [tactics] for use against the coalition."[78] The Nuclear Regulatory Commission's (NRC) Office of Nuclear Security and Incident Response in the USA took its entire website

74 AIVD 2006, p. 51.
75 Judgment by the Court of Appeal in The Hague on 18 November 2005 in connection with the appeal against Samir A., on www.rechtspraak.nl.
76 Benschop 2006a.
77 Conway 2005, p. 14.
78 Military.com 2005.

offline shortly after the attacks on 11 September, and a few weeks later the site was brought back online, stripped of about a thousand sensitive documents.[79]

Keeping information internal is only relatively useful if the security of the internal network turns out to be inadequate, or if organisations allow file-sharing or peer-to-peer programmes to be used by staff. It seems, for example, that a lot of information can leak away via the Limewire programme, because more files may be shared with other Limewire users via the Internet than the owner of information is aware of.

Figure 3.8 Examples of acquiring sensitive information legally

As material for a counterterrorism training symposium in 1996 in Nevada, the website state.nv.us contained an extensive description of the methods used for shipping nuclear waste, which routes would be used for transportation and even the weapons with which the transportation could be attacked. In the section headed "explosives" on the jihadi website almoltaqa.org, there was a link to the site in Nevada, so the information had been found, copied and further disseminated.[80]

In the Netherlands, local authority risk maps are a public source of information, from which a citizen can check on the Internet as to which potentially dangerous sites are situated in his neighbourhood. At the request of Dutch Minister Remkes of the Ministry of the Interior and Kingdom Relations, the provincial authorities decided to leave out information on the impact of calamities. It is still possible, however, to obtain the information that has been excluded directly from the relevant local authority.[81]

Another form of acquiring information via the Internet is through geospatial information, such as Google Earth. Taking the form of satellite photos, often combined with further information and aerial photos, this forms a rich and significantly detailed source of information. Information in this type of public database can help terrorists with general target selection and location: after all, it offers information in a readily accessible manner on the surrounding area and sometimes also the structure of buildings. For the actual preparation of attacks, however, they would need more detailed and up-to-date information, which they could acquire by means of observation and other sources.[82] The information available on Google Earth is also accessible either free or on commercial terms through other channels.[83] There are indeed others offering this type of material. Google is also receptive to requests to have particular areas rendered invisible. When dealing with aerial photographs rather than satellite photographs, Google is actually obliged to comply with such requests.[84] When it becomes possible to look at satellite pictures in real-time and/or in greater detail than is currently available, this might also involve further dangers of abuse. Replies to Dutch Parliamentary questions seem to indicate that it is not yet possible to indicate how far these effects will be positive or negative.[85] We can predict that it will have advantages not only for terrorists but also for investigation and security services, and that these may balance each other out. The situation is developing very quickly, however, and it would seem prudent to anticipate this type of threat.

79 Conway 2005, p. 15.
80 Weimann 2006, p. 113.
81 Planet.nl 2006b.
82 RAND 2000.
83 Justitie 2005b.
84 NCTb 2006b.

While the information contained in the examples was not always intended for the public at large, it was still freely available. The information we have discussed so far has also been available legally by looking up public sources. Information can also be obtained through the use of illegal methods. We also have to take account of infiltration of companies with sensitive customer and Internet information. An infiltrator at Google or an ISP might be able to cause significant damage by siphoning off and analysing information concerning customers, IP addresses and surfing behaviour, and then investigating it thoroughly. Information concerning IP addresses can sometimes provide quite specific knowledge: information thus became available on the name and anchorage site of an American aircraft carrier because the crew had access to the Internet.[86] We are unaware of the extent to which terrorists acquire their information illegally, whether or not this involves hacking in person, hiring hackers or inducing them to undertake challenging assignments, or through infiltration. Of course this is also partly because hackers do not leave visiting cards behind. It is, however, very likely that they apply these methods.
Hackers could also try to obtain information on the working methods of security and detection agencies in preparation for a campaign, or even just to protect or conceal their own organisation. This might involve attempts to break into police information systems, for example.

Another facility for getting hold of information is data mining: uncovering patterns, associations, changes and structures within large quantities of information stored in a database. We do not know whether jihadis are involved in this. Many publications assume either that jihadis are involved in data-mining or no distinction is made between acquiring information and data-mining.

How should we regard the threat of information acquisition via the Internet? The Internet forms an inexhaustible source of information for jihadis as for everyone else. This information can be acquired either legally or illegally, and professional tools such as data mining can be used to collate information. This information can be useful in the preparation and implementation of terrorist activities. While this information might also potentially be acquired in some other way, the facilities for gathering information via the Internet are more approachable, less expensive, simpler, less labour-intensive and on a larger scale. In particular, developments in the area of (real-time) satellite pictures, potentially combined with a permanent Internet connection, will continue to make rapid progress. This makes the acquisition of information via the Internet a very usable resource for jihadis, and this potential contributes towards the actual execution of terrorist activities.

85 Justice 2005b.
86 Newsbytes 2006.

3.6 FUNDRAISING

Fund-raising via the Internet takes various forms.[87] Its first variant is direct and public fund-raising via websites. Various sites explain, in compelling texts, that the costs of running a terrorist organisation are significant. Hamas, for example, explains the cost of bullets, the acquisition of other items and costs of bribery, while Hezbollah displays details of three bank accounts for donations on its al-Manar site, and also points out the costs associated with caring for wounded martyrs and their families (you can sponsor an orphan for $360 a year, or a widow for $300), and the Pakistani LeT goes in for public fund-raising with requests for money and computer hardware. These types of donations are a particularly useful option for Muslims who do not want to become personally involved in the jihad.[88] With many terrorist groups, the websites address the visitors directly about handing over money, or leaving their bank or credit card details, or opting for an Internet payment scheme such as PayPal. Some individuals were charged in the United States with maintaining this type of website between 1998 and 2002.[89] Public fund-raising activities also sometimes take the form of chain letters calling for the donation of money. These are sent out to sympathisers by way of e-mail. Bank account numbers are also available on radical websites, and donors can transfer money using Internet-based financial services such as PayPal and CashU.[90] Yet another example of a public appeal is the appeal dating from 2004 for financial support of Samir A.'s wife following his arrest.[91]

A *second variety* of fundraising is the use of profiling, e-commerce tools and the commission of fraud. Website visitors can be profiled via user information. This type of information can be generated from registration forms or online questionnaires, with potential donors then being written to. A common form of fund-raising via websites is the online shop, where books, CDs, DVDs, flags and T-shirts can be purchased.[92] Thus seven people were charged in Copenhagen in February 2006 after they had been selling T-shirts via an Internet shop, with the profits being destined for terrorist organisations on the EU list.[93]

Aside from direct appeals or online shops, involuntary contributions can also be generated by means of online credit card fraud, *phishing and pharming*. There are relatively few examples of this.[94] Since hackers generally appear to be showing an increasing interest in fraud in the field of cybercrime, we cannot rule out jihadi hackers following the same path, with fraud becoming an increasingly important instrument for fund-raising.

A *third variant* of fundraising is that of exploitation and abuse of charitable institutions. "Giving alms" (zakat) is one of the five pillars of Islam. Zakat amounts to 2.5% of one's wealth and is intended for the poor, widows, orphans, the sick or travellers. In addition to zakat, a believer may also make voluntary gifts, which is regarded as being very praiseworthy in Islam. Jihadi organisations appear to be abusing this "pillar" by their methods of fundraising, which often operate via charitable organisations. The rise of

87 Conway 2005.
88 Weimann 2006, p. 135-138.
89 Apuzzo 2006.
90 Thomas 2003.
91 Taken from the public prosecutor's closing speech (www.om.nl/de_hofstadgroep).
92 Conway 2005.
93 BBC Monitoring 2006a.

the Internet means that donations can be made with the click of a mouse, in a manner of speaking. Some examples of charitable institutions who are or have been active on or via the Internet include *Mercy International, Wafa al-Igatha al-Islamiya, Rabita Trust, Al Rasheed Trust, Global Relief Fund, Benevolence International Foundation*, and *HelpThe Needy*. These charitable organisations advertise on Islamic websites and chat rooms, incorporating references to their Internet pages. Existing organisations have also been infiltrated by jihadis, so that there is a secret agenda on some of these sites. A few of these organisations refer in guarded terms to this agenda on their websites.[95]
In April 2006, there were requests for donations for Palestinians on a range of jihadi forums. "Do not be lazy.... Do not stay behind. Make your move now, time passes and the situation gets worse. Transit for help and medical aid will not be prohibited, even in [sic] all the doors are locked in front of us. We will never abandon our brothers in Palestine. Put an [sic] effort to spread the campaign." The message contained the names and account numbers of some charitable institutions.[96] Occasionally there are requests for donations other than financial ones.

For jihadis, there is one important disadvantage of online fundraising: it is relatively public and can therefore in principle be observed, traced and investigated. Also, there is often a dependence on inter-bank payment traffic, which not only leaves traces but which is also very much in the international public eye, in connection with all manner of policy measures in the area of countering terrorist finance. Leaving charities to one side, this means that there are probably few other really serious examples of fundraising. Those sites recognisably incorporating fundraising for terrorist activities disappeared from the ether quite quickly, presumably as a result of government intervention. Anonymous payment methods, such as the single use "CASH U cards", which are in fact debit cards, are relatively new, however. These have the potential to significantly reduce evidence concerning the payments and the sympathisers. We can therefore predict an increase in fundraising.

How should we regard the threat of fundraising via the Internet? There are potentially many opportunities for fundraising, and we are aware of some examples, but it is not yet a common phenomenon in practice. This form of fundraising is, after all, fairly conspicuous and therefore vulnerable to government intervention. As Internet banking becomes more and more straightforward and commonplace, use and abuse of this facility by jihadis will also undoubtedly increase. Combined with the increasing interest of hackers in online fraud, this may lead to a shift from more public to more covert fundraising. Fundraising via the Internet may also increase as a result of new digital and anonymous payment facilities.

94 Conway 2005 based on Libbenga, Terrorists grow fat on email scams 28-9-2004.
95 Conway 2005.
96 Site Institute 2006t.

3.7 RECRUITMENT

If propaganda is still primarily aimed at winning over souls, then recruitment is an active attempt to involve people in terrorist activities, clearly going one step further. It would be beyond the bounds of this study to make an

extensive exploration of recruitment. For further background, we would refer you to, for example, AIVD reports, which also cover recruitment.[97] There are, however, frequent references to (opportunities for) recruitment when jihadis make use of the Internet. This is why we are specifically devoting some attention to the matter in this study.

'Recruitment' here means putting people in the picture and then checking and manipulating them in order to promote an internalised radical political-Islamic conviction within these individuals, with the ultimate aim of having them take part in the violent jihad in some way or other.[98] Recruitment is therefore aimed at "catching" people who are prepared and inclined to become involved in a violent campaign. A procedure is set in motion by a recruiter, aimed at a potential recruit. Recruitment accordingly involves two parties, with the initiative coming from the recruiter.

