National Coordinator
for Counterterrorism

Jihadists and the Internet

2009 update

Jihadists and the Internet

2009 update

National Coordinator for Counterterrorism (NCTb)
May 2010

In the Netherlands,GOVCERT.NL, NCTb and the Netherlands' Police Agency have played an important role on behalf of the government in the battle against cybercrime (including terrorism via the Internet). These organisations regularly consult on incidents and developments relating to this theme, and in their reports they try to provide as complete a picture as possible of the most important trends.

Foreword

During the last decade the greatest terrorist threat has comes from what is referred to as 'jihadist terrorism'. Certainly since 11 September 2001, many bloody terrorist attacks have been carried out under pretext of a religious armed struggle, known as the 'jihad'.
The NCTb already established, at the start of 2007, that jihadists were using the Internet widely as a resource for propaganda, for example, or to recruit people. The NCTb also investigated the threat of terrorist attacks against the Internet (Internet as a target) or via the Internet (Internet as a weapon).

Both the Internet and jihadism are continuing to develop. That is why it became necessary to review the original assessment of the threat in the form of this '2009 update'. After all, the government and private parties cannot afford to relax and let developments simply run their course. Therefore, since the publication of the earlier study at the beginning of 2007, numerous measures have been taken to counteract the threat based on Internet use by jihadists. Although this study shows that the threat has not substantially changed, the findings in this study provide useful guidelines on how to continue to respond adequately to the threat.

The National Coordinator for Counterterrorism
drs. E.S.M. Akerboom

TABLE OF CONTENTS

Management summary/ conclusions

Grounds and aim

At the beginning of 2007, the NCTb made the observation, in the in-depth study entitled 'Jihadis and the Internet' (hereafter to be referred to as the in-depth study), that jihadists were using the Internet in many ways as a resource, for example for propaganda and recruitment. In the same study the NCTb concluded that it was improbable that jihadists were using the Internet as a weapon or considering it a target. Both the Internet and jihadism are continuing to develop. That is why it became necessary to review the original assessment of the threat in the form of this '2009 update'. The accent is on changes that have occurred since the period from the end of 2006 to the end of 2009.

A The Internet as a target and as a weapon

In the event of the *Internet as a target*, the terrorist activities are aimed at (the infrastructure of) the Internet itself. This means, among other things, Internet nodes (computer parks), functionalities and junctions of the organisations that provide services which are crucial for the functioning of the Internet. One of the ways in which the Internet can be assaulted or attacked is via a cyber attack. In the event that the *Internet is used as a weapon*, attacks are carried out against physical targets via the Internet. Examples are the taking over of air traffic systems or control systems of vital installations in the chemical sector or the electricity supply.

In order to assess jihadist use of the Internet as a target or weapon, the NCTb carried out a literature study and organised an expert meeting. The participants included experts from intelligence services, the academic and scientific community, the police, other government services and from the telecom and Internet sector.

The conclusion is that, without outside assistance, jihadists are not capable of carrying out a successful complex attack on or via the Internet which would have a socially disruptive effect. Neither are there indications of jihadists having such intentions, nor that outside assistance is indeed being offered. Moreover, no serious incidents can be traced to jihadists. This conclusion is comparable to the one drawn at the end of 2006.

However, three comments need to be made about this conclusion and the conclusions below. The first relates to the period of validity. Developments are taking place rapidly, and not all jihadist activities, capacities and intentions will be identified. It is not known whether the absence of attacks on or via the Internet is due to a lack of intent on the part of jihadists, a lack of capacities, greater resilience in preventing or combating possible attacks, or a combination of these. The fact is that there are many vulnerabilities, of which we are now aware, and these vulnerabilities are also becoming more and more widely known. In addition, tests and incidents indicate that those vulnerabilities can be exploited. It is not easy to assess how things will develop in the future. The second comment concerns the focus on jihadists. From an NCTb perspective, the jihadist-terrorist threat is currently the most important threat to be considered. However, a great deal of the literature on the subject makes no distinction between the various parties that might carry out an attack, such as states, criminals, vandals or other individuals or terrorists. After all, the vulnerabilities outlined may be exploited by people other than jihadists. Conversely, this also applies to the level of resilience, in that the resilience to such attacks by jihadists also applies to all other potential threat sources. Lastly it is important to acknowledge that the assessment that a complex attack of a terrorist nature on or via the Internet with real socially disruptive consequences is not anticipated, is no reason to be less vigilant, since a simpler attack, whether of a terrorist nature or otherwise, can for example have

unexpected effects in vital sectors. Although such a disruption may then be smaller in scale, or shorter in duration, the malice behind it will generate greater unrest and media attention than a disruption caused by a technical malfunction or human error.

A1 Successful cyber attacks by jihadists *on the Internet* are possible on a limited scale, but are certainly improbable on a large scale

It is not really possible for a cyber attack to cause large-scale disruption or failure of the Internet, since the Internet is now too large, too diverse and the whole Internet industry is too resilient. However, there are still vulnerabilities, including those found in the standard Internet protocols. Luckily these are not easy to exploit, and attacks will not affect every part of the Internet to the same degree.

There are no indications of jihadists having sufficient knowledge to successfully exploit the vulnerabilities of the Internet for cyber attacks; neither are there indications that such intentions exist. Furthermore, no abuse of these vulnerabilities by jihadists have been observed. In addition, the question still remains as to whether the effects of an attack would justify the efforts, given the resilience described above. Therefore, as was the case at the end of 2006, a successful large-scale cyber attack on the Internet by jihadists is regarded as being improbable.

Other sources of threats (criminals and states) have more capacities for successful cyber attacks, and some may also have the intent to carry out such attacks. An investigation of their capacities and intentions, however, falls outside the scope of the study. For those sources of threats the Internet as such is no less resilient.

A2 Successful attacks of a different kind by jihadists *on the Internet* are possible on a limited scale, but are certainly improbable on a large scale

Terrorists will not be able to shut down the Internet by carrying out other attacks unless they acquire nuclear weapons which are exploded at a great height causing an electromagnetic pulse. If they were to have access to such weapons, the Internet would not be a key target.

The Internet has a number of weak points, such as cables and nodes and Internet exchanges, which could be the target of attacks. However, there is considerable redundancy within the Internet, numerous measures have been taken to limit the vulnerabilities, and the awareness regarding such vulnerabilities has increased. If the Internet were to be hit by bomb attacks or by power cuts or wilful flooding, the consequences would be relatively small-scale, would occur locally or regionally, and would be quite easy to deal with. However, the time it would take to recover from an attack would be (considerably) longer than the recovery-time necessary in the event of a cyber attack.

To what extent are examples known of jihadists focusing on the Internet? There is known to have been one plan for a possible bomb attack on the most important British telecom/Internet location. However, the question is whether that plan was actually aimed specifically at the Internet itself. It is conceivable that jihadists have infiltrated the sector. However, the sector was and is aware of this risk and is fairly insular in character. On the other hand, the Internet and telecom sector are expanding rapidly, and that insular nature may be coming under pressure.

Although terrorists are used to working with explosives, it would not be logical for jihadists to opt to attack the Internet using explosives since other targets are more attractive, and the 'costs' probably do not weigh up against the 'benefits'.
All in all, the conclusion has to be that a successful 'other type of' attack on the Internet, certainly one on a large scale, is improbable. As was the case at the time of the in-depth study, such an attack would be most conceivable in combination with (an) other attack(s), with the aim being to increase the chaos following said attack(s). The attacks in Mumbai at the end of November 2008 demonstrated that a mix of targets is (still) one of the jihadists' options.

A3 Successful cyber attacks by jihadists *via the Internet* are possible on a limited scale, but are certainly improbable on a large scale

IT systems for controlling processes in the vital sectors (often referred to as SCADA systems) are vulnerable to disruption or take-over by outside elements. Other critical online services, such as financial services, can be affected. There have been developments in this area which indicate an increase in risk factors, such as the increasing availability and quality of attack resources, the online discussion of vulnerabilities, an increase in the outsourcing of server management and data processing, and an increase in Internet use, including by the (vital) commercial sectors. Moreover, (young) hackers are becoming increasingly clever. Tests and incidents demonstrate in practice that vital sectors are still particularly vulnerable to insiders and dedicated teams of hackers who have at least advanced capacities. However, there are also developments that indicate a decreased risk. For example, there is now a greater focus on cyber security, governments and the business communities in various countries (including The Netherlands) are cooperating on increasing their awareness and therefore the resilience in this area, and there is also international cooperation in this field, In addition, the market may be able to respond in order to strengthen the technical defences.

As regards the threat, and based on the NCTb's intelligence, jihadists and their supporters cannot do much more than (incite people to) carry out simple cyber attacks such as the defacement of websites. There do not seem to be any intentions to carry out more advanced or complex cyber attacks, and the capacities appear to be limited. In the event that such intentions exist, the limited capacities can be compensated by seeking to cooperate with specialist individuals, states or (criminal) groups. However, there are no indications that this is the case.

If jihadists acquire the capacities to carry out more sophisticated cyber attacks, they may well be able to create social unrest, even if such attacks do not have such direct consequences that they deserve to be labelled as 'terrorism'. Social disruption is, however, improbable. In view of their intentions and capacities, in combination with the history of jihadist attacks, the expectation is that jihadists' preference will remain focused on carrying out classic bomb attacks and suicide attacks. They have more experience with these methods, and such attacks have a more direct and predictable effect than the digital disruption of a vital sector.

The conclusion is, therefore, that a successful jihadist-terrorist attack via the Internet, that is aimed at the vital infrastructure or crucial online services, is improbable in the short term, and is certainly not probable in the form of a large scale cyber attack. Vulnerabilities and possibilities have probably increased rather than decreased, but there are insufficient indications that jihadists are willing or able to exploit these successfully. However, simple disruptions are certainly possible, and can create social unrest.

There would appear to be a greater likelihood of an attack or cyber hijacking by parties *other* than jihadists, such as those acting on behalf of a foreign state, or criminals. An investigation into the intentions and capacities of those parties falls outside the scope of this study.

B Internet as a resource

Jihadists continue to use the Internet - just as ordinary citizens - for a variety of purposes, and they regard the Internet as a crucial jihad resource. Three media organisations, namely As-Sahab, GIMF and Al-Fajr, play an even more crucial role for the jihadist movement than at the end of 2006. The same applies to between five and ten so-called mother sites', from which jihadist publications and the jihadist message is first distributed, and which host forums on all kinds of jihadist issues that contain a range of information and views. By contrast, jihadists are distributing their publications and message more and more via numerous non-jihadist sites and applications such as YouTube and social network sites, which have become very popular since 2006. This can be regarded as a form of implanting process. Although jihadists have less control over these sites, their reach is many times greater than that of the jihadists' own sites. Since the end of 2006, two large-scale jihadist sites have disappeared, presumably within the framework of a counterterrorism operation, namely on the eve of the commemoration of the attacks in the US in September 2008 and 2009. While jihadists were not directly able to respond to the disappearance in 2008, they appeared to have learned some lessons in 2009. They have become less vulnerable with respect to the removal of their prominent sites from the Internet.
The following are the conclusions regarding the use of the Internet as a resource.

B1 Propaganda via the Internet contributes to radicalisation

Various sorts of jihadist propaganda can be found on the Internet. In particular, the three media organisations Al-Fajr, GIMF and As-Sahab have published a substantial flow of propagandist messages (audio, video and text). Propaganda via the Internet has become more professional since the end of 2006, has considerable reach, and meets with relatively limited resistance. Jihadists are trying to engage in more interaction with interested parties, in numerous ways. Jihadists also respond actively to news items from Western media for propagandist purposes, and are alert to alleged defamations of Islam, and respond in their own forums to related news items from Western media. The likelihood of, for example, defacements as a specific form of propaganda by jihadists will sooner increase than decrease, including in The Netherlands. Other tendencies which can be referred to are continued professionalisation and improvements in the quality of jihadist publications and the jihadist message, and a greater orientation towards a Western audience.
The combination of primarily large groups of young people who have access to the Internet and use it intensively in combination with the propaganda from the jihadist movement creates a breeding ground for (further) radicalisation.

B2 Internet use supports the entire radicalisation process

The insights into the influence of the Internet on radicalisation have not changed substantially. A supply is available for each phase of radicalisation. Using the Internet, a potential jihadist can go through the processes of ideology formation, ideology reinforcement and ideological indoctrination. The threat is greater from interactive sites, including social network sites or forums, than from static sites from which, for example, only documents can be downloaded. It is precisely the interactivity of jihadist Internet use that has increased, and with that, the influence of the Internet on radicalisation. As a consequence of

the increased interactivity, it is becoming more and more difficult to distinguish between propaganda, recruitment, virtual network formation and the influence of Internet use on radicalisation as a whole. The Internet influences radicalisation, but it is not yet clear to what extent the Internet is the only or the deciding factor in this process.