As we indicated earlier, the majority of jihadi groups have a presence on the Internet and, of course, they do their very best, in a number of ways, not only to win over souls but also to persuade individuals that they will be ready to participate in the violent jihad. Thus the military arm of Hamas has its own site, entitled alqassam.com, aimed at recruitment. It makes the usual promises about martyrdom. The site also serves as a virtual monument to those martyrs who have died.[99]

It is theoretically possible that someone from the Netherlands would allow himself or herself to be recruited directly via the Internet by recruiters from international terrorist groups, such as Hamas, on a one-to-one basis. It is not very likely, however. Radicalisation in the West, possibly leading to recruitment, is after all a process that frequently starts with the quest for answers to questions regarding life and religion. There are numerous Western and Dutch sites that make a much better attempt at this than those of the terrorist groups from "far away countries" (see section 3.8) and the threat to the Netherlands emanates primarily from local, native Dutch networks. This is not to ignore the fact that, for example, the core of Al Qaeda might have an inspirational impact in the formation of virtual networks. One example of this is mentioned in figure 3.10 of section 3.10. But it would be going too far to call this recruitment by Al Qaeda.

A markedly interactive form of recruitment is perceptible on the Internet, at the hands of local native Dutch networks, and this is strongly connected to interactive ways of spreading propaganda. The AIVD has this to say on the matter:

> *"Communication is quite open at the outset but then becomes more confidential within a limited circle and finally ends up as clearly conspiratorial behaviour. First of all there will be a posting on a website or newsgroup, including a reference to a certain site, where there can be a discussion (including on matters of faith) using a chat program with a larger number of participants or on an individual basis. Some individuals are then propositioned to explore matters further in a one-to-one chat session. This bilateral chat session will often be clearly focused on recruitment. Pundits who might be susceptible to this type of recruitment via the Internet are passed on, by participants, to certain charismatic or ideologically better-educated young people. These self-styled ideologues and recruiters frequently maintain bilateral Internet contacts with a substantial group of potential recruits."*[100]

97 AIVD 2002b, AIVD 2004, AIVD 2006.
98 AIVD 2004.
99 On this, see Weimann 2006, p. 82.

One of the Internet's primary characteristics, however, is that potential warriors are keen to report voluntarily for participation in the violent jihadi battle (conscription). The term "recruitment" does not imply that there is a hierarchical military organisation, nor does the term "conscription". Conscription (in this context) is aimed at being allowed to participate in the activities of a network or group, prepared and ready to implement a campaign of violence. The procedure is instigated in this case not by a recruiter but by the potential warrior who has, as it were, already stepped over the threshold. There is, however, a selector involved, who has to decide whether the warrior will be included as one of the members of the network or group and also whether he will receive any training to that end. Conscription does not accordingly involve recruitment in the formal sense, even though there are still two parties involved.

Conscription suits the nature of Internet, with its active dynamic and potential for ever-changing roles, quite well. Those who are interested in the jihad will take part in Internet discussions, for example. If, after some time, they become receptive to the jihadi message and radicalise yet further, the time may come when they offer their services to someone for whom they have high regard. This will be their interpretation of the general appeal on the Internet to join the "caravan of martyrs".[101] It may also be a response to a more general call. An example of the sort of process from abroad is described in the New York Post. A discussion took place in a password protected chat room at the end of September 2003. One individual wrote: *"Brother, how do I go to Iraq for Jihad? [...]"*. The message was answered after four days, with advice to look for someone he trusted, so as to be able to take the first steps on the wide open roadway. In response to a follow-up question, the person who had replied sent a propaganda video along with instructions to download PalTalk software. The potential recruit subsequently disappeared from public view.[102] Here is another example. In 2003, one Abu Thar placed the following message on an Islamic web forum:

> *"Dear Brothers,*
> *I have already succeeded with the grace of Allah and his help, to go to Kurdistan for Jihad through one of the brothers in this forum. Praise be to Allah, I have fought there, by the grace of God and his bounty.*
> *But Martyrdom was not granted to me, and therefore I ask Allah to give me more lifetime and to make my deeds good. I ask anyone who has the capacity to organize for me to go to another Jihad front to correspond with me."*[103]

100 AIVD 2006, p.48.
101 One of the first jihadi websites set up in the Netherlands was entitled 'sluit je aan' ['join up'] (with the caravan of martyrs), and Azzam, one of the founders of Al Qaeda, produced a work under this title (see section 3.3.3.3). See also, in this process of "volunteering" AIVD 2006.
102 Weimann 2006, p. 102- 121.
103 Rozen 2003.

An additional characteristic of the Internet is that roles can quickly be reversed. In the absence of any "caravan to join up with", the potential warrior may for example decide to set one up himself. The potential warrior might then become the "recruiter" for the group he is about to form or might start to take part in a virtual network contemplating the commission of attacks. The question we should be asking here is whether there is really any conscription involved if you are a member of a virtual network of like-minded individuals who do not shy away from violent campaigns. In fact it may be better described as a gradual process of mutual influencing.

Self-ignitors are also frequently mentioned in connection with Internet. This happens when someone embraces the violent jihad from in front of his computer screen, without having had any clear contacts with recruiters, without having regularly visited a radical mosque and without some other form of physical influence, and then tries to embark on the jihad on his own initiative or starts to prepare attacks in his own country.[104] Self-ignition obviously does not involve two parties: the self-ignitor will, after all, be embarking on the jihad on his own initiative and has already pushed the button. Nor can this be described as recruitment in the formal sense.

The self-ignitor laps up radical material via the Internet and may be inspired from following discussions on the Internet (either actively or passively).[105] There is no need for contact with a (virtual) recruiter or selector, and this is not conscription.

> *"At the end of September 2004 in the Netherlands, Yahya K., an 18-year-old student from Sas van Gent, who had issued threats on the Internet against the Dutch MP Hirsi Ali and the AIVD, was detained. During his arrest he was found in possession of home-made explosives that he had assembled using knowledge derived from the Internet. He had undergone the entire radicalisation process from in front of his computer screen in the virtual world as well".*[106]

If it is difficult in the physical world to distinguish between the transition from the radicalisation process to recruitment, on the one hand, and conscription on the other hand, then this is certainly the case with Internet. Roles can change quickly, and the ease of forming virtual networks (see section 3.10) blurs the picture even further. Is there really any conscription involved if you are a member of a virtual network of like-minded individuals who do not shy away from violent campaigns? Or is it perhaps better described as a gradual process of mutual influencing? The question perhaps ought to be whether the rise of the Internet means that the classic recruiter/recruit concept still persists, or whether it is gradually being replaced by a permanent and interactive mix of top-down and bottom-up information provision and acquisition, mixed with online encouragement, steering or network formation, which ultimately has the same result: the growth of the jihadi movement. In short, recruitment, conscription and self-ignition via the Internet are still relatively new phenomena and we are not yet in a position to fully understand them.

104 See, for example Van Leeuwen 2005, p. 87.
105 Partly based on AIVD 2006, p. 50.
106 AIVD 2006, p. 50.

So, what threats do these phenomena pose? Use of the Internet by jihadis results in more interactive forms of recruitment, which cannot yet be easily identified, and also in conscription and self-ignition. The distinction between this and radicalisation is a difficult one to draw. We might well say that using the Internet for this type of purpose might shorten and accelerate the transition from being a backer of jihadi ideology to being a terrorist, certainly when combined with the propaganda and training material on offer, and the formation of virtual networks.

3.8 TRAINING

The expression "training" includes tracking down or producing and/or disseminating educational material, manuals, films and suchlike on aspects of importance to the jihadi battle. Some examples of this include materials on how to conduct the jihad in heavily populated areas, how to make explosives, how to handle weapons or how to communicate securely.

A great deal of jihadi training material is available on the Internet. This has been partly prompted by the disappearance of physical training camps in Afghanistan. New ones take a while to set up, although there are still signs of physical training camps in Africa, for example. The need for virtual training camps has increased as a result of the disappearance of the camps in Afghanistan. A number of jihadi web forums also symbolically bears the names of well-known training camps in Afghanistan.[107] The importance of the Internet for training is also underlined by statements such as *"It is not necessary...for you to join in a military training camp, or travel to another country...you can learn alone, or with other brothers, in [our arms] preparation program."*[108]

Internet training principally involves the issue of manuals, for example for making explosives. The number of references to sites containing terrorism-oriented manuals doubled in the period between 2000 and 2005.[109]
One of the important works for present-day jihadis is that prepared by as-Suri, which we have already mentioned. His substantial work consists of many (strategic) manuals (see also section 3.2.3) and training materials The work is in Arabic, but some parts have now been translated into English.

There is an increasing supply of videos, in addition to manuals. These might, for example, be instruction videos on how to prepare a bomb harness, gunpowder or detonators. This material is generally set up in a very professional manner.[110] We would describe the risk arising from this low-threshold training material as being significant, certainly if it were to appear in the Netherlands in translated versions. Bearing in mind the general increase in material translated into Dutch, it is probably only a matter of time until Dutch translations of this material turn up.[111]

107 Rogan 2006, p. 26.
108 Al Qa'ida key figure Abu Hadschir al Muqrin, during an interview with Der Spiegel online.
109 Weimann 2006, p. 124.
110 Result of submitting material to experts. See also Telegraaf, 2006
111 Interview 5.

Preparation for the battle does not concentrate exclusively on explosives, however. The *online* newspaper *Al-Battar* appears currently and regularly (every two months). Al-Battar, which is attributed to Al Qaeda and started in 2004, includes a wide range of instructional material. It deals with every aspect of terrorism. Its eighth edition (April 2004) contained extensive and illustrated instructions for the use of a sniper rifle, clearly written by an expert.[112] The 10th edition (May 2004) focused on kidnapping and hostage-taking, including possible motivations for kidnappings: concession to demands, political damage by disrupting relationships between states, extracting information from the hostages, ransom money and drawing attention. Finally, Al-Battar devoted some attention to uncovering infiltrators and agents, travelling, fake documents, hiding places, communication and steps to be taken in the event of being arrested. A compilation of Al-Battar material has recently been produced.[113] Professional methodologies are often adopted from military handbooks or instruction manuals for security officers.[114] The data carriers seized from the Hofstad group also contained these sorts of military manuals, and the weblog of the 'Lions of Tawheed' published a document entitled "Lessons in security" in July 2005, indicating how to deal with arrests and interrogations, as well as providing some brief security advice.
Even the most recent developments are clearly being closely followed by terrorists, as is apparent from a contribution on a jihadi web forum. This contribution demonstrated an advanced anti-missile system for military vehicles. The Mujahideen in Iraq have clearly been experimenting with how to circumvent this active protection.[115]

The Simon Wiesenthal Center reports that, in many of the training documents they have found in the course of their investigations, there are also instructions for producing weapons of mass destruction, including target selection.[116] Some attention is paid to biological weapons. Some jihadi web forums accordingly contained a manual on the use of botulism, with discussion on how this could be deployed.[117]

A new compilation of training material was disseminated on jihadi forums recently, "hidden" in a file called *Nemo*. In addition to scenes from the cartoon film *"Finding Nemo"*, the compilation includes material concerning forgery, explosives, poison and nuclear weapons. It also includes *hyperlinks* to 17 other relevant documents.[118] Giving this type of compilation a name like Nemo is particularly treacherous, because children enter terms like this as search fields when using modern filesharing programs to download films. By doing so, they might end up being faced with violent material.

There have already been some convictions in the United Kingdom of individuals "associated with Al Qaeda" who had downloaded instructions from the Internet, for example for blowing up aircraft.[119] Manuals obtained from the Internet were also apparently found in August 2006 in the UK, following arrests in the context of the foiled plot to blow up a number of aircraft.[120]

112 Jamestown 2006.
113 Interview 1.
114 AIVD 2006, p. 51.
115 SITE-Institute 2006u.
116 National Post 2006.
117 SITE-Institute 2006v.
118 Site Institute 2006c.
119 Guardian 2005.
120 Independent 2006b, Telegraaf 2006.

Research by the AIVD has clearly shown that jihadis in the Netherlands have also been actively looking for operational information on the Internet. Home-made explosives have been found during a number of domestic raids and arrests, whose manufacture was apparently partly based on knowledge derived from the Internet.[121]The hard drives belonging to the accused in the Hofstad group contained literature from the Internet relating to military manuals.[122]

Of course not all of the material available on the Internet is realistic, reliable or (safely) useable. Experts indicate that this material is far from sufficient, for example, to allow the commission of an attack, to transport explosives and detonate them at the correct moment with the desired effect. Greater expertise is definitely required for this, and fortunately it is in short supply. A physical training camp undoubtedly provides more in the way of knowledge, and certainly experience, than manuals and videos obtained from the Internet.[123]

How should we regard the threat of online training material and training obtained via the Internet? The Internet is full of manuals, instructions and tips for individuals who want to perpetrate an attack, or who want to be prepare in a more general sense for the jihadi battle. The Internet's primary benefit here is the ease of access when looking for and supplying such material, so much so that it could be described as a large-scale virtual training camp. It is however an important additional consideration, when contemplating the material that is available and the concept of a virtual training camp, that a person always has to be able to understand, practise, apply and carry out the instructions properly, and that the discipline required for a successful battle or carrying out a large-scale attack is much more readily developed in an actual training camp. Some of the instructions also deserve an emphatic question mark regarding their "ease of use" and safety. The threat emanating from available online material for smaller scale attacks (explosions or poisonings) is, however, much more significant, for four reasons:

- at least part of the descriptions is complete and explicit, with the quality and availability increasing all the time;
- the amount of material on the Internet translated into English, French, German and now Dutch is also on the increase;
- even individuals who had no concrete plans to commit an attack may find inspiration in the abundance of richly illustrated material;
- there is material available for a variety of types of attacks, including those using chemical, biological, radiological and nuclear resources.

3.9 MUTUAL COMMUNICATION AND PLANNING

In addition to its other functions, the Internet is an outstanding communication environment. It is no surprise, therefore, that jihadis use the Internet for mutual communication within their own groups or networks and also for planning terrorist activities. While this involves a distinction, it is only one

121 AIVD 2006, p. 51.
122 Rechtspraak.nl 2006.
123 Our own enquiries with experts. See also Washington Post, 2005

of degree. Mutual communication (with a terrorist group or network) can be about anything. In the context of assessing the threat, we are not, of course, concerned with exchanges of family news but rather with communication relating to terrorist activities. And this quickly moves on to planning terrorist activities.

There are good reasons why the Internet is regarded as a global communication environment. One of these is the simplicity of access to the medium, with limited costs. To elaborate on this, we should point out that many people in traditional Muslim countries do not yet have access to the Internet, although such access has increased significantly in recent years, primarily through an increase in the number of Internet cafes. Another attractive point is that the Internet can operate more or less as an electronic nervous system for a network and can therefore neutralise the inherent disadvantages of networks, such as the difficulty of coordinating activities and targeted duties.
An extra attraction for jihadis is that communication and the exchange of operational information can take place fairly anonymously, so that it makes it difficult for detection agencies to find evidence. This puts the Internet at an advantage in relation to other communication media, both for the core of Al Qaeda and for the networks inspired by Al Qaeda.
Even small networks can derive benefits from the Internet. After all, physical contact might allow observation teams to catch sight of or eavesdrop on the network.

These benefits of the Internet are only partially effective in relation to jihadi networks. Communication, and the exchange of information, are and remain a risky business, because information might unintentionally leak out to third parties. Private organisations patrolling the Internet for illegal activities may, for example, intercept information and pass it on to detection agencies. Weisburd in the USA, who patrols the Internet for jihadis like a sort of Simon Wiesenthal, has already built up a reputation in this area.[124]
If the network is to operate properly, then the members have to share information and knowledge. This may well have advantages, but there are also possibilities for abuse and unintentional dissemination of crucial and sensitive information. Virtual networks are certainly difficult to control in this respect. One member might for example pass information to other members, perhaps using other networks. Nor is there any guarantee that detection agencies will not be intercepting communications, so that face-to-face communication is still necessary sometimes.
While there are accordingly benefits for networks communicating and exchanging information via the Internet, both within and between existing networks, there continue to be some disadvantages.[125]

Do the advantages outweigh the disadvantages? As we stated at an earlier point, the jihadi movement in general has a high degree of computer skill, along with the most recent software and adequate hardware in many cases. They also use these for communicating and planning terrorist activities

124 See, on Weisburd, e.g. Labi 2006.
125 Suggested by Kortekaas 2005, p. 51-55, 69-70, 103-107 and 123-129.

(see figure 3.9). In doing so, the jihadis are well aware of the risk of communications being intercepted, so that they are increasingly communicating "behind closed virtual doors" (see section 3.2.3). The German Bundesverfassungsschutz has apparently indicated that mobile telephones are barely used any longer for communication, and that they are concerned that a system of secret communication via the Internet, for planning and coordinating attacks, has taken their place.[126] This does raise a few questions.

Figure 3.9 Examples of communication via the Internet

Detailed plans for an attack on the Saudi Minister of Internal Affairs were found on the website of some Al Qaeda operatives in Saudi Arabia.

There are indications that the Internet was used for the strategic planning of the attacks in Madrid in March 2004. A strategic document dating from December 2003 on the GIMF site indicates Spain as being a most appropriate candidate for attack, to ensure that Spain would leave the coalition, thereby weakening it. Even the timing (elections in March) and method ('several attacks or blows') are mentioned in the document.[127]

Bearing in mind the general Internet skills of jihadis, it is likely that they will also start to use Internet telephony (VOIP) and other modern applications in order to frustrate eavesdropping and tracing of their communications. But we still see reports of the leaders of the "core of Al Qaeda" using couriers. The messages may well be prepared and printed on a PC, but they are sent by hand.

All in all, we can therefore conclude that jihadis are using the Internet for mutual communication and planning. In doing so, they make use of the facilities for anonymous and secretive communication. As well as having benefits for jihadis, this usage of the Internet offers security and protection agencies the opportunity to intervene. The jihadis are very well aware of this.

3.10 CREATION OF VIRTUAL NETWORKS

Jihadis frequently operate in local or international networks.

> *"A jihadi network is a fluid, dynamic, frequently demarcated structure, containing a number of individuals (radical Muslims) who have a mutual relationship with each other, both on an individual and a collective level (cells/groups). They are linked, at least temporarily, by a common interest. This interest will be an attempt to achieve an aim related to Jihadism (including terrorism).*
>
> *Individuals forming part of the network are designated as members. Membership is obtained by actively and consciously making a contribution to the achievement of the said aim, within the limits of the network."*[128] [129]

126 BBC Monitoring 2006b.
127 Weimann 2006, p. 130 en p. 134.
128 AIVD 2006, p. 14.
129 For further background information on terrorist networks, see AIVD 2006, p. 13-19.

One of the major benefits of the Internet is that it is possible to form virtual networks, in the sense that members "have met" each other online and consequently have meetings exclusively online. These virtual networks may range from entirely new networks, through a combination of a new network and an existing one to a combination of existing networks. There is the potential for worldwide networks to be created via the Internet, even though access to the Internet is still somewhat restricted in traditional Muslim countries. By following individuals during chat rooms sessions, for example, then measuring them up on an individual basis and finally communicating with them on a one-to-one basis in a closed environment (see section 3.4), it is possible to obtain an accurate impression of someone's reliability and devotion to their cause. The AIVD also mentions some further advantages. Using virtual networks, individuals from local networks can quickly establish contacts throughout the world, for example to organise logistical support or resources for their battle when preparing for attacks. The members of the network can take part with a considerable degree of anonymity.

> *"Since the network only exists in the virtual world, and since there is no need whatsoever for actual contact between the various members in the real world, this type of network is difficult to detect, and individuals taking part (sometimes under frequently changing virtual nicknames) are not easily identified by the police or the security and detection agencies. [....] Moving the jihad into the virtual world in this way offers enormous opportunities for international collaboration between networks and individuals, and thus increases the strength of the jihadi movement."*[130]

Virtual networks are also subject to some disadvantages. A characteristic of virtual networks and communities is the *volatility* of *contacts* and *identities*. Mutual communication within virtual networks has never been straightforward, because individuals can have such widely varying backgrounds. The obstacles to leaving the community, for example, are quite low. The result of this volatility is that you really do not know who your contact is, and your contact can quickly disappear. Individuals can also adopt a range of identities (nicknames) and can change them quickly. It is also easy to put up a barrier between an electronic identity and a natural one. A virtual individual might appear to be a detective or a security services employee. Inside illegal networks, it is particularly crucial that people can be trusted. Based on the comments we have made, this is an important issue with virtual identities. Precisely because it is an intrinsic characteristic of networks to have a certain degree of fluidity, this is certainly the case for virtual networks where people do not (physically) know each other and will not have met each other in person. All of this renders the functioning of virtual networks far from straightforward.[131] In this context, the AIVD has this to say:

> *"[....] the mutual distrust and the great awareness of the need for security among jihadis can also hinder the speedy formation of virtual networks. It is only if and when there is an actual degree of mutual trust that activities can be jointly developed via the Internet. This then means that individuals will frequently know each other already from the physical world, or else they can refer to mutual acquaintances, clan or family members. There are often detailed ideological discussions designed to measure each other up, or a process of stringent selection for the admission of members to certain closed websites (or parts of them), which can usually only be accessed with (sometimes quickly changing) passwords."*[132]

130 AIVD 2006, p. 49.
131 Kortekaas 2005, p. 107-114, basing this on other authors in the field of organised crime.
132 AIVD 2006, p. 49.
133 Washington Times 2006, Bell 2006.
134 SITE-Institute 2006h.