B3 The formation of virtual networks increases the jihadist movement's power to act

It is still likely that the formation of virtual networks can lead to the creation of an informal pool of people who are willing to become involved in the jihad, and who - in varying combinations - are able to devise violent activities with each other or individually. As a consequence, local and international elements can become more interwoven.

B4 Recruitment via the Internet primarily takes place in an interactive manner

It is unlikely that someone from The Netherlands can be recruited via the Internet directly and through one-on-one contact by recruiters from international terrorist groups. However, the interactive jihadist sites can provide an ideal recruitment location. After all those sites are visited by people who have a far-reaching interest in the jihad. It is also true that young people feel attracted to scenes of jihadist action, and use the Internet to search for a way of getting there. On the Internet, a very interactive form of recruitment has been observed which is strongly linked to interactive propaganda methods. However, due to the diversity in casuistry, no general pattern can be identified other than that recruitment takes place interactively via the Internet, and that usually the people involved have 'presented themselves' rather than being 'recruited' in the classical sense of the word.

B5 Applications for acquiring information via the Internet potentially support the carrying out of terrorist activities

Internet applications offer quite a lot of possibilities for obtaining information, and terrorists 'talk' about those possibilities or are already using them. The possibilities offered by those applications make it easier for terrorists to prepare their terrorist actions. The applications provide information in an easy and anonymous way about a certain object, location, organisation or person, and they reduce the need to carry out reconnaissance locally. The information is accessible because organisations or people are insufficiently security-conscious, and divulge too much information about themselves and their surroundings online. Nevertheless, some of the information is also available in another way, for example in the case of aerial photos obtained from commercial sources. In addition, physical reconnaissance still appears to be essential in order to be properly prepared. The expectation is that the possibilities for obtaining information will only increase in the future. Moreover, in the future the Internet will be available at even more locations than is currently the case.

B6 Fund-raising via the Internet by and for jihadists only takes place on a limited scale

Potentially there are still many possibilities for fund-raising by and for jihadists. A number of examples of these variants are known, but are still seldom used in practice. The expected increase in abuse of Internet banking and the expected shift from more public to more secretive fund-raising have failed to materialise.

B7 Training via the Internet lowers thresholds but the danger posed by physical training is greater

The expectation that the Internet can take over the role of physical training camps has now been shown to be misplaced, through the practical reality of the fact that numerous physical jihadist training camps

exist, to which, moreover, people are still travelling, or trying to do so. For budding jihadists, the Internet is more likely to be seen as a library of training material and, to a certain extent, a virtual classroom. Someone still has to be able to understand the instructions or manuals properly themselves, and then practise, apply and execute what is in them (in a disciplined fashion). In the case of certain instructions, one can definitely question their 'ease of use' and safety. Nevertheless, the training material and the sites where experiences and insights are shared are not harmless. They can be used, certainly by home-grown terrorists, and can thereby lower the threshold to the potential for carrying out attacks.

B8 Jihadists use the Internet to communicate with each other and make plans

It is very likely that jihadists still use the Internet to communicate with each other. Logically, this will largely take place in a protected manner. Strictly speaking it does not make any difference to the threat whether jihadists communicate by telephone or via the Internet. As is the case with other means of communication, intelligence bodies and the police can also intercept Internet traffic. Jihadists are aware of this and warn each other accordingly.

B9 As far as the jihadist movement is concerned, the Internet is first and foremost a crucial means of interactive communication and a resource to be used for (the preparation of) terrorist activities

Jihadists still make extensive use of the Internet as a resource. They use it in a more interactive way. That increased interactivity makes it easier to spread propaganda, set up networks and 'recruit' interested individuals, and to communicate and make plans with each other. As a result, the effect on radicalisation is also greater. In addition, the Internet fulfils a supporting role for jihadists as regards (the preparation of) terrorist activities. Besides fund-raising and communication and mutual planning, the threat is primarily the result of using the Internet for the creation of virtual networks, for the acquisition of information, and for training purposes.

C Jihadism on the Dutch Internet

C1 Number of jihadist expressions on the Dutch Internet has decreased

Jihadist expressions can still be found on the Dutch Internet but their number has decreased since 2006. This can probably be explained by the active moderation policy pursued by the administrators on the mainstream sites, the decrease in the activities of local autonomous jihadist networks in The Netherlands itself, and the increased 'security awareness' among jihadists: the realisation that they are being monitored by investigation agencies and security services in The Netherlands. In addition, since 2006, a number of jihadist websites appear to have repeatedly had technical problems and have been frequently offline.

Nevertheless, for someone who wants actually to acquire knowledge about the violent jihad, enough material can be still be found on the Dutch web. Of course, jihadist information can also be obtained from Arabic and/or English language jihad websites. The fact that various individuals in The Netherlands are still active, possibly in groups, with online propaganda related to the violent jihad, is also a negative sign. This carries with it the risk that people will continue to become (even more) radicalised.

C2 Dutch online jihadism is aimed almost entirely at spreading propaganda

As was also observed in 2006, Dutch online jihadism is aimed almost entirely at spreading propaganda. The propaganda varies considerably as regards content and style. On static websites, (translated) jihadist

literature can still be found. In addition, there are more modern, Web 2.0 based knowledge exchanges on the jihad. Since the end of 2008, a number of Dutch clips of jihadist nasheeds (Islamic non-instrumental songs) have been posted on YouTube. These jihadist songs on YouTube primarily try to stir up a feeling of anger towards the West among Muslims, and call upon Muslims to take action. In addition, these nasheeds project a romantic image of the violent jihad. No examples have been observed on the Dutch 'public' Internet of direct recruitment and/or the distribution of (Dutch) manuals on explosives and the use of weapons.

C3 The focus of Dutch jihadists on the Dutch Internet is on international aspects of the jihad

The jihadist focus on the Dutch Internet is mainly on international aspects of the jihad, namely the traditional conflict areas in Afghanistan and Pakistan, but also - and this is relatively new - in Somalia. This is in line with general findings on jihadist networks in The Netherlands.

D Overview of the most important changes

The main conclusions are no different to those stated in the original in-depth study. This is remarkable in the light of the rapid developments on the Internet and within jihadism.

As regards the Internet as a target and weapon, the most important changes are that the vulnerabilities for cyber attacks against and via the Internet have increased, and that these vulnerabilities are becoming more and more widely known. A positive sign is that the awareness of those vulnerabilities has also grown, and that countermeasures are being, or have been, taken. As a consequence of the assessment that jihadists are unable to carry out a complex attack and that there are also few indications that they intend to do so, the conclusions about (cyber) attacks against and via the Internet have remained almost identical to those established in the original in-depth study.

The conclusions about jihadist use of the Internet as a resource have also largely remained the same. However, there were some differences. In line with developments on the Internet itself, the most important change was the increased interactivity. This was evident at the end of 2006 on the 'Dutch jihadist Internet', but it is now present at international level. Such increased interactivity makes it easier to spread propaganda, set up networks and carry out 'recruitment' activities, and to communicate and make plans with each other. As a result, the effect on radicalisation is also greater, and it has become more difficult to define when, for example, propaganda turns into recruitment or network formation. The phenomenon of jihadists making improper use of neutral sites, which was already evident on the Dutch Internet at the end of 2006, is now also taking place at the international level. Besides this wider manifestation of jihadist expressions, there is the even greater role of three so-called jihadist media organisations, and between five and ten so-called mother sites. The increase in the abuse of Internet banking which was expected at the end of 2006, and the expected shift from more public to more secretive fund-raising via the Internet, have failed to materialise. It is now also clear that the expectation - expressed at that time - that the Internet could take over the role of physical training camps has turned out to be false. It is generally agreed that the Internet influences radicalisation, but it is not yet clear to what extent the Internet is the only or the deciding factor. The nature of this phenomenon makes it difficult to carry out research with regard to this issue.

The most important change as regards jihadism on the Dutch Internet is the decline in jihadist expressions since 2006. These conclusions are also in line with those drawn at the end of 2006.

1 Introduction

1.1 Grounds

In January 2007, the in-depth study entitled *Jihadis and the Internet* by the NCTb was published, hereafter to be referred to as 'the in-depth study'. The study was intended to provide an insight into the use of the Internet by jihadists. An insight into Internet use by jihadists was (and is) considered to be crucially important for the drawing up and evaluation of counterterrorism policy. The study included an assessment of the use of the Internet as a weapon for an attack on, for example, the vital infrastructure in The Netherlands, and the use of the Internet as a resource, for example, for propaganda and recruitment. An assessment was also carried out of the vulnerability of the Internet itself to terrorism: Internet as a target. An assessment of the threat was drawn up for all the different facets. In effect, the research period of the study extended from the time the Internet was created until mid 2006. Only some of the literature from the second half of 2006 was used when the study was being written. In that period an expert meeting was also held to test a number of hypotheses and provisional conclusions. A substantial contribution by the AIVD was also included in the texts. The final result of the study has led to a variety of policy initiatives.
As it may now clearly be assumed, ICT-related developments take place rapidly, and jihadism too is developing and will continue to do so. That is why it became necessary to review the original assessment of the threat in the form of this '2009 update'. The accent is on changes since the publication of the in-depth study at the beginning of 2007. The aim is, nevertheless, to produce a publication that may be read in its own right.

1.2 Aim, research subjects and scope

The primary aim of the study is to acquire a basic insight into changes in the use of the Internet by jihadists, and the threat which this entails, with respect to an assessment of possible measures to avert the threat. The secondary goal is to identify issues which require further analysis and/or research.

The research subjects which are derived from this goal are:

- To what extent have significant changes occurred since the end of 2006 in the way in which jihadists use the Internet as a target, weapon and resource, and what are these changes?
- To what extent have significant changes occurred in the way in which the use of the Internet as a resource by jihadists influences radicalisation, and what are those changes?
- To what extent have significant changes occurred in the way in which jihadism has manifested itself on the Dutch Internet since the end of 2006?
- To what extent do the identified changes in the use of the Internet by jihadists result in changes in the threat by jihadists against The Netherlands or Dutch interests?

The scope of the new study is the same as that of the in-depth study. This update therefore focuses primarily on jihadist terrorism and jihadist radicalisation, also referred to in the past as Islamic terrorism and Islamic radicalisation. In The Netherlands, and in Europe as well, the greatest threat comes precisely from this category of terrorists. Unless indicated otherwise, for the sake of convenience we use the term jihadism or jihadists (see paragraph 1.3). For a definition of the terms, please refer to the List of Terms. No attention is paid to the criminal use of the Internet (cybercrime, such as phishing). Neither is there any detailed focus on the use of the Internet for economic and industrial espionage, for political-military purposes (cyberwar) and by activists. An exception to this is a case in Estonia. This is often referred to as an example of how a cyber attack can seriously disrupt a country's Internet infrastructure. This case is also often referred to as an example of cyberterrorism, a term which the NCTb prefers not to use, or cyberwar.

The report does not deal with any ICT-related issues such as jihadist use of satellite telephones and mobile telephones, or the use of satellite transmitters.

When the results of the study were set out, and the conclusions were drawn, the scope referred to turned out to be perfectly usable for the 'Internet as a resource' section (Chapter 3). However, it proved more difficult to apply that scope to the 'Internet as a target and weapon' section. A great deal of the literature on the subject makes no distinction between the parties that might carry out an attack, such as states, criminals, vandals or other terrorists. After all, the outlined vulnerabilities can be used by others than jihadists, and the capacity to resist attacks is not limited to attacks by jihadists alone. Only the assessment of the intent and capacities of jihadists falls entirely within the scope. In accordance with the scope of the update, the conclusions focus specifically on the use of the Internet as a target and weapon by jihadists.

Another aspect of the scope, namely terrorist use, was sometimes difficult to apply. Every cyber attack can be characterised as serious. However, in order to speak in terms of a terrorist attack, which is the NCTb's specific focus, based on the objective, such an attack has to fit the definition of terrorism (see List of Terms). The focus then is on the specific intent: bringing about social changes, instilling fear in the population or influencing political decision-making, and the consequences: violence aimed at people, or actions aimed at causing socially-disruptive material damage.

1.3 Justification of the method of working

The decision was taken to opt for a general but broad orientation which could then serve as a basis for follow-up studies. Once again, four research methods were chosen, namely:

1) interviews,
2) a literature study,
3) an investigation of use on a number of Dutch websites and forums, and
4) an expert meeting.

Interviews were held with several experts from organisations which are involved in the phenomenon of Internet or vital sectors in The Netherlands. The interviews and background discussions were processed anonymously. The authors also took part in congresses and used the relevant findings.

The literature study focused on scientific literature, and open and closed sources. The scientific literature and open sources were used for a detailed examination of the use of the Internet by terrorist groups and jihadists. The primary focus is on foreign literature and sources from an international perspective. Literature tailored specifically to the Dutch situation is relatively scarce. That is no real surprise, given that the Internet and jihadism are, by nature, international phenomena. Dutch and foreign intelligence and investigation agencies also focus on this phenomenon and have issued publications in both freely available and classified documents. This information has also been studied and, in so far as the classification allows, has been included in this study.

On 11 June 2009, the NCTb organised an expert meeting within the framework of this study (almost exactly three years after the previous one), which was again attended by researchers and representatives from government services and the business community who are involved in the terrorism, telecom and Internet

sectors. Once again the focus was on the issue of 'Internet as a target and weapon'. The outcomes of that expert meeting are included in Chapter 2.

The research on behalf of Chapter 4 involved an analysis of the 'public part' of the Dutch Internet which can be searched using search engines such as Google. This involved the use of search terms, in some cases in Arabic, which can be linked to jihadism. Wherever jihadist content was found on a website, it often transpired that these referred to hyperlinks or references to other jihadist web locations. The findings in Chapter 4 are also based on regular Internet monitoring activities, public sources and interviews.
The period to which this study relates ends in December 2009. Later developments have not been included.

In this publication, the term jihadism has the following meanings:

- Jihadism is a movement within political Islam whose aim, based on a specific interpretation of the Salafist teachings and the body of thoughts of Sayyid Qutb, is to achieve the global dominance of Islam and the re-establishment of the Islamic State (Caliphate) by means of an armed struggle (jihad).

See Annex 1 for a more detailed description.

1.4 Clarification of the structure

This update largely follows the structure of the original in-depth study. Chapter 2 analyses the Internet as a target and weapon and Chapter 3 analyses the Internet as a resource. Chapter 4 examines the situation on Dutch Internet. The study ends with a documentation list, list of terms and an annex.

2 The Internet as a target and weapon

2.1 Introduction

This chapter describes to what extent jihadists regard the Internet as a target or use it as a weapon. In the case of the 'Internet as a target' the focus is on terrorist activity aimed at (the infrastructure of) the Internet itself, while in the case of the 'Internet as a weapon' the focus is on terrorist activity via the Internet aimed at physical or online targets such as the vital infrastructure, or online services such as Internet banking, key search engines, news sites and Internet stores. This description does not cover state terror or Internet attacks carried out by or on behalf of states. This is also important to prevent confusion with terms such as cyberwar or hacktivism in all kinds of guises.

A number of definitions apply to the term cyberterrorism.[1] The NCTb deliberately does not use this term. The term cyberterrorism is prone to exaggeration. In addition, an excessive term may be used in the form of 'electronic Pearl Harbor', 'digital Waterloo', or 'cybergeddon'.[2] However, the most important argument for not using the term cyberterrorism is based on the question of whether a certain modus operandi (which using the Internet actually is) deserves a special definition.
The broad term of cyberterrorism is therefore not used in this update. However, for practical reasons it has been decided to use a compact term for a terrorist attack on the Internet itself or on the vital infrastructure or critical online services for which the Internet is used as a vehicle. As was the case in the in-depth study, this term is 'cyber attack'.

2.2 Background information

The focus of this paragraph is on certain terms and developments which feature in the discussion of the Internet as a target (2.3), as a weapon (2.4) and as a resource (chapter 3). It ends with a general examination of indicators of interest among jihadists for cyber attacks.

2.2.1 New forms of Internet use/data on Internet use

In recent times there has been a rapid growth in mobile Internet in particular. These days Internet access is even possible in aircraft.[3] Internetting via laptops, netbooks and mobile telephones, without being dependent on 'old fashioned' hot spots, has become a feature of everyday life.[4] As a result, more and more information, some of which is sensitive information, is being exchanged - often wirelessly - between people and companies. Bandwidth is also increasing, and that means the time is ripe for another important change, namely the shifting of computer applications from laptops or desktop computers to the Internet. In effect, this is turning the Internet into a new operating system, with email, word processing, photo and video editing and customer relationship management now available online. This is referred to as *cloud computing*, and offers a wide range of benefits. For example, users do not have to install the software themselves and their own data is available anywhere and at any time. However, the data in question is no longer on their hard disk but in the *cloud*. This means that people may be able to exploit the vulnerabilities of an online service via the Internet. The terms and conditions of use can be changed unilaterally which can be a problem, particularly for businesses. The fact that more people are online, are online more often, work more often via a wireless connection and use new applications, offers - in principle - more options to the terrorists as well, as regards phishing, information gathering, social engineering, propaganda and cyber attacks.

1 For a Dutch definition of cyberterrorism see: Luiijf 2008.
2 Stohl 2007.
3 Fox News 2008.
4 The following passage is based largely on: GOVCERT 2009.

2.2.2 Mass overload attacks and targeted hacking: variants

Mass overload attacks and targeted hacking are still the two methods used to create an actual terrorist effect via the Internet. Mass overload attacks, generally referred to as *Distributed Denial of Service* attacks (DDoS attacks), are primarily suitable for attempts to knock out (parts of) the Internet. Targeted hacking is a method to launch attacks on, for example, the vital infrastructure. DDoS attacks tend to be used to affect the availability of Internet services (with the consequence being a failure of Internet banking), while targeted hacking is used to affect reliability (with the consequence being compromised data and/or false transactions). However, DDoS and virus attacks can also be used in the vital sectors due to their disruptive effect. However, this will not mean that a controlled take-over of such a sector will occur.[5]

More and more effective botnets which are also becoming increasingly inexpensive

The number of DDoS attacks is still increasing, and has reached 6000 per day worldwide. A DDoS attack is usually carried out using a botnet. Put briefly, a botnet is a network of hacked computers which can itself expand in size.[6] Botnets are subject to a technological race. One trend is for experts or technologists to be hired in to make independent botnets. The market is large, but the profit margins are becoming smaller. Among others, GOVCERT.NL has reported on the developments relating to botnets and malware. The number of different variants of malware is rapidly increasing.[7]

Techniques are also being used to give botnets a different structure, without any traceable owner. Such botnets make better use of the possibilities provided by the Internet, and make it more difficult to prevent attacks. This does not increase the chance of a cyber attack, but it does increase the effectiveness of such an attack.[8] Other techniques make it more difficult to prevent or trace cyber attacks because they affect Internet memory, as it were. Such techniques were used by a worm like Confickr, which was widely reported in 2009 and about which there was a great deal of uncertainty.[9] Despite all these techniques and possibilities, most incidents involving botnets, other than those related to cybercrime, do not amount to much more than vandalism. [10]

2.2.2.1 Level of cyber attacks

It is and continues to be important to make a distinction based on the feasibility and effects of cyber attacks.[11] Some cyber attacks, defacements and small-scale DDoS attacks are largely automated and can be carried out inexpensively, although they also have little effect as regards both duration and seriousness. They fall within the category of 'simple attacks, '*script kiddie* attacks' or 'hacktivism'. The same applies to defacements as a result of the film *Fitna*[12], which focused on simple, old vulnerabilities in server software. Although there was some targeting (only servers within the NL domain were affected) this was indiscriminate and automated. The effects were small and were easy to rectify. Simple attacks can also generate a certain amount of publicity, as was the case in The Netherlands at the time of the defacements relating to *Fitna* and

5 Interviews.
6 Botnets are not only used for DDoS but also and primarily to send spam.
7 GOVCERT 2008 and CRS 2008, p.5.
8 Expert meeting 2009.
9 Expert meeting 2009: the focus was on, for example, peer-to-peer botnets and the fastflux technique.
10 Expert meeting 2009.
11 Based largely on Lachow, p.443-445.
12 Pers 2008 and Parool 2008.

in the US at the time of the simple DDoS attacks on South Korea and the US in July 2009. In the case of the latter incident, the term *cyber warfare* was used, and that led an American member of congress to call for 'a show of force or strength' against the presumed perpetrator (North Korea).[13] Such developments also result in cases where the issue of electronic warfare becomes - often wrongly - the subject of a discussion of terrorism on and via the Internet. This does not mean that the issue of electronic warfare and the role of third countries is unimportant, as the capacity of certain countries to wage such warfare may be substantial.

A higher level of cyber attacks are advanced attacks for which programming skills are required, or with regard to which another party's programmes have to be changed, meaning that the perpetrators have to have considerable knowledge of networks and operating systems and be able to exploit relatively unknown vulnerabilities or find new ones.[14] These are serious attacks which will, however, be aimed at one kind of network which is used in a particular vital or government sector. This requires, at least, knowledge of the target's characteristics. Such attacks can have serious consequences but are not necessarily effective (in the long term), let alone socially disruptive. This kind of attack can usually be carried out quite inexpensively. In fact this type of attack in combination with the right publicity can, in particular, achieve a strong propagandist effect and social unrest.

Lastly, there are complex attacks which are aimed specifically, from beginning to end, at for example one vital sector. Such attacks are characterised by in-depth preliminary research into the system to be attacked, the possession or hiring in of the right knowledge and skills in the field of programming and *social engineering*, the availability of a team, equipment and very probably a test environment in which to practise and to predict effects, and possibly chain effects as well. Such a setting requires time, discipline and funding. Lachow refers to an example by which such a complex cyber attack could, for example, be aimed at a large logistical operation, such as the deployment of troops (involving a combination of logistical planning, communication and transport).

As demonstrated by the above descriptions, there is a major difference between what is needed for a simple or short-term cyber attack and a long-term, socially disruptive attack. Certainly, more and more hacked process control programmes are available on the Internet, as well as related official handbooks and cheap industrial hardware. This means it has become possible for parties with malicious intentions to set up a test environment. The focus on ICT vulnerabilities in vital sectors is also said to have increased strongly since 2005. In view of the increased attention paid to this issue in a general sense, a third category cyber attack can certainly not be ruled out, although only a limited number of people are actually capable or have the attention of carrying out such an attack. The issue of whether such an attack by jihadists should be expected is dealt with from 2.2.3 onwards.

2.2.3 Developments relating to cyber attacks by jihadists

On 12 February 2009 the *Director of National Intelligence* stated, before an American Senate Committee that, among others, Al Qaeda had indicated that it wished to carry out cyber attacks on the US.[15] FBI assistant-

13 Washington Times 2009.
14 Zero day exploits can also be purchased on the 'black market', see Council of Europe 2007, p.26.
15 US Senate Select Committee 2009.

Director Henry is reported to have said that terrorist groups are working on a virtual 9/11.[16] Mark Oram, head of the *Threat and Information Security knowledge department of the Center for the Protection of National Infrastructure* (CPNI) warned about cyber espionage, but believes that there is only a small chance of a terrorist cyber attack due to their limited capacities and the difficulties associated with understanding vulnerabilities in the infrastructure.[17] By contrast, Lord West of Spithead (*Home Office*, UK) stated that the greatest threat comes from hackers who are supported/sponsored by terrorists who, for example, try to break into the electricity network.[18]

Opinions differ regarding the actual threat. Some people place a considerable emphasis on the level of *threat*, while others pay too little attention to the degree to which vital sectors are linked with the Internet and the fact that *vulnerabilities* exist.

With a view to estimating the threat of a jihadist cyber attack, the paragraphs below examine the following questions.[19] Have attacks taken place? Are jihadists investing in cyber attacks? Are they perhaps hiring in or purchasing knowledge? Are any (significant) statements being made on the matter, and do the intentions appear to be serious? Are jihadists interested in or experienced with hacking? Are they experienced with/competent in the use of computers and the Internet? These questions are discussed in the following general paragraphs and grouped under the key concepts of intentions and capacities. In some cases it is, however, difficult to make a strict differentiation between these two concepts.

2.2.3.1 Intentions

General intentions and statements: changeable in nature and fairly vague

The intentions of jihadists as regards attacks on the Internet were analysed in the in-depth study. In a general sense there was evidence of intent, at a strategic level, to affect the economy. The economic crisis at the end of 2008 was also a source of inspiration to jihadists and their supporters, as demonstrated in a video interview with Bin Laden and discussions in jihadist web forums.[20] The Internet is essential for the government, for (vital) companies and therefore for the economy. Despite assertions on this regularly being made or being referred to, the authors have not been able to find any instances of Al Qaeda leaders making direct statements regarding attacks on the Internet. The closest reference to actual Internet-related intentions came from the second in command at Al Qaeda, Al-Zawahiri, in his *Knights Under the Prophet's Banner* dating from 2002.[21] This document was not specifically assessed at the time of the in-depth study. In the document he talks about goals (such as banishing Western influences from the Islamic world), enemies (the West) and criteria for target selection/resources (causing large number of victims/martyrdom). This classification groups 'international networks for information and communication technology' in a general sense under 'the enemy' and places them at the same level as, for example, the international media. This does not mean, however, that the Internet is a target; it is rather seen as a part of the concept of 'the enemy'.