How realistic is the creation of virtual networks in the light of the advantages and disadvantages we have cited? And, if people know each other already from the physical world, are we still talking about a virtual network? The fact is that there are documented advantages to virtual networks. Earlier in this chapter, we indicated that Dutch jihadis consciously sought out interaction with individuals interested in Islam and the jihadi battle. This can give rise to completely new virtual networks and the creation of a virtual jihadi community on the Internet. There are some indications that this is actually what is happening. We also stated that Dutch jihadis use translations prepared by others and refer to other websites. This too can be viewed as being a virtual network. There are two publicly known examples of a virtual network undertaking preparations for attacks (see figure 3.10). We should point out that, now that the networks in question have been wound up, this is not contributing to jihadis' confidence in virtual networks.

Figure 3.10 Examples of virtual networks

Various operations that have led to arrests in Europe and North America in recent months indicate the presence of virtual networks. Jihadi suspects arrested in Canada formed part of an international virtual network, a number of whose members were also physically in touch with each other.[133] *Two Americans in the (alleged) network carried out target reconnaissance in Washington, DC in the spring of 2005. These reconnoitres took place less than one month after the two Americans had had a meeting in Canada with three of the 17 extremists recently arrested in Canada. The material from the reconnaissance was found with Irhabi007 (a well-known jihadi hacker) in the United Kingdom. The network appeared to have an even wider reach, because one month before the arrest of Irhabi007, one of his accomplices - a man born in Sweden - was arrested in Bosnia for planning an attack. This arrest in turn led to the detention of four Danes, who allegedly also formed part of the same network.*
According to the SITE-institute, it is clear that these individuals would probably never have met, far less collaborated, without the Internet.[134]

A plan was recently frustrated "to destroy an underwater tunnel connecting New Jersey and New York City and inundate lower Manhattan". [....] The plot that was disrupted in the first week of July was still in the planning stages and was led by a 31-year-old Lebanese national named Assem Hammoud. Living in Beirut when arrested, Hammoud is a 2002 graduate in commerce of Concordia University in Montreal and was teaching economics, business ethics and human resources at the Lebanese International University. [....] Hammoud was living a normal life, had no police record and had an extended family, none of whom seems to have known of his radical tendencies.

Assem Hammoud-who was using the alias Amer al-Andalusi-appears to have been the leader of an entirely "virtual" would-be terrorist operation. Accounts to date show that Hammoud and seven other individuals had joined together to plan a suicide attack on a tunnel connecting New Jersey and lower Manhattan. The group had never met as a unit, and instead had communicated via the internet and was spread over three continents. Three of the eight are now under arrest: Hammoud, an unnamed Syrian and an individual of undisclosed nationality. [....] The FBI has said that the five others involved in the plot-a Saudi, a Yemeni, a Jordanian, a Palestinian and an Iranian Kurd-have been "largely identified" but have not been apprehended. [....] The FBI and the U.S. Department of Homeland Security (DHS) have underscored that the Hammoud-led plot was very much still in the planning stages; no explosives had been acquired, financial support was not apparent and none of the plotters had visited New York. [....] While there is not yet any information showing a direct connection between the plotters and al-Qaeda, Assem Hammoud told his Lebanese interrogators that he had been motivated by the example of Osama bin Laden and al-Qaeda's attacks, and that he was acting "on a religious order from bin Laden." For instance, Hammoud told the Lebanese: "I am proud to carry out his orders"." [135]

There will be a lesser need for trust for relatively innocent and non-punishable activities, such as discussing certain topics, than for truly criminal acts such as the commission of terrorist activities. After all, the consequences with non-punishable activities are much more limited if there is a breach of trust and information leaks out, or if it turns out that a member of the network is a detective passing himself off as someone else. But there is still an impression that the most important factor in martyr-type activities is not always their successful completion but rather the fact that the individual was prepared to commit the act in the first place. The Prophet, after all, said that it was not the deed in itself that is important but the intention behind it. In this respect, even some action contrived in virtual reality and then frustrated may still be successful. Discovery no longer matters so much. In this sense, it is therefore also conceivable that some individuals who only know each other on a virtual basis might at some point get together for an attack. This would be the fulfilment of a similar group process on the Internet as happens in physical networks.

In addition, some active jihadis on the Internet know each other already via physical contacts or networks. Can we really talk about a virtual network in that case?
The fact that people already know each other does not mean that they would feel as free to discuss particular matters in the physical world, or that they would share the same ideals and perceptions or form part of the same virtual networks. It is imaginable, for example, the two individuals might know each other from the same mosque, but might only communicate with each other about participation in the jihad on an interactive basis and using nicknames, without realising that they knew each other. The fact that people know each other is not, therefore, the deciding factor in distinguishing them from ordinary networks and the threat they pose: there is a difference.

135 Scheuer 2006.

As far as the creation of virtual networks is concerned, the AIVD concludes that, in the longer term and particularly because of "virtualisation", there might eventually be an undifferentiated and informal pool of those who are ready and willing to undertake the jihad

> *"[....] who plan acts of violence in varying combinations with each other or on an individual basis. This will increase the risk of local and international elements becoming more closely interwoven with each other. In particular, the Internet makes it easy to forge short-term contacts, either within one's own country or abroad, and to create a temporary virtual network in order to prepare for campaigns.*[136]

The position in such cases, in the words of the AIVD, is that the power of the international jihadi movement will be significantly increased.[137]

3.11 THE INFLUENCE OF THE INTERNET ON RADICALISATION

In its threat scenarios, the NCTb talks about "the Internet as a catalyst for radicalisation" and the AIVD talks about "the Internet as the turbocharger of the jihadi movement".[138] But how exactly does the Internet influence radicalisation? Radicalisation is seen primarily as a process with some sort of start, and can end in the worst cases with a transition to terrorism. Indicating where radicalisation starts and ends is not an exact science, however, and there are also a range of determinative positions. What possible explanations do we have for the role played by the Internet in the onset of radicalisation?

We must, of course, recognise two different sides of the "radicalisation coin": the *demand side* and the *supply side*. Radicalisation has a *demand side* from individuals who, covertly or otherwise, are looking for material on Islam, the life of a Muslim in a non-Muslim western country or perhaps for radical material. On the *supply side*, radicalisation includes Salafis and jihadis.

There is a large group of Muslims, mostly young people, in non-Muslim western countries, who feel isolated within the societies in which they live. Because these youngsters see their future in the West, unlike their parents, while at the same time experiencing a strong element of distrust from Western society, they are looking for their own identity and for a position to adopt in Western society. This is their quest for their own identity, and they struggle with numerous issues concerning life and religion. When hunting for answers to these questions, they may end up in an environment with which they are familiar and which is easily accessible, namely the Internet. Not only can they find a great deal of information there, but they can also become part of a virtual (Muslim) community, exchanging ideas and blowing off steam by expressing their frustrations with other like-minded individuals who share their fate. They experience the Internet as "[...] one of the few available resources in their 'battle', and they feel relatively safe while using the Internet. Safe as regards the police, security and protection agencies, but also safe as regards their families and traditional influences. The corrective influence of parents and cultural standards and values disappears to a large extent while they are using Internet."[139] Young Muslim women in particular regard the Internet is being a safe environment.

136 AIVD 2006, p. 61.
137 AIVD 2006.
138 NCTb 2006b, AIVD 2006, p. 43.
139 Roy 2005, p. 153-170, AIVD 2006 and interview 4.

"These young Muslim women take to the Internet like a hot bath. This is the place where they can be themselves, without interference, where they can get in touch anonymously with other young Muslim women and can also get in touch with the opposite sex in a way that is socially acceptable within Islam. This means that the Internet becomes an extension of their physical being for young Muslim women, whose scope for physical movement is severely restricted when they attain the age of puberty."[140]

The combination of young Muslims in non-Muslim western countries and the facilities of the Internet for creating virtual communities and collecting information are the reasons why the Internet can have a part to play in the demand side of radicalisation. But the part played by the Internet in this context is more important for its social significance than as a catalyst or turbocharger for radicalisation. We are still missing an important aspect to explain why and how the Internet can contribute toward radicalisation, and for this we have the turn to the supply side.

The Salafi's and jihadis are clever at exploiting questions about life from the homeless Muslims, through packaging and selling Islam and the jihadi battle in one-liners. The Salafi intention, with their presence on the Internet, is to mobilise Muslims via the provision of information and propaganda for their own vision of Islam. Although some of Salafis do not support participation in the armed jihad, their view of Islam may make some individuals more receptive to armed conflict. Depending on how receptive the individual in question is, the Salafi material may, however, be more of a hindrance than a help.[141]

The jihadis go one step further and try to mobilise other Muslims for the jihad by way of propaganda, recruitment and by offering training material, as well as providing them with knowledge about how to engage in the battle. The universal and global nature of the (ideal) virtual community, the scope for self interpretation of Islam, linked with religious ignorance on the part of a large proportion of European Muslim youths and their lack of a mastery of Arabic, mean that the information is prescriptive, fundamentalist/orthodox, simple in nature, conceptually impoverished and that its underlying ideology is frequently incoherent. The supply outlines a Muslim identity that is quite distinct from national or ethnic origins, and an idealised picture that is quite alien to the concrete society where these homeless people live. There is also a lack of any critical reflection or information concerning context and history. There is little evidence of true discussion between protagonists and antagonists, although a certain amount of religiously or ideologically inspired discussion can be traced on the Internet in the Netherlands. Internet is also the perfect place for self-appointed masters providing a different religious interpretation, and for the self-taught.[142]

The Internet's problems are therefore that the supply is largely based on a limited, one-sided and simplistic (i.e. orthodox and/or radical) interpretation of Islam and that the supply is not aimed at letting the homeless operate

140 Pels 2003.
141 Buijs et al, 2006, p. 275.
142 Roy 2005, p. 153-170, AIVD 2006.

better in the society where they live, but rather at mobilising them for the 'pure' Islam or the global jihad. By broadcasting certain messages or videos time after time, and by repeatedly presenting justifying texts as the truth, the result is a culture where some individuals may become receptive to the jihad or else feel that the jihad is normal. This means that, in addition to its useful function, the Internet definitely plays a part in the onset of radicalisation.