16 AFP 2009.
17 ZDNet 2008.
18 Times 2008.
19 Partially taken from Denning 2007, p.5-p.15.
20 Weimann 2009.
21 Mansfield 2006.

Another statement, which was likewise not assessed in the in-depth study, can be attributed to Bin Laden. After '9/11' he is said to have told the editor of the Ausaf newspaper that many Muslim scientists supported him and would use their knowledge "in chemistry, biology and [sic] ranging from computers to electronics against the infidels".[22] This statement is insufficiently concrete to serve as a basis for a strategy, and appears to be intended to have primarily a propagandist effect. This would appear to be backed up by the fact that, since 2001, no successful chemical, biological or cyber attacks have taken place. However, chemical knowledge and knowledge of electronics have been used to produce IEDs, general computer knowledge has been deployed for propaganda purposes, and lorries carrying chlorine were used in attacks in Iraq for a short period of time.

Lastly, there is the similarly older theory that describes Al Qaeda's 'seven phases of conflict'. The fourth phase (*The healing stage and gathering strength for change*, from 2010-2013) is also supposed to include cyber attacks against the economy in the US.[23] A previous phase (from 2003-2007) also covered preparations for an electronic jihad via the Internet. It is unclear whether this electronic jihad refers only to propaganda-related activities or cyber attacks as well. In any event, according to the theory of the seven phases of conflict, the phase of, among other things, cyber attacks is to start in 2010.

All in all these are dated statements which are not very specific, and with regard to which it is not yet clear whether they should be taken very seriously. During the expert meeting it was indicated that there is no knowledge of any intentions on the part of jihadists to carry out a serious cyber attack.

The legitimacy of cyber attacks also featured in the in-depth study, with references being made to two relevant fatwas. Since the in-depth study, a new discussion has taken place in 2009 on the Internet, in this case in the Ansar Al-Haqq forum, regarding the question of whether cyber attacks are permitted. This discussion was a result of a critical piece in a Tunisian newspaper about the legitimacy of *cyber jihad*. Various forum members were convinced that *cyber jihad* is permitted. One participant posted the text 'the Prophet recommended that we combat miscreants through all means... [and] fight jihad through all means.' This statement was greeted with some enthusiasm.[24] There is no knowledge of any other discussions of the legitimacy of cyber attacks. This may mean that the legitimacy is not open to discussion, or that the issue is not really relevant.

Scientific opinions regarding jihadist intentions are diverse. Some believe that jihadists do not regard a cyber attack to be sufficiently interesting (and that this is unlikely to change) or that they have (and will continue to have) insufficient capacities to carry out such an attack.[25] Others think that terrorists will continue to be interested but that it is difficult to see this interest in isolation from other options, and that the combination of a cyber attack and a physical attack may be a more attractive option.[26] Something

22 Denning 2007, p.12.
23 Spiegel 2005 and Denning 2007, p.13, referring to al-Zarqawi: al-Qaeda's Second Generation by the Jordanian reporter Fouad Hussein, on the basis of interviews with Al-Zarqawi and various leaders within the Al Qaeda network.
24 SITE 2009a.
25 Stohl 2007.
26 Lachow 2009.

that might diminish their intentions as regards a cyber attack is the chance that a cyber attack will lead to a (further) increase in, on the one hand, security measures in vital and government sectors and, on the other hand, in monitoring, control and regulation by authorities of the Internet and Internet use.[27] Such an action would also end up restricting the jihadists' possibilities to carry out propaganda activities, which is, after all, their core activity on the Internet.

All in all, on the basis of general intentions, there are few indications that cyber attacks will develop rapidly into an important method for a jihadist attack.

Investments in capacities are barely perceptible or effective
'Investments in capacities' is an aspect of intentions which is more difficult to describe. If such investments are taking place, they are imperceptible. For example, people can attend formal ICT training courses which are needed to acquire a level of expertise which is needed in order to carry out complex cyber attacks. On the other hand this does not mean that people who complete such courses actually intend to carry out attacks. For example, the various doctors who were involved in the bomb plot in the United Kingdom in 2007 did not use their medical skills to carry out the attacks.

There are a few (older) examples of people from the field of ICT who are associated with terrorist groups and who are reported to have been active in the US, particularly in the field of fund-raising, recruitment or facilitating.[28] No newer examples are known, let alone examples of knowledge actually being acquired with cyber attacks in mind.

In addition to obtaining knowledge via formal ICT training courses, knowledge can also be increased by researching the possibilities, by setting up training facilities and by distributing knowledge. Since the in-depth study, not much meaningful information has become available. As far as is known, no training facilities have been found, despite operations in Iraq and Afghanistan, and only a small number of 'supporters' on jihadist forums seem to be interested in researching the possibilities (see below). However, the latter says relatively little about the intentions of actual jihadist groups.

There is, however, clear evidence of knowledge being combined and distributed. At the end of 2006, just before the in-depth study was published, the Al-Fajr Information Center (see paragraph 3.2.1) presented the first copy of 'The Technical Mujahid Magazine'. This article was directed at computer and Internet security, and also examined the use of GPS. The concept of *Jihad in the information sector* is regarded as an important tool in fighting the 'crusaders'. The article is very general in nature. It advocates participation in the form of sharing of information, ideas etc.[29] The Al-Fajr Center is divided into various brigades, including the Hacking Brigade (for the hacking of websites, DDoS attacks and identification of vulnerable websites) and the *Cyber Security Brigade* on behalf of the security of jihadist websites. Each group has its own message boards to which only members of the brigade in question have access, and each brigade has leaders who coordinate matters with *'the jihadist leadership'*.[30]

27 ITAC 2006.
28 Denning 2007.
29 SITE 2006a.
30 Katz & Devon 2007a.

During the course of 2007, hacking handbooks were found on southeast Asian websites which were originally from Arabic websites. However the plans were limited to hacktivism: the forum members in southeast Asia (who claimed to be students from Indonesia and Malaysia) encouraged each other to attack websites that propagated liberal Islamic views.[31]

An extensive (1,000 page long) hacking and cyber security compendium was posted in an Arabic jihadist forum.[32] Besides containing a basic explanation of how the Internet, networks and servers operate, it also focused a particularly large amount of attention on website security and hacking via, for example, *SQL injection*, which means finding vulnerabilities in servers, websites and web forums, and DDoS attacks. The explanation, in Arabic, is detailed and is thought to have attracted considerable attention in the forum.

The above-mentioned knowledge-oriented activities may constitute an investment in the development of an ideology and strategy for cyber attacks by jihadist hackers, but do not constitute a direct reason for concern.

2.2.3.2 Capacities

Experience with the use of computers and the Internet is present in abundance
There is no doubt that jihadists and their followers have general experience with the use of computers and the Internet. Jihadists use the Internet in abundance for propaganda purposes, for example. The in-depth study and this update as well include many examples (see Chapter 3). However, this says nothing about capacities for carrying out a cyber attack. However, it may provide a basis for generating enthusiasm for such attacks or for recruitment.

Experience with cyber attacks and hacking continues to be limited
The in-depth study discusses a number of examples of hacking experience and refers to Irhabi007, a well-known jihadist hacker who was arrested in the United Kingdom. The reputation that Irhabi007 built up among jihadists in the field of computer skills is an indication of the modest state of computer skills among jihadists in general. The work of Irhabi007 consisted largely of the relatively simple 'hijacking' of web space, the setting up of websites for the publication of jihadist material, and the hacking of websites with a view to carrying out simple DDoS attacks. He used (and recommended) standard tool kits[33] and did not constitute a threat to the security of the Internet or services which are (partly) dependent on the Internet. He may well have inspired others. The fact that, since his arrest in 2005, there have not been any successful cyber attacks which could be traced to jihadists, may say something about his actual knowledge and the effect of this knowledge on others in the short term.

During the period since the in-depth study, there have, otherwise, been few new indications that jihadists are developing more skills or are developing these more rapidly. The main references found in jihadist forums are to (hacked) software for the security of computers and data. In the forum of an Arabic, jihadist website, one forum member was looking for an instruction film showing how to hack servers. Another forum member gave the user a link to the international hacking website *milw0rm*. This is a site used by well-intentioned hackers to publish their methods. Usually these leaks in software are only published after

31 Agence 2009.
32 SITE 2007a.
33 Lachow 2009, p. 448-449.

producers have had the opportunity to rectify the vulnerabilities, although they sometimes appear before that point as well.[34] The site may therefore contain usable information about so called exploits. Milw0rm is a website for experts. The fact that the website is well known to certain jihadists is in itself not that unusual. The question is whether those who are aware of the site also intend to carry out a disruptive cyber attack. The goal of server hacking is most probably to be able to host (propaganda) material, or to acquire information. The in-depth study includes a number of (older) examples.

In a general sense, however, the skills of young ICT specialists, and therefore of potential hackers, is continuing to increase at a considerable rate.[35] In addition, young people grow up with ICT and sometimes discover unexpected possibilities, outside the customary methods of, for example, fraud. From a demographic point of view, the expectation is that the above also applies to people who are sensitive to jihadist propaganda. Via them, knowledge could also end up in the hands of terrorist organisations. Jihadists who want to fight but who do not (physically) have the opportunity to do so may see the 'cyber jihad' as an interesting alternative. For the time being, however, there are few indications that interest or experience have substantially increased since the in-depth study.

There is no knowledge of any serious cyber attacks

The categories of 'advanced' and 'complex' cyber attacks can include different types of attack of varying severity. A failed attack directed at a drinking water facility probably says more than a successful one aimed at a government website, while a simple attack says less than a multiple one. Neither during the research for the in-depth study, nor during the ensuing period did a jihadist-terrorist cyber attack take place, in any shape or form. However, defacements from the category of 'simple cyber attack' did take place (see 3.3.2.2).

Hiring in capacities continues to be a possibility, but there are no indications

As regards knowledge, the learning curve required to go from an attack from the first two categories to an attack from the third category is exponential (see 2.2.2.1). That exponential curve can be bridged by hiring knowledge in. The question is, however, whether the hiring in of knowledge would be sufficient, since staff probably have to be hired in to do the work as well. One of the conclusions in the in-depth study was that no-one really knows whether the average hacker actually wants to contribute to terrorist activities. Seen from the points of view of, for example, personality and group culture, this is improbable. In addition, it can also be claimed that there is a risk for terrorist organisations of hackers boasting about what they have done on certain websites, which would increase the chance of discovery.[36]

At the time of writing this update, however, there is a worldwide economic crisis. This is also affecting the ICT sector. There will now be few highly trained ICT specialists who are willing to be hired in for dubious activities, certainly when these involve terrorism. It is conceivable, however, that such specialists include people who are motivated, by a combination of lack of money and ill-will towards their ex-employer and/or society, to attempt to get back at their 'enemies' with the help of jihadists. Specialists may also be forced to cooperate. Combined with the fact that most serious ICT incidents are caused by insiders, there is every reason to be cautious as regards cooperation with individual specialists (see 2.4.2).

34 Techworld 2009.
35 Background interview.
36 Lachow 2009, p. 451.

Criminal knowledge could also be hired in. However, this will lead to a risk of early detection, for example because the criminal group has been infiltrated. There is also the question of whether criminal groups want to cooperate with such an operation. Although it may enhance their reputation[37] and although they may have the capacities to hijack a vital infrastructure via the Internet, criminals are generally not that willing to make sacrifices. Although there are no guarantees of success, the investigative capacity deployed after a successful terrorist cyber attack will be considerable. Despite all the ICT skills that criminal groups have, the risk of detection is always present. For example, professional botnets and cybercrime activities do get dismantled. The police in Mumbai (India) are also reported to have traced the IP addresses of those involved in preparing the attacks there at the end of 2008 and to link them to individuals.[38] What successful cyber criminal is going to risk his career in order to help terrorists?

The same argumentation can be applied to state support for terrorists. Even in the case of small-scale incidents like short-term DDoS attacks, suspicion often falls on states, as in the case of Estonia in April 2007 and the attacks in July 2009 on the websites of organisations in South Korea and the US. As far as is now known , there was no state involvement in either case.

2.2.4 *Conclusion as regards backgrounds*

It still applies that a cyber attack fits in particularly with the general strategy of Al Qaeda, given that such attack can result in substantial economic damage. However, no specific statements have been made. Neither do jihadists appear to have any intentions of carrying out a serious, complex cyber attack.

Although the general computer knowledge of jihadists and their supporters is considerable, such knowledge does not generate sufficient capacities for a serious cyber attack. Neither has any information come to light that indicates that jihadists are hiring in external knowledge or skills. Jihadists themselves distribute knowledge about hacking, with the focus up to now appearing to have been on cyber security.
Generally speaking, the number of DDoS attacks and the use of hacking and botnets for cybercrime is on the increase. The threshold for attacks is lower, while the relevant knowledge has increased. Although there is a degree of interest in cyber attacks among jihadists and although actions have been announced, these have not had any noticeable effect. If jihadists do carry out DDoS attacks, these are probably attacks classed in the simple category, although an attack from the advanced category cannot be ruled out.

A key fact continues to be that, since the in-depth study, no (new) serious cyber attacks have been known to have been perpetrated by jihadists, despite the fact that they have indeed frequently carried out or prepared other types of attack. Neither has any information come to light that indicates that jihadists are hiring in external knowledge or skills, although the chance of this occurring cannot be entirely ruled out.

Another striking aspect is the mix of threats and vulnerabilities. Concepts like cyberwar and hacktivism, for example in the form of defacements, are often confused with terrorism. Hacktivism does not appear to be a step up to terrorism, primarily because of the considerably more complex nature of a serious cyber attack. Above all, the fear generated by the confusion between threat and vulnerabilities serves the terrorists' goal.

37 Lachow 2009, p. 452.
38 United News of India 2009.

There does not appear to be any reason to be fearful, but neither should we rest on our laurels. There is indeed a reason to be vigilant, to eliminate vulnerabilities and to continue to prepare for cyber attacks. The fact that jihadists do not appear to be focusing on this modus operandi (to any great degree) does not eliminate the possibility that others (cyber criminals and states) will do so. It is important to increase resilience to all sources of threats.

2.3 The internet as a target

2.3.1 *Clarification*

Our society is becoming more and more dependent on the Internet. This increased dependence is a vulnerability which might give jihadists the idea of choosing the Internet itself as a target. Just as in the in-depth study, we describe here four different types of attacks on the Internet: a cyber attack via the Internet, or a physical, electromagnetic or indirect attack, aimed at (core) nodes, core functionalities, junctions, the electricity supply, cooling facilities or equipment to calibrate the internal clock (due to, for example, disruption of the GPS signal) as a result of which (the infrastructure of) the Internet is unable to function (optimally).[39]

2.3.2 *Possibilities for cyber attacks, vulnerabilities and resilience*

One of the most important conclusions of the in-depth study was that the Internet has now become so robust that it is in fact not feasible to paralyse it completely. This update assesses whether that conclusion is still applicable.

2.3.2.1 *Cyber attack on root servers on 6 February 2007 dealt with effectively*

Shortly after the publication of the in-depth study, a large-scale cyber attack took place over a period of seven hours on the thirteen DNS root servers which fulfil an essential role in the Internet's 'address book'. There is not a single indication that terrorists were behind this attack. A very cynical but possible explanation for the attack is that it was a publicity stunt to highlight the quality of a botnet available for hire.[40]

This attack on 6 February 2007 was the largest attack since 2002, when some of the most important root servers were brought down during an attack. Depending on where the measurements are taken, the effects of a disruption or an attack like the one dating from February 2007 can differ greatly. According to media coverage, six root servers were affected, of which two seriously. According to experts, the technique used in the attack of 6 February 2007 was basically quite simple. The strengthening effect of the attack was worrying. A comparison can be made with a successful chain letter action whereby the letters are not only sent but also answered. However, the fact that root servers use different techniques (anycast, and others) means the level of resilience is considerable.[41]

39 See In-depth study.
40 ICANN 2007, p.5.
41 These two were said to be the only servers which did not use a relatively new technique referred to as Anycast. This is a routing scheme for networks whereby data packages for a certain address can be sent to physically different locations. In this way, a large quantity of traffic can be spread over various servers at different geographical locations. An additional advantage is that the services are not jeopardised if a server fails due, for example, to an earthquake. The Anycast technology means it has become more difficult to paralyse root servers, although it should be noted that this has led to a shifting of the problems to other layers of the Internet. However, the root servers which use other techniques do not contribute to this shifting effect. In the event of serious problems, traffic can continue by users entering IP addresses into the browser themselves. The DNS server is then circumvented. In practice this is not a serious option for the average user.
Sources: Tweakers 2007 and expert meeting in 2009.

As regards resilience to cyber attacks, it is also important to remember that the Internet is a network of networks. The diversity this implies is increasing all the time, and not only with regard to root servers, meaning that attacks can never affect all the sections of the Internet to the same degree.[42] On the other hand, Verisign, the administrator of the *.com* sites, warns that criminal networks are becoming more and more professional, that they thereby constitute a threat to the infrastructure of the Internet, and that attacks to date could be dealt with by increasing the bandwidth, but that there will come a time that such a response no longer works.[43]

2.3.2.2 *Cyber attack on Estonia successful due to limited infrastructure*

In May 2007 a cyber attack was launched against Estonia. This attack was aimed primarily at local level and was a response to the relocation of a war monument. Russia was suspected of being behind the attack and people started talking about 'cyberwar' which, according to the participants at the expert meeting, hyped the incident. Estonia is a country with a strong Internet orientation, but at the time it did not have the accompanying infrastructure with redundancy and sufficient data transport capacity.[44] That is why the effects of the botnets used was so considerable and long-term. A comparable attack would probably have little effect in The Netherlands. It is, however, possible to render government websites inaccessible for shorter periods of time.

2.3.2.3 *Internet infrastructure vulnerable*

The infrastructure of the Internet appears to be vulnerable. GOVCERT.NL talks of 'cracks in the foundations of the Internet'.[45] A number of communication protocols (such as TCP, DNS and BGP: the 'languages' which computers and networks use)[46] appear to contain vulnerabilities which mean that the foundations of the Internet do not link up with the requirements imposed by modern usage. According to GOVCERT.NL, Internet maintenance or repairs are urgently needed but are not easy to carry out due to the size of the Internet and the fragmented responsibilities.[47] The vulnerability of DNS can be tackled by introducing DNSSEC (secure DNS).[48]

2.3.3 *Intention of jihadists as regards cyber attacks*

The in-depth study described the intentions of jihadists and the advantages and disadvantages for them of attacking the Internet. These appear to be still valid. A cyber attack aimed at the infrastructure of the Internet fits the general strategy of Al Qaeda. A cyber attack has the potential to cause substantial economic

42 Expert meeting 2009.
43 Automatiseringsgids 2007.
44 Expert meeting 2009.
45 GOVCERT 2009.
46 All computers have a unique IP address. DNS links names to IP addresses. This means you can type in www.nctb.nl and DNS will then translate this into the IP address. BGP can be used to determine the route of networks which you travel from computer A to computer B. TCP provides the actual link between two computers (source GOVCERT.NL).
47 GOVCERT 2009.
48 Automatiseringsgids 2009a.

damage. A cyber attack is a useful weapon in an asymmetric conflict. The combination of the unknown quantity of cyberspace with terrorism increases the psychological fear of such an attack. In addition, the organisation itself will not suffer direct casualties as in the case of a suicide attack. Computers, Internet access and hacking tools are much more readily available than weapons or explosives. The terrorists can also determine the time, the location and the circumstances themselves, and operate remotely. The (relatively) anonymous character of an attack makes it more difficult to find and apprehend the perpetrator. Moreover, a cyber attack has a lower threshold than an ordinary attack, and one that is certainly lower than a suicide attack.

On the other hand, it is difficult to predict the actual amount of damage that can be caused. A cyber attack on the Internet will probably not produce any spectacular images of smoking debris, fatalities and casualties. A successful cyber attack takes a long time to prepare, is complex and is made difficult by the dynamism of the Internet. A cyber attack requires a strategic vision, training, and the availability of money and resources. Anonymity is also relative on the Internet. A cyber attack does not fit in with the jihadists' goal of martyrdom. The high level of resilience makes it an unattractive area.

Another argument against a jihadist cyber attack, referred to in the in-depth study, is still valid but requires modification. Jihadists use the Internet in abundance for other purposes (see Chapter 3). If they were to disrupt the Internet as a whole, the jihadists would shoot themselves in the foot because, in such a situation, they would not be able to use the Internet themselves either, let alone claim responsibility via the Internet for the cyber attack, and because a terrorist cyber attack could result in an increase of monitoring, control and regulation of the Internet and Internet use by the authorities. Jihadists would possibly be more concerned about the second consequence than the first.

2.3.4 *Jihadist cyber attack capacities*

Paragraph 2.2.2 describes two methods for carrying out a cyber attack, namely mass overload attacks and targeted hacking. It would be most logical to use the first method for an attack on the Internet, certainly in the case of one that focuses on the vulnerabilities in the Internet structure (see 2.3.2.3). Such an attack on the Internet itself would require a great deal of preparation, but no excessively in-depth knowledge, since sufficient money and effort would enable an enormous botnet to be used.

Nevertheless, the chance of success is small due to the resilience of the Internet. If jihadists were to (be able to) infiltrate the Internet sector, this would cause the possibilities for carrying out a cyber attack to increase. This option is described in the in-depth study. The comment is made that in order to achieve a real effect, jihadists would have to infiltrate the organisations of the major Internet parties. Just as in 2006, the conclusion is that this would have little chance of success because the technicians who have the right knowledge are part of a close-knit community and know each other well. Of course it is important that suspicious behaviour is detected in good time. Although it might be easy to trace the guilty party, the damage will already have been done. The telecom market is also a growth market whose vulnerability to infiltration is increasing as a result. Having more employees also means a greater likelihood of successful *social engineering*.[49]

49 Expert meetings in 2006 and 2009.

2.3.5 *Consequences of a cyber attack*

The in-depth study describes the consequences of a successful cyber attack aimed at the Internet. The view is expressed that the consequences of the Internet collapsing would be considerable in an economic sense, but that the likelihood of human victims is small, except perhaps in the context of a breakdown of telecommunication systems, meaning that emergency numbers could not be contacted. In the meantime, the Internet is being used even more widely and dependence on the Internet is rising. Although Internet telephony was only in its infancy a few years ago, the number of subscribers is now considerable.[50]
In addition, 'smart energy meters' are now available, patients' records are being digitised and vital sectors worldwide are also continuing to use the Internet more and more. This is creating all kinds of links between systems or infrastructures. As a result, new vulnerabilities are being created which have not yet been identified. The increased dependence on the Internet means it is probable that (even relatively short-term) downtime will have a greater social impact than in earlier years. Just as in the case of a sudden electricity failure, such downtime will reveal just how much modern life is linked to the Internet. A recent estimate of a large-scale failure of the *critical information infrastructure* puts the worldwide costs at 250 billion dollars.[51]
Availability is therefore very important and downtime can damage confidence. However, consumers still trust digital money transfers despite the fact that a number of incidents have taken place, and despite the risk that the system might become the object of cybercrime. This consumer trust appears to be remaining stable, for as long as, for example, banks reimburse the resulting damage. In addition, various sociological studies have shown that consumers still believe that the institutions will be able to solve the problems.[52]

The expectation was and still is that any Internet downtime due to a cyber attack will be relatively short.[53] Technical malfunctions occur quite regularly and, although they are inconvenient, they do not cause panic. One logical argument is then that, all in all, the effects are not worth the efforts required to ensure that such an attack is successful. However, it is conceivable that a malicious disruption caused by jihadists, even one that is limited in size and time, will cause proportionally more unrest than a regular technical malfunction. Such an incident will probably be experienced differently by citizens, the media and politicians. A limited disruption will therefore also be interpreted as a 'success' for the jihadists.

2.3.6 *Assessment of the threat of cyber attacks by jihadists*

Enormous botnets are required to attack the Internet itself. The number and size of botnets is increasing while their price is falling. Moreover, the vulnerability of the Internet has increased since the in-depth study. This does not alter the fact that the level of resilience continues to be substantial. The fact that an attack on the root servers on 6 February 2007 was dealt with without too many problems and that no other (noticeable) attempts appear to have been made since then, confirms the capacity and degree of redundancy of the Internet. Moreover, as regards resilience it is also important to remember that the Internet is a network of networks. The diversity this implies is increasing all the time, meaning that attacks can never affect all the sections of the Internet to the same degree. The attempt in 2007, albeit not by terrorists, shows that such a cyber attack can never be completely ruled out.

50 However, television via the Internet is still only used on a relatively small scale.
51 Global Risks 2008.
52 Expert meeting 2009.
53 Expert meeting 2009.

The NCTb is not aware of any intentions by jihadists with regard to cyber attacks on the Internet, despite the fact that the vulnerability of the Internet has increased and our society is becoming more and more dependent on it. Neither are there any indications of jihadists having sufficient knowledge and capacities to successfully exploit the (increased) vulnerability of the Internet for cyber attacks, although new knowledge can always be acquired. Insider knowledge, however, still appears to be necessary for a truly effective attack.

All in all, a large-scale, successful jihadist cyber attack aimed at the Internet is not probable. However, one should take account of the fact that a small-scale, malicious disruption by jihadists, which cannot entirely be ruled out, will cause a comparatively large amount of consternation.