Jihadi propaganda is not, however, confined to mobilisation of ordinary Muslims, but also extends to further radicalisation. Interested parties are lured to more radical sites with hyperlinks on discussion forums. The propaganda is also aimed at those who have already undergone radicalisation and provides them with even tougher material. Websites offer the facility for chatting with jihadis and two-way communication among radicals, thus facilitating the formation of groups. Research has shown that anonymous communication by computer results in a stronger group identity, with stronger feelings of responsibility among the group, and results in more straightforward group polarisation. This might mean that groups on the Internet could turn into radicals more quickly. One-sided propaganda and repetition of messages via the Internet will make a further contribution towards this.[143] "Communication is quite open at the outset, but then becomes more confidential within a limited circle, and finally ends up as clearly conspiratorial behaviour. First of all there will be a posting on a website or newsgroup, including a reference to a certain site, where there can be a discussion (including on matters of faith) using a chat program with a larger number of participants or on an individual basis. Some individuals are then propositioned to explore matters further in a one-to-one chat session. Such bilateral sessions are often clearly aimed at recruitment."[144] The intentions of the jihadis also therefore include recruiting individuals via the Internet for actual campaigns, as well as contributing towards further radicalisation. They also provide training material, and attempt in this way to provide individuals with knowledge on how the battle can be waged, using which resources. This can vary from relatively innocent actions, such as hacking into particular web sites, through to terrorist attacks. On the other hand, radical individuals may volunteer to commit violent activities (conscription) or deepen their radical outlook quite independently, resulting in the 'self-igniting' effect.

One illustration of the influence of the Internet on further radicalisation is that the Internet played an important part in the formation of the group of perpetrators of the July 2005 attacks in London, and thus in the commission of an attack. "It just starts with a few youngsters [...]. They feel angry or insulted, they want to belong somewhere, and they are looking for an aim in life. They find like-minded individuals on the Internet, so they have no further idea of how small the world really is. 'The Internet is really stimulating. Whatever you do, you get the feeling that you're changing the world.'"[145] It is also interesting that Imam Samudra, convicted as field coordinator for the attacks in Bali on 12 October 2002, stated that he had become convinced by reading a number of standard works and articles on radical websites.[146]

143 Meertens et al. 2006.
144 AIVD 2006, p. 48.
145 Persson 2005.
146 Weimann 2006, p. 106.

There is also one known example in the Netherlands of an individual who underwent the radicalisation process largely via the Internet, namely that of the self-igniter from Sas van Gent, whom we mentioned earlier. The Internet was also influential in the radicalisation of Samir A. And the two main suspects in the failed attacks on German trains at the end of July 2006 only apparently became radicals after their arrival in Germany and as a result of Al Qaeda propaganda on the Internet. They also came across instructions on the Internet for the manufacture of the bombs. The bombs in the suitcases that were found were 90 per cent in line with these instructions.[147]

All things considered, our conclusion is that the Internet facilitates the entire process of radicalisation. There is a supply available for every phase of radicalisation, to "[...] indoctrinate interested parties step by step in jihadi ideology, either with help or on their own." The supply is often also in multimedia format and more interactive than other sources, making it more attractive to youngsters.[148] In this way, a potential jihadi can undergo processes of formation and reinforcement of ideology and ideological indoctrination. It also contributes to the formation of groups and networks of like-minded individuals. This may mean that individuals and groups start to turn against society, ideologically in the first instance but possibly in an activist, violent manner in the fullness of time.

The question of how and how much the Internet actually plays a part in radicalisation, and ultimately in leading to terrorism, cannot be fully addressed in this study, and it remains an interesting research question. Does the journey towards dependence on radical ideology start on the Internet, or is that merely a stopping-off point or terminal? To what extent do radical mosques and imams have a part to play? Is the case of the self-igniter from Sas van Gent an isolated one, or should we expect more cases of self-ignition in the future? The final answers to these questions can only be provided by further research.

3.12 FINAL ASSESSMENT

The threat emanating from the Internet as a resource is primarily an indirect one. Terrorist activities per se are not involved, by contrast with use of the Internet as a target and a weapon. What is involved is the creation of conditions in which jihadis can reach a wider target group, can function better, can disseminate and acquire relevant knowledge, and can communicate amongst themselves. The use of the Internet can also simplify the preparation and implementation of terrorist activities, thanks partly to the opportunities for gathering information and creating virtual networks.

Looked at from the perspective of radicalisation, the greatest threat at this point emanates from propaganda spread via the Internet, combined with the relatively large group of primarily young Muslims looking for answers to numerous questions on life and religion. The propaganda is disseminated professionally, with great penetration and relatively little by way of contradiction. The propaganda is not restricted to one-way traffic: the jihadis actively attempt to enter into an interaction with interested parties. When combined with the fact that it is primarily large groups of youngsters who have access to the Internet and use it intensively, it becomes clear that Internet propaganda contributes towards (further) radicalisation. This is certainly case for young Muslim women because of the attraction of the Internet for them (demand side) when combined with the active role of radical young Muslim women on the supply side.
There is a potential for reaching a large group of Muslims who have not yet turned into radicals. And it is this contribution of propaganda towards radicalisation that is worrying, because radicalisation operates not only to lower the barriers to recruitment for the jihad, but might also lead in future to an increase in terrorist activities.

Looked at from the perspective of terrorism, the greatest threat at the moment emanates largely from the (facilities for) creation of virtual networks and the use of the Internet for training purposes. Being prepared to carry out terrorist activities is one thing, but having the personnel, knowledge, skill and resources to do so is just as important. If virtual networks primarily increase the support base for the jihadi movement, then - for the category of individuals designated as "home grown terrorists" in particular - the readily available training material may contribute towards converting intentions into actions as regards carrying out terrorist attacks. This is certainly the case when we consider that the Internet is also extensively used for acquiring information, with a great deal of information on potential terrorist targets being accessible. Dissemination of knowledge via the Internet and virtual networks by jihadis, in the form of training material, also contributes towards a speedy dissemination of doctrine. Practical experience built up in Iraq, for example, quickly finds its way to the Internet and is accessible on a worldwide basis within a short space of time.

The threat emanating from other forms of Internet usage, such as mutual communication, planning, recruitment or fund-raising, is less concrete or (as far as the NCTb is concerned) less obvious. Either they occur less often and/or are less obvious, or else the medium of the Internet distorts the classic image of them, as in the case of recruitment.

147 ANP 2006.
148 This final point is based on NRC 2005.

4

CONCLUSIONS

Before presenting our conclusions, it would be appropriate to make a remark on their shelf life. The Internet is a quickly developing environment, and jihadis not only anticipate this but also respond to "threats" from governments. Jihadis' use of the Internet is therefore extremely dynamic. Our conclusions are based on how we see things at the present time (the end of October 2006), although where possible we have taken account of predictable developments. Any developments that might alter the perceived threat will be reported in the Dreigingsbeeld Terrorisme Nederland (DTN) [Terrorist Threat Assessment Netherlands], which is issued regularly, along with any updated assessment of the threat.

1 Cyber attacks by jihadis against (the infrastructure of) the Internet are unlikely

A cyber attack on the global or Dutch Internet itself is not considered likely. While a cyber attack involves a lower threshold than, for example, suicide attacks, so that there is a potential for larger numbers of jihadis being willing and able to undertake them, the most significant counter-arguments are that bringing the Internet to a halt would also switch off the jihadi infrastructure on the Internet, and it would not appeal to their sense of martyrdom. Other arguments we have considered include that different types of attack - such as bomb attacks on public transport - have a greater impact, whereas the consequences of cyber attack may well be significant, but cannot be guaranteed (from the terrorists' perspective).
Also, a successful cyber attack is not a realistic possibility, primarily as a consequence of the measures already taken against this. If we were to expect a cyber attack, then it would be a small-scale attack for a limited period, or else a coordinated combination of small-scale cyber attacks.

2 Other types of cyber attacks by jihadis against (the infrastructure of) the Internet are unlikely

Other types of attack against Internet including (a) a physical attack, (b) an electromagnetic attack, or (c) indirect attacks such as via power supplies, are considered unlikely.
Neither the Dutch nor the global Internet would actually be disrupted by such an attack. There may well be opportunities for small-scale attacks, but on the other hand steps have been taken to minimise the chances of these and to restrict the effects they would have. While one of these other sorts of attack against the infrastructure of the Internet appears more likely than a cyber attack, and has its own attractions for jihadis, we are justified in asking whether terrorists would not prefer a bomb attack against a soft target instead of an important Internet location.

3 Cyber attacks via the Internet are unlikely

An attack via the Internet, with the Internet operating as a weapon against other targets, may well be foreseeable, but is considered to be unlikely. There are nevertheless opportunities for

this resulting from vulnerabilities in, for example, software for process management (SCADA) used by a variety of sectors. In addition, there are some attractive aspects, but such attacks generally require a great deal of (insider) knowledge. Classic attacks, such as bomb attacks or suicide attacks, can also be better exploited for publicity purposes. A combination of one or more classic attacks, deploying the Internet as a weapon, appears more probable. This would amplify the effect of such an attack.

4 Propaganda via the Internet contributes towards radicalisation

Propaganda is disseminated professionally via the Internet, with great penetration and relatively little by way of contradiction. The propaganda is not restricted to one-way traffic: the jihadis actively attempt to enter into an interaction with interested parties.
When combined with the fact that it is primarily large groups of youngsters who have access to the Internet and use it intensively, it becomes clear that the result is a breeding ground for (further) radicalisation. This is certainly the case for young Muslim women because of the attraction of the Internet for them (demand side) when combined with the active role of radical young Muslim women on the supply side.

5 Acquisition of information via the Internet potentially contributes towards the commission of terrorist activities

For jihadis, as for everyone else, the Internet is an inexhaustible source of information, which can also be collated using professional tools such as data mining. This information can be useful in the commission of terrorist activities. While this information can also be acquired in other ways, the facilities for gathering information via the Internet are more approachable, less expensive, simpler, less labour-intensive and larger-scale. In particular, developments in the area of (real-time) satellite pictures, potentially combined with an Internet connection, as in the case of Google Earth, are making rapid progress. This makes the acquisition of information via the Internet a very usable resource for jihadis, and potentially contributes to the perpetration of terrorist activities.

6 Fundraising via the Internet by and for jihadis is still quite limited: a shift towards more covert fundraising can be expected

There are potentially many opportunities for fundraising by and for jihadis, and we are aware of some examples, but it is not yet a common phenomenon in practice. This form of fundraising is, after all, fairly conspicuous and therefore vulnerable to government intervention. As Internet banking becomes more and more straightforward and commonplace, use and abuse of this facility by jihadis will also undoubtedly increase. Combined with the increasing interest of hackers in online fraud, this may lead to a shift from more public to more covert fundraising. Fundraising via the Internet may also increase as a result of new digital and anonymous payment facilities.