2.3.7 Other kinds of assaults and attacks on the Internet

Besides cyber attacks, other kinds of assaults and attacks on the Internet itself are also possible, namely a physical attack, an attack using an electromagnetic pulse, and indirect attacks - like those directed at the electricity or telecom sectors - which result in (the infrastructure of) the Internet being unable to function.

2.3.7.1 Possibilities, vulnerabilities and resilience

The in-depth study contains descriptions of a number of locations and elements in The Netherlands which are vulnerable to this type of attack, such as core nodes, core functionalities and junctions which are important for the Internet in The Netherlands, and sometimes for European or even worldwide Internet as well. SIBN administers the '.nl-domain' in The Netherlands via servers of which a number are located in The Netherlands, and the Amsterdam Internet Exchange (AMS-IX), which fulfils a global function, is a key node. The AMS-IX is a kind of roundabout where many roads end up and which facilitates links between networks. However, there is no traffic control system and the AMS-IX itself does not administer any data. Providers and other parties who use the roundabout are themselves responsible for routing their data. Therefore, such data can be sent using other routes which avoid the roundabout. The data exchanged mutually between networks could be considerably disrupted if the AMS-IX were to fail, although the data would soon be automatically diverted. This may have a detrimental effect on speed. If more exchanges were to fail, this would cause capacity problems, although much of the network traffic would then still pass via other connections.[54] If these connections were also to fail, the malfunction would be a drastic one. The resilience to this type of attack is considerable, however. This is shown by, among other things, an article on the *Reken- and netwerkcentrum SARA* which is located in Amsterdam.[55]

The equipment used on the (core) nodes for the core functionalities is strongly dependent on electric power, is sensitive to water and electromagnetic radiation, and requires a great deal of cooling. This equipment is also concentrated in the west of the country. Given the geographical location of The

54 The parties connected to an IX decide themselves to exchange data with each other via their IP networks bilaterally and on a voluntary basis. This voluntary nature is reflected in the fact that the exchange of data takes place not only via an IX but also via private connections (private interconnects) and by purchasing transit from so-called carriers. Which of these alternatives is chosen and the distribution within that (redundancy), is the prerogative of the individual party that wants to links its network to other networks.
55 Spangers 2007.

Netherlands, it receives a large number of transatlantic cable connections and also facilitates cable links between European countries. The vulnerability of such connections was demonstrated by a number of incidents in the Mediterranean and the Persian Golf which occurred in quick succession in January 2008 and which had considerable consequences for specific regions. Two incidents were probably caused by a combination of corrosion and movement of the seabed (which is apparently not unusual), another cable was damaged by the anchor of a derelict ship and lastly, a trunk had to be closed down due to problems with the power supply in a station where the cable arrived on shore.[56] The effects were limited, certainly at global level, and did not have a detrimental effect on people's trust in the system. Sometimes, cables are maliciously destroyed for economic reasons or cables are stolen and the material sold.[57]

Businesses, whether in the vital sectors or not, are having to deal with existing and new risk factors. Outsourcing tasks leads to vulnerabilities. Outsourcing is 'extending the layer of trust'. A company that works for a variety of customers soon has a great deal of knowledge and a strong position, and is attractive to infiltrators. *Supply chain security* is also an issue that companies need to pay attention to, partly in connection with the danger of counterfeit hardware. However, more and more resilient mechanisms are also being constructed. This means there is a better screening of staff and better supervision of staff who leave the company.[58] The authorities are also becoming more and more aware of the importance of Internet exchanges and ICT centres.

2.3.7.2 Intention as regards other kinds of attacks

The only example of an attack like those described above - in this case an attack plan or possibly only an intent - comes from the United Kingdom. Jihadists wanted to blow up a large telecom node in London (Telehouse) from the inside, after infiltration and, in that way, disrupt the British Internet. According to British media, this conspiracy was discovered by Scotland Yard in files they came across during arrests at the end of 2006.[59]

Although a new aspect is that serious plans may have existed for such an attack, the question justifiably remains as to whether jihadists want to devote their capacity and materials to such a target. However, this example again shows that jihadists are considering new methods of working and new targets, are also focusing on economic targets, and are apparently aware of the value or even necessity of infiltration.

Online jihadists responded to the incidents relating to the cable fractures referred to under 2.3.7.1. Via a web forum they drew the attention of their brothers to these vulnerabilities, including a description of fibre optics cables, FLAG (Fiberoptic Link Around the Globe) cable routes, consequences, the way in which repairs take place and the modus operandi for the attack, namely divers who cut through the cables by hand.[60] However, such messages from 'supporters' in jihadist forums say little or nothing about the intentions and capacities of actual jihadist groups. Nevertheless, they can still inspire people.

56 Wolfe 2008.
57 Expert meeting 2009.
58 Expert meeting 2009.
59 Leppard 2007.
60 SITE 2008a.

No information is available on intentions to use electromagnetic attacks on the Internet infrastructure.[61] The American *Department of Energy* estimates the chance of an EMP attack to be many times smaller than that of an attack in cyberspace.[62] Incidentally, an EMP attack also means a large-scale attack with *high altitude detonation* of nuclear weapons. This does not apply in the context of terrorism, and if terrorists were already to have such weapons, their first or most important goal would not be to shut down the Internet. Within the framework of terrorism it is more conceivable that they would carry out a small-scale, specific attack using a more compact (non-nuclear) NNEMP weapon.

There are also no known intentions with regard to other ways of shutting down the Internet. The in-depth study reported that other kinds of attacks - as referred to in the above paragraphs - are not as inexpensive, nor do they have as low a threshold, as cyber attacks, and that physical preparation is needed which will leave traces and make the terrorist vulnerable. This description still applies in 2009. In addition, it was and is the case that even a group would have to make a considerable effort in order, for example, to cause cable breaks at numerous critical locations, blow up various Internet exchanges or deactivate them in some other way. This type of attack can generate spectacular images which may then have to be displayed using media channels other than the Internet. The (visible) consequences of such an attack may cause unrest and indirectly have a (temporary) effect on the economy. Due to the dependence of the economy on the Internet, such an attack is certainly in alignment with the strategy of jihadists.[63] However, it is still very much the question whether terrorists would regard this as a sufficient terrorist effect. From that perspective it is logical to assume a strategy by which multiple attacks or a mix of attacks would be carried out, of which one or more would be directed at the Internet. An attack like the one in Mumbai at the end of November 2008 is suitable for a scenario like this, and is therefore not inconceivable. Of course, a more complex attack does increase the chance of earlier discovery.

2.3.7.3 Capacities

Information about important nodes is relatively easy to access. The required knowledge and materials for the use of (home-made) explosives is also reasonably accessible. As indicated in the in-depth study, sufficient training material for home-made explosives is available on the Internet. Handbooks on home-made explosives also make it simpler for people without the right experience or the required level of training to experiment with, and manufacture, such explosives.

Manuals and study material are also available for electromagnetic attacks and equipment and they are thought to be becoming increasingly available and accessible.[64] This implies a risk.[65] Nevertheless, it still appears to be quite difficult to achieve sufficient capacity to carry out an actual attack. As far as is known, this capacity has not yet been used by terrorists. More knowledge and resources are required than is currently available for a specific and large-scale electromagnetic attack.

61 However this does not detract from the fact that the NCTb has included such a threat in the scenario for an exercise with one of the sectors within the Counterterrorism Alert System *[Alerteringssysteem Terrorismebestrijding]*.
62 EETimes 2009.
63 Based partly on the expert meeting 2006.
64 Automatiseringsgids 2009b.
65 Graham 2004. This research report shows that *hardening* of equipment against EMP implies surveyable (1-3%) extra costs if this is included in the design and production of new equipment.

It must be assumed that the degree to which the telecom sector depends on electricity is common knowledge. Whether an attack on the energy sector, if one were to take place, can be regarded as actually being directed at telecommunications is improbable, unless jihadists publish explicit claims to this effect following such an attack. A specific attack on the power supply of a key node can be seen as such. On the other hand, the effects of such an attack are easier to deal with at local level.

2.3.7.4 Consequences

The consequences of other kinds of attacks on the infrastructure of the Internet are similar to those of cyber attacks. However, if explosives are used, this may well result in immediate deaths and casualties, for example among staff of the company targeted and possible bystanders. A major difference with cyber attacks is also that damage caused by this type of attack entails a longer recovery period.[66] For that reason, causing physical damage at key points can, in particular, be effective (during the conflict in Georgia mid 2008 ISP routers were blown up). A broken building and server equipment cannot be replaced or 'reset' that quickly, as for example in the event of a cyber attack. On the other hand, the case of the fire at the University of Twente at the end of 2002 showed that parties are able to supply each other quickly with equipment. For competition reasons this will not be possible in all cases.[67] An estimate of the consequences of cable sabotage can be made on the basis of an incident in the US, where dozens of wrecked fibre optics cables at four different locations resulted in a failure which lasted for seventeen hours.[68]
As also stated in the in-depth study, Internet companies like AMS-IX often operate from a range of different co-locations, which means that, even during downtime, the effects are relative for that specific service provider. Redundancy is increasing and visibility decreasing. The result is protection, not only against DDoS attacks, but also against physical attacks.

2.3.8 Assessment of threat of other kinds of attacks

Terrorists will not be able to shut down the Internet by carrying out other attacks unless they acquire nuclear weapons which are exploded at a great height and which cause an EMP. If they already had such weapons, their first or most important goal would not be to shut down the Internet.

The Internet has a number of weak points, such as exchanges and cables, which could be the target of attacks. However, there is considerable redundancy within the Internet, numerous measures have been taken to limit the vulnerabilities, and awareness regarding vulnerabilities has increased. If the Internet were to be hit by bomb attacks or by power cuts, the consequences would be relatively small-scale, would occur locally or regionally (except in the event of a national power cut) and would be quite easy to deal with. However, the recovery time after a bomb attack can be (considerably) longer than in the case of a cyber attack. There may also be deaths and casualties. Although terrorists are used to working with explosives, it would not be logical for jihadists to opt to attack the Internet using explosives, since other targets are more attractive and the 'costs' probably do not weigh up against the 'benefits'.

66 Expert meeting 2009.
67 Expert meeting 2009.
68 Webwereld 2009. The first cable that had been cut provided the AT&T network with fixed telephone lines and the underlying network for mobile telephones. After that another fibre optic cable was destroyed, affecting a telecom provider (Sprint) and a data centre. The sabotage also affected mobile telecom providers such as Verizon and Nextel because they use the AT&T and Sprint lines.

News of a possible bomb attack on the most important British telecom/Internet location is important in this regard. It ties in with the numerous conspiracies and networks, whether inspired by (core) Al Qaeda or otherwise, which the United Kingdom was confronted with at that point in time. Moreover, the idea for the attack may never have materialised. However, it is in any event an indication of possible intentions on the part of jihadists, and an acknowledgement of the risk of infiltration. As stated in 2.3.4 the sector is aware of this risk.

All in all it has to be concluded that another kind of jihadist attack directed at the Internet is improbable, but more probable than a successful cyber attack directed at the Internet. As was the case at the time of the in-depth study, such an attack appears to be most conceivable in combination with other attacks, with the aim being to increase the chaos. The attacks in Mumbai at the end of November 2008 demonstrated that a mix of targets is (still) one of the jihadists' options.

2.4 The Internet as a weapon

2.4.1 *Clarification*

The in-depth study focused in particular on the digital vulnerabilities of vital companies, meaning the hostile takeover or manipulation via the Internet of the control systems of, for example, a nuclear power station, or the long-term rendering unusable or unreliable of essential (for example financial) services: the Internet as a weapon.[69]

2.4.2 *Possibilities for using the Internet as a weapon, vulnerabilities and resilience*

The in-depth study examined the role of process control systems like SCADA[70] in vital sectors. SCADA *(Supervisory Control And Data Acquisition)* is a generic term for process control systems used by numerous business sectors, including the transport sector, the chemical industry, and water and power companies. A SCADA system monitors *(view)* and manages *(control)* complete installations, with data often being controlled or read out remotely. In simple terms this means checking whether all the valves are in position, receiving signals from measuring points and making adjustments on the basis of these signals. This makes SCADA attractive for targeted hacking in that the real systems manager then experiences *a loss of view*, as a result of which he can no longer see what the system is doing. *A loss of control* may also occur, as a result of which the operator loses control over the system to, for example, an unauthorised third party. To the perpetrators of the attack this may be a goal in itself, although it could also be used for blackmailing purposes. The CIA issued information on such a case, which was probably carried out with help from someone on the inside, and which was directed at a number of vital sectors outside the US.[71] Blackmailing would be evidence that this type of a case is on the increase because, up to now, online gambling and pornography companies had been affected.[72] As is always the case with such notices, the question is whether the process control network has actually been hijacked or just the administrative part of, for example, a gas company. Although this is also annoying, it is a different kind of attack and would not have any terrorist effect.

69 In this context it also applies that cyber attacks used to make a political statement (referred to as hacktivism) is not included because neither the intent, nor the consequences, are covered by the definition of terrorism. It is also important to (continue to) make a clear distinction between this and the use of the Internet as a resource. The distribution of information via the Internet regarding the locations of nuclear power stations or the threat of an attack as a way of creating a sense of fear are activities for which the Internet can be used as a resource, rather than a weapon.

70 Previous publications by, for example, the Ministry of Economic Affairs were also discussed.

As regards the remote controlling of process control systems, the vulnerability of wireless connections has again increased due to the partial cracking of the WPA key.[73]

Numerous incidents and vulnerabilities have come to light since the end of 2006. In the US, for example - albeit in a test environment - a fire was caused by a cyber attack on the electricity network, resulting in a turbine becoming so overloaded that it eventually shut down.[74] It is striking that the incidents are often related to *insiders*. In this context, the in-depth study referred to the well-known incident in Australia in 2001, when an angry former employee of a water purification company allowed millions of litres of non-purified water to escape.[75]
The vulnerability of process control systems such as SCADA can partly be explained by the differences with regular ICT. For example, a SCADA system has to be operational 24/7. The logical standard solution for problems in ICT office environments, referred to as a reboot (restart) is not an option.[76] There is also said to be 'active and sophisticated chatter' in the (general) hacker community, involving exchanges of knowledge, experience and exploits.[77] Although the existing heterogeneity of systems reduces the chance of broad-based, successful attacks,[78] more and more process control systems work using standard operating systems, and there is also a limited number of suppliers of process control software.

As far as the Dutch situation is concerned, it appears that a many vital sectors are aware of the vulnerabilities and possible consequences, and are also taking appropriate action. The government is bringing relevant organisations and knowledge together to tackle this issue. The market may be adapting to this development by offering instruments to reinforce the defences. On the other hand, certain incidents and penetration tests indicate that things are sometimes made very straightforward for parties with malicious intentions, and that security measures should focus on three different aspects, namely technical aspects (for example firewalls and logging), process-oriented aspects (for example authorisations), and staff-oriented aspects (for example the increasing of resilience to *social engineering*).[79]

2.4.3 *Intentions of jihadists as regards the use of the Internet as a weapon*

As in the case of the Internet as a target, both advantages and disadvantages apply to the use of the Internet as a weapon; these factors play key roles with regard to the question of whether, and to what extent, jihadists would want to use the Internet as a weapon. The advantages are: the potentially substantial economic damage; a link with the concept of an asymmetric conflict; the creation of cyber fear; the exploitation of existing vulnerabilities; the fact that computers, Internet access and hacking tools are available to all; the possibility of remote operations, (relative) anonymity and a (relatively) low chance of getting caught; a low threshold (in comparison with a (suicide) attack; and no losses for the organisation itself. Moreover, by attacking the vital infrastructure jihadists do not end up burning their own fingers, as in the case of

71 Computerworld 2008 and SANS 2008. Later notices refer to Brazil as the possible victim.
72 Buxbaum 2008.
73 ZDNet 2009.
74 National Terror Alert 2007.
75 Kravets 2009.
76 Cheong 2008.
77 Forbes 2007.
78 Expert meeting 2009 and Lachow 2009, p.453.
79 Also see: Lachow 2009, p.445

an attack on the Internet itself. The disadvantages are the complexity of a serious cyber attack, and uncertainties regarding both the chance of success and the consequences of an attack. In addition, the visibility of the consequences may be less direct than in the case of a regular bomb attack.

The in-depth study claimed that discussions *(chatter)* about SCADA in jihadist web forums would increase. The general paragraph 2.2.3 describes terrorists' interest and skills. During the past three years there has been little evidence of an increase in interest or 'chatter'.[80] However, at the end of 2009 it was reported that the FBI is investigating people who may have links with Al Qaeda, or who support this organisation's ideas, and who are thought to be aware of the vulnerability of the vital infrastructure in the US for cyber attacks and to have also discussed this vulnerability.[81] This would, however, appear to be an exception.

Many jihadist websites have subforums on 'technology' and 'the Internet'. In quite a few cases these comprise topics whereby hacked operating systems, software packages, other programmes/tools (including security and encryption-related tools) and serial numbers are provided and discussed. In this context (supporters of) jihadists have just as much knowledge of illegal software as others, but this is scarcely an indication of other kinds of intentions or capacities. This issue may well be a hot item on other locations on the Internet or elsewhere. Little relevant information is available however.
An exception was a message that appeared on the jihadist al-Ekhlaas forum, which has no longer been available since September 2008, which included numerous suggestions for attacks (such as the previously mentioned possibilities for attacks on cables, see 2.3.7.1). One forum member reported in detail about a penetration test that had been made public, and 'technical' forum colleagues were urged to get involved in such thing.[82] Such a post does not contain any new details for expert readers. To those for whom it is news, it is almost certain that they do not have the knowledge to do anything with the information.
It may be a source of inspiration, but not a risk in the short or medium term.[83] The fact that jihadists are aware of vulnerabilities does not mean that they are able or willing to act on that knowledge. Much of that knowledge results from discussions of vulnerabilities in the West. For example, Al-Zawahiri was reported not to be interested in CBRN attacks until he read how easy it is to obtain certain materials, and how much of a threat such attacks were perceived to be in the West.[84]

2.4.4 *Capacities of jihadists as regards the use of the Internet as a weapon*

It has been known for some time that laptops seized in Afghanistan contained information on certain vital objects. In an interview in 2003, which was not referred to in the in-depth study, an American former government official stated that such laptops had been used to collect information on SCADA systems in the electricity sector. Others reported on the presence of information on SCADA in the drinking water sector.[85] The lack of actual access to such material makes it difficult to assess the information. Was it information on the fact that SCADA systems are used in certain sectors, that these systems are vulnerable to manipulation via the Internet, or did it comprise detailed instructions and tools for actually taking action? Was the

80 In a general sense this interest has certainly increased since 2005
81 Wall Street Journal 2009.
82 SITE 2008b.
83 Expert meeting 2009.
84 Stenersen 2008, p.41.
85 Luiijf 2008.

SCADA information secondary information gathered while searching for physical vulnerabilities? Was the information no more than some rudimentary ideas, or a target selection or preparation for action? Were the owners or users of the laptops inspired by reports of the vulnerability of SCADA systems, and were they simply looking for more information? This does not make them experts, and one cannot then really speak of a threat. As mentioned in 2.2.2.1 it is possible to set up a test environment on the basis of hacked process control software, handbooks and components/equipment obtained via the Internet. The fact that no information about such a test environment has become available since the 2003 interview, and that terrorists have not claimed any such incidents as attacks, may be the beginning of an answer to the above questions.

Targeted hacking is the most logical method for carrying out attacks via the Internet, although specific DDoS attacks can also lead to disruptions in vital sectors. A serious attempt at hacking is not something that can be done at any odd moment. Despite reports about successful penetration tests suggesting otherwise, the expectation is still that terrorists need a long time to prepare such an activity, and have to invest money. In the in-depth study and in paragraph 2.2.3 reference is made to the level of computer and Internet skills and the interests of jihadists. This level and interest, and the fact that there are no known examples of the Internet being used as a weapon by jihadists, do not lead us to suspect that an attack should be expected in The Netherlands in the short term. However, simpler cyber attacks which disrupt processes cannot be ruled out, since they do not required any advanced capacities. A risk is also present in methods other than technical ones, such as social engineering and infiltration.

2.4.5 *Consequences*

The in-depth study stated that countless scenarios are conceivable but that it is difficult to imagine that a cyber attack would cause large numbers of deaths and casualties. Exceptions may be hospitals and passenger transport systems. A major power cut may cause panic among some members of the population, resulting in reactions such as people hoarding supplies and repercussions on the stock exchange, and may eventually cause disruptive damage to society. The failure of virtual services such as Internet banking, on which society depends to an increasing extent, will cause huge problems. However, terrorists will have to attack several targets simultaneously for a longer period of time in order to achieve a socially disruptive effect.[86] The disruption of the process control of a single power station is more likely to be used for propagandist purposes than seriously jeopardise the electricity supply.

As in the context of the Internet as a target - where the services sector can just as easily be a victim - trust in the institutions involved has remained stable for a long time now, and consumers have faith that these institutions will solve the problems that arise.[87] Not every disruption will also actually be perceived or experienced as an attack. As indicated above, people are used to, for example, electricity and computers malfunctioning. Lastly, there are always people who can detect those malfunctions and changes at an early stage, and who can then limit the consequences. However, as referred to in the section on the Internet as target, in these cases as well, the expectation that malicious disruption will have a greater impact than just a technical failure must also be taken into account.

86 Lachow 2009, p446 and expert meeting 2009.
87 Expertmeeting 2009.

2.5 Conclusion as regards the Internet as a weapon

Developments are taking place which indicate an increase in risk factors, such as demographic details, the increasing availability and quality of attack resources, 'chatter' regarding vulnerabilities, the risk of outsourcing, and the increase in use of, and dependence on, the Internet, which also applies to the (vital) commercial sectors. However, efforts are also being made with respect to resilience. For example, there is now a greater focus on cyber security, governments and the business communities in various countries (including The Netherlands) are cooperating on *awareness* and with that resilience, and there is also international cooperation in this field to which the market may be able to respond in order to strengthen the relevant technical defences.

Nevertheless, tests and incidents also demonstrate in practice that vital sectors are still vulnerable to insiders and dedicated teams of hackers. Such examples raise questions as to whether a network penetration would only have caused a disturbance or would have led to a complete takeover. As far as the NCTb is aware, jihadists and their supporters cannot do much more than (incite people to) carry out simple cyber attacks such as defacements, which is an important indicator of their intentions and capacities. This does not alter the fact that, if jihadists succeed in achieving a different effect, which still does not have to mean immediate consequences which can be labelled terrorism, the spectre of *cyber fear* can always rear its ugly head. The resulting inconvenience and unrest can also be seen as a jihadist 'success'. Yet, if we examine their intentions and capacities, in combination with the history of jihadist attacks, the expectation is that jihadists' preference will still be for carrying out classic bomb attacks and suicide attacks. They have more experience with these and such attacks have a more direct and predictable effect than an attempt at the digital disruption of a vital sector.

The conclusion is, therefore, that a successful jihadist-terrorist attack via the Internet aimed at the vital infrastructure or crucial online services is still improbable in the short term. Vulnerabilities and possibilities have probably increased rather than decreased, but there are insufficient indications that jihadists are willing or able to exploit these successfully. However, simple disruptions are certainly possible. The resilience of the vital sectors and crucial online services must be increased (even more) to avoid making it too easy for parties with malicious intentions, including perhaps jihadists, to cause more serious damage.

2.6 Concluding observations

This research is limited to jihadists, given that jihadist terrorism is the most significant threat from the NCTb perspective. As regards the 'Internet as a target and as a weapon' aspects, as far as the NCTb knows, jihadists are unable, without outside help, to carry out a complex cyber attack successfully which would have a socially disruptive effect. Neither are there many indications of jihadists having such intentions, nor that outside assistance is indeed being sought or offered. No serious cyber incidents can be traced to jihadists.

Three comments need to be made with regard to the above statements.

The first concerns the period of validity of the conclusions. Developments are taking place rapidly and not all intentions and activities will be identified. One reassuring thing is that the conclusions which the NCTb drew in 2006 have remained accurate to date. In the meantime we have become aware of all manner of vulnerabilities. However, these vulnerabilities are becoming more and more widely known and tests and incidents indicate that, certainly in combination with social engineering, they can actually be exploited. It is not easy to assess how things will develop in the future. In order to avoid a decline in resilience, it is important in any event that such vulnerabilities are eliminated.

The second comment concerns the focus on jihadists. As indicated in the introduction, much of the literature on the subject makes no distinction between the parties that might carry out an attack, such as states, criminals, vandals or other individuals or terrorists. After all, the vulnerabilities outlined may also be exploited by people other than jihadists. By contrast, raising the resilience to cyber attacks by jihadists affects the effectiveness of *all* threat sources.

Lastly it is important to acknowledge that the assessment that a complex attack of a terrorist nature on or via the Internet with real socially disruptive consequences is not anticipated, is no reason to be less vigilant, since a simpler attack, whether of a terrorist nature or otherwise, can for example have unexpected effects in vital sectors. Although such a disruption may then be smaller in scale, or shorter in duration, the malice behind it will generate greater unrest and media attention than a disruption caused by a technical malfunction or human error.