7 Use of the Internet results in more interactive forms of recruitment, which cannot yet be easily identified, and also in conscription and self-igniters

It is not really likely that anyone from the Netherlands would allow himself or herself to be recruited directly by recruiters from international terrorist groups, such as Hamas, on a one-to-one basis, via the Internet. This is not to ignore the fact that, for example, the core of Al Qaeda might have an inspirational impact on the formation of virtual networks, but it would be going too far to call this recruitment on the part of Al Qaeda. A markedly interactive form of recruitment is, however, perceptible on the Internet, strongly associated with the interactive methodologies of propaganda companies. One of the Internet's primary characteristics is that potential warriors are keen to report voluntarily for participation in the violent jihadi battle *(conscription)*. Conscription does not involve recruitment in the formal sense, even though there are still two parties involved. There can also be *'self-ignition'* in relation to the Internet, where someone might decide to embark on a jihad on his or her own initiative, and where it is impossible to distinguish between two different parties. Self-ignition cannot be described as recruitment in the formal sense. If it is difficult in the physical world to distinguish between the transition from the radicalisation process to recruitment, on the one hand, and conscription on the other hand, then this is certainly the case with Internet. The question perhaps ought to be whether the rise of the Internet means that the classic recruiter/recruit concept still persists, or whether it is gradually being replaced by a permanent and interactive mix of top-down and bottom-up information provision and acquisition, mixed with online encouragement, steering or network formation. Recruitment, conscription and also self-ignition via the Internet are certainly still quite new phenomena and we are not yet in a position to fully understand them.

8 Use of the Internet for training purposes has the effect of lowering the threshold against the commission of attacks

Being prepared to carry out terrorist activities is one thing, but having the knowledge, skill and resources to do so is just as important. For "home grown terrorists" in particular, the readily available training material may contribute towards converting intentions into actions as regards carrying out terrorist attacks. This is certainly the case when we consider that the Internet is also extensively used for acquiring information, with a great deal of information on potential terrorist targets being accessible. Dissemination of training material via the Internet by jihadis also contributes towards a speedy dissemination of doctrine. Use of the Internet for training purposes has the overall effect of lowering the threshold against the commission of attacks.

9 Jihadis use the Internet for mutual communication and planning

There are sufficient indications that jihadis communicate among each other and plan terrorist activities via the Internet. In doing so, they make use of the opportunities for anonymous and secretive communication. As well as having benefits for jihadis, this usage of the Internet affords security and detection agencies the opportunity to intervene. The jihadis are very well aware of this.

10 Virtual networks increase the support base for the jihadi movement

An informal pool of those ready and willing to undertake the jihad is formed as a result of the formation of virtual networks, and they can develop violent activities either on their own or in varying combinations with each other. This allows local and international elements to become intertwined with each other, significantly increasing the power of the international jihadi movement.

11 Use of the Internet sustains the entire process of radicalisation

Every phase of radicalisation requires an element of supply. Using the Internet, a potential jihadi can undergo processes of formulation and strengthening of ideology as well as ideological indoctrination. We would, however, like to see further academic investigation into group processes via the Internet, and the influence of Internet usage on radicalisation.

12 From the perspective of radicalisation, the greatest threat emanates from propaganda spread via the Internet, combined with the relatively large group of young Muslims looking for such information

Propaganda is disseminated professionally and interactively, with great penetration and relatively little by way of contradiction. If we combine this with the potentially substantial target market of vulnerable young people, then it is clear that propaganda via the Internet makes the largest contribution to (further) radicalisation, more so than other forms of Internet usage. And it is this contribution of propaganda towards radicalisation that is worrying, because radicalisation operates not only to lower the barriers to recruitment for the jihad, but might also lead in future to an increase in terrorist activities.

13 From the perspective of terrorism, the greatest threat emanates largely from the (facilities for) creation of virtual networks and the use of the Internet for training purposes

If virtual networks primarily increase the support base for the jihadi movement, then - for the category of individuals designated as “home grown terrorists” in particular - the readily available training material may contribute towards converting intentions into actions as regards carrying out terrorist attacks.

Finally we would present our findings based on the analysis of Jihadism on the Dutch Internet:

1. Dutch jihadis have hitherto focused primarily on organising, offering and circulating jihadi information and materials. This information is primarily for propaganda purposes, but is also to some extent focused on training.
2. Many sites offer the facility of interaction between jihadis and a wide and varied public of interested parties, as well as between jihadis themselves. It is not just information fully targeted and customised that can be exchanged with interested parties, based on specific issues or current events, but this can also lead to the formation of virtual networks, or else the recruitment of those who are truly interested in the jihad battle.
3. Virtual Jihadism on the Dutch Internet may be a pointer towards real-life jihadis in the Netherlands.
4. Dutch virtual jihadis take inspiration from an international, virtual translation program, and they primarily translate material taken from the range of “pre-selected” material made available by others.
5. Young Muslim women are very active as translators, in the development of sites and in dealing with the public.
6. Dutch virtual jihadis operate either on a structural basis or sporadically on a variety of neutral discussion forums of a non-jihadi nature. The jihadi message reaches a much wider audience, with new possibilities for growth, but with a more limited risk of intervention by government.

LITERATURE

AIVD 2002a
AIVD, *Jaarverslag 2002 Algemene Inlichtingen- en Veiligheidsdienst,* 2003.
[Annual Report for 2002, General Intelligence and Security Service, 2003.]

AIVD 2002b
AIVD, *Rekrutering in Nederland van incident naar trend* [Recruitment in the Netherlands, from incident to trend], The Hague: Ministry of Home Affairs and State Relations, 2002.

AIVD 2004
AIVD, *Van dawa tot jihad. De diverse dreigingen van de radicale islam tegen de democratische rechtsorde* [From dawa to jihad. The various threats against the democratic system from radical Islam], The Hague: Ministry of Home Affairs and State Relations, 2004.

AIVD 2006
AIVD, *De gewelddadige jihad in Nederland: Actuele trends in de islamistisch-terroristische dreiging* [The violent jihad in the Netherlands: current trends in the Islamic-terrorist threat], 2006.

ANP 2006
ANP, *Mohammed cartoons motive for suitcase bombs*, 2 September 2006.

Apuzzo 2006
M. Apuzzo, *'Britisch man indicted on terrorism charges over Internet sites'*, Associated Press Newswires, 20 July 2006.

As-Suri 2004
As-Suri, *Oproep tot het universeel islamitisch verzet* [Call for universal Islamic opposition], 2004.

Bang et al 1996
S. Bang et al, *Het complete internet handboek* [The complete Internet Handbook], Schoonhoven: Academic Service, 2nd fully revised edition 1996.

BBC Monitoring 2006a
'Seven to be charged in Denmark over terror-support T-shirts', BBC Monitoring Service, 20 February 2006.

BBC Monitoring 2006b
'Authorities concerned about Hezbollah, Hamas presence in Germany', BBC Monitoring European, 24 July 2006.

Bell 2006
S. Bell, *'Two Toronto suspects took part in discussions. Web forum linked cells'*, National Post, 15 June 2006.

Benschop 2004
A.Benschop, *Kroniek van een aangekondigde politieke moord - Jihad in Nederland* [Chronicle of an announced political murder - Jihad in the Netherlands], 2004 .
(www.sociosite.org/jihad_nl.php)

Benschop 2006a
A. Benschop, *CyberJihad Internationaal: Waarom terroristen van internet houden* [CyberJihad International: Why terrorists like the Internet], 2006.
(http://www.sociosite.org/)

Benschop 2006b
A. benschop, *CyberTerrorisme: Dodelijk geweld vanaf het toetsenbord* [CyberTerrorism: Deadly violence from the keyboard], 2006.
(http://www.sociosite.org/)

Buijs et al 2006
F.J. Buijs, F. Demant, A. Hamdy, *Strijders van eigen bodem* [Home-grown warriors], Amsterdam: University Press, 2006.

Bunt 2003
G.R. Bunt, *Islam in the Digital Age. E-Jihad, Online Fatwas and Cyber Islamic Environments*, London: Pluto Press, 2003.

Castells 1998
M. Castells, *The Rise of the Network Society. Volume 1 of the Information Age*, Blackwell Publishers Inc., 1998.

Colin 1997
B. Colin, *'The Future of Cyberterrorism'*, Crime and Justice International, March 1997, p. 15-18.

Computable 2006
'Ook AMS-ix heeft last van stroomstoring Amsterdam' ['Even AMS-IX is troubled by Amsterdam power cut'], Computable.nl, 30 May 2006.

Conway 2005
M. Conway, *Terrorist 'use' of the internet and fighting back*, Dublin: Department of Political Science College Green Trinity College, 2005.

Cops@Cyberspace 2006a
Cops@Cyberspace, Annual series 9, no. 31 2006.

Cops@Cyberspace 2006b
Cops@Cyberspace, Annual series 9, no. 29 2006.

CRS 2005a
C. Wilson, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS-report for Congress, 1 April 2005.

CRS 2005b
J. Rollins, C. Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, CRS-report for Congress, 20 October 2005.

Dasselaar 2006
A. Dasselaar, *En toen lag alles plat* [Then everything came to a halt], Planet.nl, 8 May 2006.

Denning 1999
D. E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Georgetown University, 1999.

EZ 2005
Dutch Ministry of Economic Affairs, *Questions from MP Gerkens (SP) to the Minister and Secretary of State for Economic Affairs on underestimated cybercrime,* Answers to Parliamentary questions dated 7 July 2005, Lower House 2004-2005, 2023, 2005.

Foxtrot 2004
'Jihaad planning part2', Foxtrot.messageboard.nl, 2004.
(foxtrot.messageboard.nl/2767/viewtopic.php?t=108, Jihaad planning deel 2, 020104).

Gibson 2002
S. Gibson, *The distributed reflection DoS-attack,* 2002.
(http://grc.com/dos/drdos.htm)

Green 2002
J. Green, *'The Myth of Terrorism'*, Washington Monthly, November 2002.

Guardian 2005
'Algerian guilty of downloading bomb data', The Guardian, 25 November 2005.

Higgins et al 2002
A. Higgins, K. Leggett, A. Cullison, *'How al Qaeda put Internet to use'*, The Wall Street Journal, 11 November 2002.

Hoffman 2006
B. Hoffman, *The Use of the Internet by Islamic Extremists*, Testimony presented to the House Permanent Select Committee on Intelligence, May 2006.

Holst 2006
R. van Holst, *'Mediagebruik van allochtonen in Nederland'* ['Media usage by immigrant citizens in the Netherlands'], Mira Media January 2006.

Huizer 1998
E. Huizer, *Structuur en organisatie van het internet* [Structure and organisation of the Internet], 1998,
(http://nieuws.surfnet.nl/nieuws/snn-archief/achtergrond/jg97-98/internet.html.)

Independent 2006a
'The new breed of cyber-terrorist', The Independent, 1 June 2006.

Independent 2006b
'Tight security as suspects accused of airline bomb plot appear in court', The Independent, 23 August 2006.

Jamestown 2006
'Jihadi forums marvel at new role of snipers', Jamestown Terrorism Focus, 4 April 2006.

Justitie 2005a
Minister of Justice, *Answers to Parliamentary questions from MP De Wit (SP) to the Minister of Justice concerning the proposed duty to retain data traffic information*, 6 September 2005.

Justitie 2005b
Minister of Justice, *Answers to Parliamentary questions from MPs Weekers (VVD) and Wolfsen (PvdA) to the Ministers of Justice and Home Affairs and State Relations, concerning programs on the Internet that might be of assistance to terrorists*, 6 October 2005.

Kortekaas 2005
J. Kortekaas, *Risico-analyse georganiseerde criminaliteit. Uitwerking instrumentarium en toepassing op de ICT-ontwikkelingen* [Organised crime risk analysis. Elaboration of mechanisms and their application to ICT developments], The Hague: Elsevier overheid 2005.

Kwint 2004
Project group KWINT *Continuïteit, Rapportage Internationale Kwetsbaarheden NL Internet* [Report on International Vulnerabilities of the Dutch Internet], 23 November 2004.

Labi 2006
N. Labi, *'Rapportage terroristen op het internet. Jihad 2.0'* ['Reporting terrorists on the Internet. Jihad 2.0'], Vrij Nederland 1 July 2006.

Lewis 2002
J.A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, CSIS, December 2002.

Lia 2006
B. Lia, *'Al-Qaeda online: understanding jihadist internet infrastructure'*, Jane's Intelligence Review 18, January 2006, p. 14-19.

Luiijf 2006
H.A.M. Luiijf, R. Lassche, *SCADA (on)veiligheid: een rol voor de overheid?* [SCADA (in)security: a role for government?], TNO 15 April 2006.

Meertens et al 2006
R.W. Meertens, Y.R.A. Prins en B. Doosje, *In iedereen schuilt een terrorist* [There's a terrorist inside everyone], Schiedam: Scriptum 2006.

Military.com 2005
'Army to Crack Down on Military Bloggers', Military.com, 31 August 2005. (www.military.com/NewsContent/0,13319,76350,00.html).

Mitnick 2006
K. D. Mitnick, W.L. Simon, *The Art of Intrusion*, Wiley Publishing, 2006.

Muller et al 2004
E.R. Muller, R.F.J. Spaaij, A.G.W. Ruitenberg, *Trends in terrorism*, Alphen aan den Rijn: Kluwer, 2004.

Nationaal 2006
'Jihad krijgt girlpower op; Radicale moslima's tokkelen nieuw' [Jihad gets girlpower; Radical Muslim girls play a new tune], Nationaal (Flanders), 3 July 2006.

National Post 2006
'Online hate growing rapidly', National Post, 6 April 2006.

NCTb 2006a
NCTb, *Dreigingsbeeld terrorisme Nederland nr.5* [Terrorist Threat Assessment Netherlands no. 5], 2006.

NCTb 2006b
Google Earth, 2006.

Newsbytes 2006
Newsbytes News Network, *New Internet Threat Emerges: 'website cloaking'*, 9 March 2006.

Nieuwsblad 2006
'Ik zoek een bruid voor mijn man' [I'm looking for a bride for my husband], Het Nieuwsblad 4 July 2006.

NRC 2005
'Het ronselen voor de jihad gaat volop door' [Recruitment for the jihad in full swing], NRC-Handelsblad 3 January 2005.

NRC-Next 2006
'Mediamachine wapen van terreur, op basis van een interview van K. Gannon met een camera-man van As-Sahab' [Media machine weapon of terror, based on an interview by K. Gannon with a cameraman from As-Sahab], NRC-Next 26 June 2006.

Nu.nl 2006a
'Marokkanen hacken Israëlische websites' [Moroccans hack Israeli websites], Nu.nl 29 June 2006.

Nu.nl 2006b
'Terreuraanval op internet blijkt heel eenvoudig' [Terror attack on the Internet looks quite simple], Nu.nl 8 May 2006.

Nu.nl 2006c
'Website Geert Wilders opnieuw gehackt' [Geert Wilders' website hacked again] Nu.nl 16 July 2006.

Nu.nl 2006d
'Verdonk getroffen door Google-bom' [Verdonk hit by Google bomb], Nu.nl, 3 March 2006.

Pels 2003
T. Pels, *'Respect van twee kanten, over socialisatie en lastig gedrag van Marokkaanse jongens'* [Respect from two sides, on socialisation and troublesome behaviour by Moroccan youths], Migrantenstudies, themanummer Jeugd, 19(4) 2003, p. 228-239.

Persson 2005
M. Persson, *'Het begint met een stel jongens; Terrorisme'* [It starts with a few boys; Terrorism], de Volkskrant, 23 July 2005.

Planet.nl 2005
'Meer dan een miljoen patiëntengegevens op straat' [More than one million patient files on the street], Planet.nl, 2 September 2005.

Planet.nl 2006a
'Reacties: Grotere én andere gevaren' [Reactions: Bigger and different dangers], Planet.nl, 12 May 2006.

Planet.nl 2006b
'Leven na de internetaanslag' [Life after the Internet attack], Planet.nl, 11 May 2006.

Planet.nl 2006c
'24 uur internet onder vuur' [24 hours under fire], Planet.nl, 9 May 2006.

RAND 2000
RAND, *Mapping the risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information,* 2000.

Rechtspraak.nl 2006
'Rechtbank heeft uitspraak gedaan in zaken verdachten Hofstadgroep' [Court has passed sentence in the cases of the Hofstad group accused], Rechtspraak.nl, 2006. (http:/www.rechtspraak.nl/Gerechten/Rechtbanken/s-Gravenhage/Actualiteiten/Rechtbank+heeft+uitspraak+gedaan+in+zaken+verdachten+Hofstadgroep.htm).

Rogan 2006
H. ROGAN, *Jihadism online- A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes*, Kjeller: Forsvarets Forskningsinstitutt Norwegian Defence Research Establishment (FFI/Rapport-2006/00915), 2006.

Roy 2005*
O. Roy, *De globalisering van de islam* [The globalisation of Islam], Amsterdam: Van Gennep, 2nd edition 2005.

Rozen
L. Rozen, *'Forum point the way to jihad'*, Wired News, 6 August 2003, (http://www.wired.com/news/culture/1,59897-0.html)

* The French language version was published in 2002.

Scheuer 2006
M. Scheuer, *'The New York Plot: The Impact of Bin Laden's Campaign to Inspire Jihad'*, Terrorism Focus, 3 (28), 18 July 2006.

SITE-Institute 2005a
SITE-Institute, *Global Islamic Media Front Issues 'Jihad Candid Camera' Video of Insurgency in Iraq,* 6 September 2005.

SITE-Institute 2005b
SITE-Institute, *Al-Qaeda university for jihad subjects*, 10 October 2005.

SITE-Institute 2006a
SITE-Institute, *Zawahiri video exemplifies latest jihadi media distribution trends,* 12 March 2006.

SITE-Institute 2006b
SITE-Institute, *The Global Islamic Media Front Circulates 'The Comprehensive study on how to Hack the Crusaders' and the Zionists' websites, as was authored by Irahbi 007,* 2 May 2006.

SITE-Institute 2006c
SITE-Institute, *The 'Nemo Document' of Comprehensive Mujahid Training for Jihad - Explosives, Poisons, Physical Preparation, Nuclear Weapons, and Guns*, 26 May 2006.

SITE-Institute 2006d
SITE-Institute, *Complete Audio Message of Usama bin Laden from 4/23/06,* 26 April 2006.

SITE-Institute 2006e
SITE-Institute, 12 May 2006.

SITE-Institute 2006g
SITE-Institute, *The Global Islamic Media Front announces the initiation of infiltrating western internet forums, and issues a call to able muslims to join the information jihad,* 12 January2006.

SITE-Institute 2006h
SITE-Institute, *Canadian arrests portray the value of the internet in global networks,* 6 June2006.

SITE-Institute 2006k
SITE-Institute, *A Forthcoming Video for the First Anniversary of the July 7 London Bombing,* 6 July 2006.

SITE-Institute 2006l,
SITE-Institute, *Plan to inexpensively kill Thousands of American Citizens,* 6 February 2006.

SITE-Institute 2006n
SITE-Institute, *Final Warning from the Taliban to the Afghanis in the Armed Forces and Police in Afghanistan to Remove Themselves from the Battlefield,* 25 July 2006.

SITE-Institute 2006o
SITE-Institute, *A Forthcoming Message from Ayman al-Zawahiri,* 26 July 2006.

SITE-Institute 2006p
SITE-Institute, *The Global Islamic Media Front Presents a Film of the Condition of the American Soldier: 'They are Hurting',* 4 August 2006.

SITE-Institute 2006q
SITE-Institute, *Jihadist Forum Member Advocates Users Beware of Google and its Software Applications,* 28 March 2006.

SITE-Institute 2006r
SITE-Institute, *A Guide for Internet Safety and Anonymity Posted to Jihadist Forum*, 24 March 2006.

SITE-Institute 2006t
SITE-Institute, *A Flyer Providing Information How One May Send Donations to Palestinians Posted to Jihadist Forums,* 25 April 2006.

SITE-Institute 2006u
SITE-Institute, *Jihadist Forum Member Provides a Video of an Advanced Protection System to Military Vehicles and How to Circumvent its Effectiveness*, 3 May 2006.

SITE-Institute 2006v
SITE-Institute, *A manual instructing in the use of clostridium microbe and clostridium botulinum toxin as biological weapons*, 27 January 2006.

Stratix 2004
H. Rood, *Gevolgen uitval .nl domein* [Consequences of the .nl domain going down], Stratix Onderzoek, Schiphol 2004.

Telegraaf 2006
'Algerijn Abbas Boutrab mogelijk al in Nederland bezig met 'Operatie Bojinka 2006' [Algerian Abbas Boutrab possibly already at work on 'Operation Bojinka 2006' in the Netherlands], De Telegraaf, 19 August 2006.

Thiele & Van Vliet 2005
V. Thiele, E. Van Vliet, *Kwetsbaarheid van internet voor bewust menselijk handelen* [Vulnerability of the Internet to deliberate human action], The Hague 2005.

Thomas 2003
T.L. Thomas, *Al Qaeda and the Internet: the danger of 'cyberplanning'*, Parameters, 2003, p. 112-123.

Van Leeuwen 2005
Van Leeuwen, *'Ronselen in Europa voor de Heilige Oorlog'* Recruitment in Europe for the Holy War], in: Justitiële Verkenningen, 31, 2/2005.

Van Yperen 2005
S. van Yperen, *Al-Qa'ida-video's in het NOS-journaal* [Al Qaeda videos in the NOS Journal] Master's Thesis, Erasmus University of Rotterdam, Faculty of History and Humanities, 1 September 2005.

Volkskrant 2005
'Vijver voor extremisten' [The breeding ground for extremists], De Volkskrant, 26 November 2005.

Volkskrant 2006
'Praten met Al Qa'ida en Hamas, er zit niks anders op; Het debat in: de Verenigde Staten' [Talking with Al Qaeda and Hamas: there's no way to avoid it now; The debate in the United States], De Volkskrant, 13 May 2006.

Washington Times 2006
'Nobles & Knaves', The Washington Times, 10 June 2006.

Washington Post 2005
'Al Qaeda and the Internet (Evan Kohlmann, interview transcript)', The Washington Post, 8 August 2005.

Washington Post 2006
'Even terrorists worry about Internet security', The Washington Post, 13 April 2006.

Weimann 2006
G. Weimann, *Terror on the Internet. The New Arena, the New Challenges*, Washington D.C.: United States Institute of Peace Press, 2006.

Wilson 2006
C. Wilson, *Terrorist Capabilities for Cyberattack*, CIIP Handbook, 2006.

Zerkin 2006
A. J. Zerkin, *Thinking the unthinkable: Negotiating with terrorists*, Lecture at the University of Amsterdam, May 2006.

GLOSSARY

Amsterdam Internet eXchange (AMS-IX): the networks of nearly every Internet provider in the Netherlands are connected here. National and international traffic is exchanged. The AMS-IX is the largest Internet injunction in the Netherlands.

Commercial-off-the-shelf: Commercial-off-the-shelf (COTS) software is software developed for an entire market, rather than for individual customers. One example of this is Microsoft Office.

Computer Emergency Response Team (CERT): A CERT is a team that assists in resolving security breaches. Some of the larger CERTs (such as GOVCERT.nl) also fulfil an important informative function and issue what they term 'advisories', with warnings on recently discovered software loopholes and methods for resolving the problems.

Dawa: literally 'a call' to Islam, currently used in the debate on radical Islam to mean the dissemination of radical Islamic ideology.

Defacement: defacement (or defacing) involves unauthorised amendment, replacement or destruction of a website, or else redirecting Internet traffic to a different website by means of DNS hacking or spoofing.

Denial of Service (DoS): limiting or frustrating the operation of the system, application or network.

Distributed Denial of Service (DDoS): Limiting or frustrating the operation of one or more networks, systems, or applications thereon, by misusing a large number of computers. A 'controller' directs the computers to attack a network, system or application at the same time and en masse.

Domain Name Server (DNS): the Internet cannot discharge its functions without support services. Thus there is a link between the normal IP address (a number) on the Internet and the user's known designation by means of a hierarchically organised service. This is the Domain Name Server (DNS). The service operates like a telephone directory. Services such as the World Wide Web, file transfers and e-mail are heavily dependent on the proper operation of this facility.

Encryption: encryption is the process by which data is encoded and decoded using a key consisting of a number of digits and a mathematical algorithm, so that the data cannot be read by anyone without authorisation. This allows confidential communication between parties.

Firewall: this is a protection between the Internet and an internal (possibly commercial) network. It is designed to prevent computer break-ins and the spread of viruses.

Violent political activism: The distinction between this and terrorism is the absence of an intentional targeting of human victims, or the explicit acknowledgement that campaigns will result in mourning for human lives.

The Internet as a target: When the Internet is used as a target, the violence or commission of serious socially disruptive damage is aimed at the Internet itself and its infrastructure. This might take a variety of forms:

- a cyber attack using computers via the Internet;
- a physical attack using conventional weapons against computer hardware or lines of communication;
- an electromagnetic attack using, for example, electromagnetic energy (EMP);
- other indirect attacks or strikes, for example against the electricity supply, so that the Internet (or its infrastructure) can no longer function.

The Internet as a weapon: When the Internet is used as a weapon, attacks are committed against physical targets using the Internet. This might, for example, involve taking over air traffic control systems or management systems for vital installations in the chemical sector. Another example is the disconnection of emergency control centres or crisis organisations, for example by hacking or causing overloads.

Internet Service Provider (ISP): an organisation offering its customers access to the Internet. To do this, the ISP maintains one or more POPs, access points to the Internet for the ISP's subscribers. In addition to providing access, many ISPs nowadays also offer other services. These include, for example, news services, transactional solutions and entertainment services.

IP: IP means Internet Protocol. IP is similar to the postal system. A package of information can be addressed (using an "IP address" or "IP number"), sent over the Internet and finally "delivered" to the correct computer system. IP addresses are allocated by the authorised bodies, for example providers. Every domain name has a corresponding IP number. The IP address of surfopsafe.nl, for example, is 213.156.7.44. It is possible to type an IP address into the "address" field of your browser. This takes you to the domain's Internet pages.

Jihad (in this context meaning armed conflict): the development of violent campaigns against perceived enemies of Islam, in order to achieve a world which as purely as possible reflects what is considered to be contained in the earliest sources of the Islamic faith.

Jihadis: a collective term for jihadi terrorists and jihadi radicals.

Malware: a contraction of malicious and software. A collective name for evil software such as viruses, trojans, spyware, adware, browser hijackers and dialers.

Phishing: a collective name for digital activities aimed at pilfering personal information from people. Using a nepsite or e-mail, the thief (fisherman) tries to get hold of personal information such as credit card numbers, pin codes, national insurance numbers and so on.

Radical Islam (or Islamism): the political-religious quest to bring about a society, using extreme resources if needs be, which as purely as possible reflects what is considered to be contained in the original sources of Islam.

Radicalisation: a mental attitude indicating a readiness to accept the ultimate consequences of an ideology and to convert them into deeds. The result of these deeds can be that resistance, in itself manageable, can escalate to a level that disrupts society because violence is involved, where the conduct results in people being deeply affected as regards their freedom, or because certain groups turn their backs on society.

Recruitment: recruitment involves putting people in the picture and then controlling and manipulating them in order to encourage an internalised radical-political Islamic conviction within these individuals, with the ultimate aim of having them participate in the violent jihad in some way or another.

Root server: a server at the highest level of the hierarchical Domain Name System (see DNS), accordingly fulfilling an essential function in the Internet's 'address book'.

Router: sends packages of information across a network to the correct address.

Salafism/Salafis: When we mention Salafism in this study, what we mean by this is the non-jihadi oriented form of Salafism, with "Salafis" referring to the supporters of this variant. This is in contrast to the jihadi form, which we refer to using the expression "jihadis".

SCADA: covers the entirety of computerisation, electro-technical and information and communication technology deployed for the monitoring (Supervision), direction and surveillance (Control) of processes, And the collection of information (Data Acquisition).

Single Point of Failure: is a single part of a system, which affects the operation of the entire system if it fails.

Spoofing: a technique for obscuring or changing the point of origin of messages. Through the use of spoofing, the identity of an entity (e.g. an individual or system) can be taken over, enabling abuse of an existing trusted relationship.

URL (Uniform Resource Locator): unambiguous location of a file, web page, program, service of some other random item on the Internet, stating not only the location but also the protocol by which the file, web page, program, service or "other random item" can be accessed. The designation URL is often used to provide the web address, for example http://www.surfopsafe.nl/.

Terror: a reign of terror by a state against its own subjects, frequently intended to maintain the power of the ruling political, religious or ethnic elite.

Terrorism: the commission of threats of violence aimed at human life, or the commission of serious socially disruptive material damage, with the aim of causing social change or influencing political decision-making.

Weblog: pages on which the owner (the blogger) reports his discoveries while surfing the Web. This is usual in the form of short messages, sometimes linked with a brief comment or description by the blogger. It is a way of forming interesting lists of links, making it easier for a curious surfer to find specific sites. A weblog does not usually contain links to homepages or domains, but rather direct links to pages within a site.

World Wide Web (WWW): Like "surfing" it, the World Wide Web has now become accepted terminology. Technically speaking, from the point of view of protocols, the most important service at its roots is the hypertext transfer protocol (http), which takes care of the transfer and consultation of web pages. Over the years, the functionality of the Web has been extended with dynamic content and more extensive graphic layouts (Java, ActiveX, flash and so on), data object oriented presentation and exchange (XML).

APPENDICES

APPENDIX 1 Classifications of terrorist / jihadi Internet usage *

Conway	Weimann	Benschop
1. Information provision	1. Communicative use	1. Publicity and propaganda
2. Financing	2. Instrumental use • datamining • networking • recruitment and mobilisation • instructions and online manuals • planning and coordination • fundraising and attacking other terrorists	2. Internal communication
3. Networking		3. Socialisation and discipline
4. Recruitment		4. Psychological warmongering
5. Information gathering	3. Use of the Internet as a weapon	5. Acquisition of information
		6. Fundraising
		7. Recruitment
		8. Training camp
		9. Mobilisation and campaign coordination
		10. Mass destruction (cyber terrorism)
		11. Virtual Islamic state

* Conway 2005, Weimann 2006, Benschop 2006a.

APPENDIX 2 Criteria for determining whether a site is jihadi

A site is jihadi if it proclaims and disseminates jihadi teachings by means of articles, audio-visual documents and other Internet functionalities (such as mailing lists, chatrooms or PalTalk rooms). Jihadism, and therefore a jihadi website, can be recognised by the following characteristics:

- The notion of God characterised by the absolute uniqueness of God (Tawheid).
- The doctrine of Salafism proceeding from belief (Iemaan) in the teaching of the uniqueness of God (Tawheid) and the concrete profession of that faith in practice. This doctrine is the basis of the other doctrines.
- The worship (Ibadaat): this consists of the accepted pillars of Islam (profession of faith, prayer, fasting, paying religious taxes and pilgrimage). The Salafis place special emphasis on the performance of these ritual duties.
- The application of the divine law and legislation (al-Hukm bima Anzala Allah, Shari'a). This involves topics such as God's sole right to make laws and the invalidity of "man-made laws". This doctrine forms the basis of Salafi theory concerning the foundation of an Islamic state and the establishment of an Islamic society.
- The ethic of loyalty and aversion. This means that a Muslim is obliged to confine his loyalty to those of his faith and to display aversion to unbelievers.
- The doctrine of the "chosen group" (at-Ta'ifat al-Mansoera): they considered that they make up this group, as being pure in terms of doctrine.
- The teaching that the jihadi battle for God's sake (al-Jihad fi Sabili Allah), or armed conflict is an obligation on individual Muslims to engage in battle against unbelievers and apostates and to found the Islamic state (the caliphate).

The jihadi Internet sites in the Netherlands can be distinguished from the Salafi ones because of the explicit politicisation of these theological, dogmatic, liturgical and ethnic principles and a call to the (armed) jihadi battle.

Colophon

Publishing
February 2007,
The National Coordinator for Counterterrorism (NCTb)

Translation
Amstelveens Vertaalburo B.V., Amstelveen

Design & coverphotography
Richard Sluijs, The Hague

Printing
DeltaHage, The Hague

The NCTb helps make the Netherlands a safer place to live

The task of the National Coordinator for Counterterrorism is to minimise the risk of terrorist attacks in the Netherlands and to take prior measures to limit the potential of terrorist acts.
The NCTb is responsible for the central coordination of counterterrorism efforts and ensures that cooperation between all the parties involved is and remains of a high standard.