3 Internet as a resource

3.1 Introduction

It is very important to realise that the use of the Internet by jihadists cannot be based on an isolated study of general developments in society, on the Internet and within jihadism. Developments on the Internet take place rapidly, with new applications appearing all the time, and the use of the Internet is becoming more and more interwoven with our daily lives. In this context it is not strange that Internet use by jihadists is also continuing to develop.

This chapter starts with a general description of the use of the Internet as a resource (paragraph 3.2). The conclusion drawn is that the Internet is a crucial resource for the jihadist movement and is used for many purposes. The analytical distinction between types of use, as applied in the in-depth study at the end of 2006, can still be used as such, although it is by no means possible to always make a clear distinction between these types of use. For example, propaganda can contribute to radicalisation, recruitment and fund-raising and recruitment can take place within virtual networks. The relevant literature also refers simultaneously to radicalisation via the Internet, propaganda, recruitment and virtual network formation.[88] For the sake of clarity, and due to the connection between certain types of use, a decision has been taken to use a sequence for the types of Internet use which is different to the one used in the in-depth study. Paragraphs 3.3 to 3.10 successively examine the different types of Internet use by jihadists. Each paragraph ends with an assessment of the threat of this type of Internet use for The Netherlands or for Dutch interests, viewed in the international context. The chapter ends with concluding observations.

3.2 Use of the Internet as a resource

This paragraph outlines a number of general notions about jihadist Internet use. It examines :
a) the jihadist movement on the Internet,
b) the use of applications,
c) the disappearance of prominent international jihadist sites,
d) the increasing focus on a Western audience and
e) the relationship between virtual and physical activities.

3.2.1 The jihadist movement on the Internet

Jihadist concepts, theoretical insights, views and notions are (re)produced and distributed in numerous ways via jihadist mosques, training and education institutions, via regular media, and certainly, or perhaps primarily, via the Internet. According to Sageman, the major role the Internet plays within the jihadist movement has not been planned, but is rather the consequence of a spontaneous evolution, based on the growth of the Internet and the attention paid by the government to meeting places and mosques.[89]

Production, reproduction and distribution is carried out by various leaders of the jihadist movement. First and foremost there are the spokespeople of core Al Qaeda, particularly Osama Bin Laden and Ayman al-Zawahiri, A. Y. al-Libi and M. Abu al-Yazeed. In the second place there are the leaders of the self-proclaimed ‘Islamic states’ in Afghanistan, Iraq and Chechnya. Thirdly there are the local or regional leaders of various jihadist groups. In addition, jihadist ideology and strategy are being (re)produced and distributed by spiritual (aspirant) scholars, preachers, strategists and analysts, translators and jihad fighters in the field.

88 Examples are Sageman 2008a, ICSR 2007 and ICSR 2009.
89 Sageman 2008a, p. 110, 121.

The strategists and analysts are people who produce visions and evaluations about the progress of the jihadist conflict. From time to time, the names or pseudonyms of leading analysts appear in various jihadist forums where they explain the course that is being taken by Al Qaeda and the jihadist movement. Translators form an important link between the often Arabic producers and the members of the second and third generation of Muslim young people in the West. Individuals often perform this translation work voluntarily. Examples of productions by jihadist fighters are 'stories by Arabic fighters' and texts by individual jihadist fighters who have died as martyrs. These stories taken from real life appear to be primarily intended as a recruitment resource. In addition, numerous sympathisers participate in a wide range of discussions. All this leads not only to a global distribution of ideas and materials, but also to a global brainstorming session about the way in which the jihad can be served.[90]

The manifestation of virtual jihadism is based primarily on three virtual media organisations. These play a crucial role in the creation of jihadist publications and audiovisual productions and are also responsible for their punctual and simultaneous distribution among designated websites and forums. These are:
1) As-Sahab ('Al Sahab Institute for Media Production'),
2) Global Islamic Media Front (GIMF) and
3) Al-Fajr (Media Centre).

These media organisations are relatively autonomous and they have varying organisational links with jihadist groups. They operate in virtual networks, with tasks being allocated to a certain degree. The nature and quality of productions, the methods of working and the areas of special interest vary. As-Sahab, which means 'The Clouds', acts as the media organisation of core Al Qaeda. The messages are produced in various languages and versions, and are aimed at a wide audience. It is the only and exclusive organisation which maintains physical contact with the Al Qaeda leadership. The GIMF is one of the largest and, up to now, the longest-lasting media organisations. Up to now it has not had any direct links with the Al Qaeda leadership. The GIMF operates on the Internet in a more or less open way. Its productions focus more on the conflict in the field, than on the jihadist movement leadership. Presumably the GIMF is run by amateurs who develop a variety of media projects, such as Internet TV. However, the GIMF also acts as a publisher of digital books and magazines. It has also made video training courses on how to handle weapons, ammunition and explosives. Lastly, Al-Fajr is one of the distribution centres which focuses on supporting various jihadist groups in Iraq, as well as in North Africa and the Arabian Peninsula. Al-Fajr, which means 'The Daybreak' and which is the title of soera 89 in the Koran, was established at the beginning of 2006 and was responsible for a number of Al Qaeda websites, such as the al-Falluja and Shumukh al-Islam websites, as well as for new publications and media productions. This centre supports the 'al-Malahem Foundation', the Al Qaeda media organisation in the Arabian Peninsula. It reproduces the media productions of as-Sahab and Labbayk, the Taliban's media organisation. An independent product of the al-Fajr centre is the magazine entitled 'The Technical Mujahid', which focuses on ICT methods and techniques.

Besides these 'large' media organisations, there are also a number of small-scale virtual media organisations which focus on specific tasks such as the media coverage of jihadist actions of some groups. A prominent example of a small-scale media organisation is the 'Al-Furqan Foundation for Media Production', an organisation which is undergoing rapid development.

90 For the latter, see Hegghammer 2006.

In addition to media organisations there are also numerous terrorist groups and sympathisers on the Internet. They use static websites and interactive forums, chat rooms, blogs, etc. At international level there are hundreds if not thousands of jihadist sites, forums etc.[91] As a result, jihadism on the Internet comes across as very chaotic. Nevertheless, there is a certain structure. On the one hand that structure is created as a consequence of the three virtual media organisations referred to and, on the other hand, by the presence of a limited number of so-called mother sites, an initial layer of primary sources from where distribution takes place. For example Al-Fajr controlled and ran a number of (former) mother sites such as al-Ekhlaas, al-Boraq, al-Firdaws and al-Hesbah.[92] The number of mother sites varies between five and ten sites active at any given time.

Although limited in number, the reach of the mother sites is considerable. On the one hand this is the consequence of the large number of registered members and, on the other hand, of the fact that the message is quickly distributed to or is adopted by a second layer of sites and then a third layer. This facilitates the optimal combination of the benefits of both a more centralised and a decentralised communication, which are the authenticity of the messages, and a broad distribution of these messages. Once the messages have been posted on one of the mother sites, it stays on the Internet for some time.[93] In addition, the traditional mass media regularly adopt messages from the media organisations, thereby ensuring even wider distribution of the message. This rapid and broad distribution can contribute to the image of a strong and united jihadist movement.

Nevertheless there are also disadvantages associated with this method of working. The more the distribution extends into the periphery, or the more messages are adopted by the traditional mass media, the easier it becomes for the message to be distorted or commented on by opponents.[94] Another disadvantage is that although there are many jihadist sites, these only attract people who are interested in the jihadist conflict. As a result, they do not reach a wider group of surfers.

Jihadists not only use specific jihadist sites, but are also active on more general sites which focus on Islam or Muslims in general. Jihadists are increasingly using more Western and general media like YouTube. For example, one jihadist site contains a detailed invitation to use popular American web forums to distribute jihadist films and disinformation about the war. The invitation is accompanied by tips on how to present yourself, which parts of the forum to use, what type of discussions to look for or initiate and what topics to avoid. The suggestion is that you should, for example, start a topic about a fictitious American soldier who you supposedly knew well and who committed suicide in Iraq.[95] The major advantage of this is that the message reaches a wider audience. The disadvantage is that the message can be distorted, commented on or deleted by moderators and that there is an increased probability that intelligence bodies and investigation agencies will also read it.

It is also worth mentioning the existence of mailing groups. The 'Ansar al-Jihad' mailing group has, for example, been active since 2007 and sends jihadist publications and video films to members who have

91 The umbrella term used hereafter is 'sites'.
92 For the latter, see inSITE 2008.
93 Katz & Devon 2007a, p. 4-5.
94 See for example Rogan & Stenersen 2008..
95 The following sources refer to the invitation: Special 2007, Australian Financial Review 2007.

registered on the website with the same name. Another group, called al-Ansar, distributes messages via e-mail from the leaders of the Islamic State of Iraq. Another group is the 'Jihadist Brigades for Dispatches on the Internet'.

Taking everything into account, it can be concluded that the mother sites play a crucial role as the first layer in the propaganda of the jihadist movement, in the distribution of other jihadist material, and probably also in the mutual communication between key figures in terrorist networks and in the formation of virtual networks. Sageman even goes so far as to state that the discourse on the six or so influential mother sites is the real leader of the jihadist movement and not the leader of core Al Qaeda, Osama bin Laden. Even he cannot influence the multitude of jihadist forums and participants.[96] The greater the distance between a site and the parent site, the less grip the jihadist movement has on its use and the users, and therefore the less suitable the sites become for direct recruitment, communication, the planning of operations and the creation of virtual networks. There is also the chance that jihadist contributions will be quickly deleted, certainly now that many of the more neutral sites have moderators and offer the option of reporting unacceptable content for deletion. On the other hand, the reach is increasing. This certainly applies to the large number of sites which focus on the distribution of knowledge about the various general aspects of Islam and other neutral sites in which jihadists can become established. In this way jihadist ideas can spread further and further across the Internet, but the control over the content is becoming more and more limited.

Sageman regards the Internet as crucial for the jihadist movement and describes it as the 'invisible hand which organises worldwide Salafist terrorism' and states that 'jihadist sites are the core of this *leaderless organization*'.[97] [98] Europol alleges that the Internet continues to be a factor which facilitates the activities of terrorist groups, including jihadists, to a considerable degree.[99]

3.2.2 *The use of applications*

In recent years the use of social networking sites has become extremely popular throughout the world as a whole, including The Netherlands. A personal profile can be linked to other profiles to set up a kind of social network. In view of their interactive nature, such social networking sites are illustrative of Web 2.0. Although Dutch people use a variety of (international) social networking sites (including Facebook, Myspace and Netlog), the Dutch site Hyves is the most popular networking site. In July 2009 the website, which was set up in November 2004, had more than nine million members, of whom five and a half million log in every month.[100] As a consequence of their general popularity, social networking sites are also popular among jihadists. For example, the FBI discovered in March 2009 that Somali Americans were actively preaching jihadist violence on Facebook.[101] In February 2009 jihadists - united in the group called 'Facebook invasion' - incited people to post propaganda on social networking sites.[102] Incidentally, the developments referred to above appear to be matched by countermeasures. Currently, social networking sites are being moderated more and more effectively. For example, pages which contain photos or messages which are threatening, offensive or malicious are being removed from Facebook.

96 Sageman 2008a, p. 118.
97 Sageman 2008a, p. 121.
98 In this context the terms 'Islamic' and 'Salafist terrorism' are regarded as synonyms for jihadist and jihadist terrorism.

An application which has gained considerable popularity in a general sense, although that popularity has now peaked, is the three-dimensional virtual world Second Life (SL). In SL you can create a character (an avatar) and then lead a second life. These avatars can carry out all kinds of activities which people also carry out in real life, such as purchasing land, real estate and goods, and can also offer all kinds of services, for payment or otherwise. Potentially, jihadists could use SL:
a) for propaganda and communication with others or each other, for example in the form of house meetings,
b) for the creation of radical groups or areas,
c) for the construction and practising of scenarios and
d) as a means for financial transactions or for money laundering.
What the participants create is, in fact, the property of that person. The value of virtual land, real estate, goods and services cannot actually be determined. Moreover, the Linden dollars can be exchanged for real money. All this makes SL or other virtual worlds potentially attractive for money laundering purposes.[103]

Researchers at the University of Arizona carried out an exploratory study into the use by international jihadist extremist groups of a number of Web 2.0 media, namely blogs, YouTube and SL. Using a number of search criteria the researchers found six important so-called blog hosting sites and twenty-eight large blogs which are important for the international jihadist movement. Using selected jihadist terms they found 265 videos on YouTube, of which 34% (90) are actually jihadist by nature. These dealt generally with explosives, attacks, bombardments, hijackings and the like. Although YouTube removes such videos, they will have already been distributed or reappear at a later date. In SL the researchers found a large number of groups that claimed to be terrorists, although the researchers were under the impression that these were mainly groups of jihadist sympathisers or distributors. Those groups were successfully building up their virtual infrastructure and community. Some of those groups already had hundreds of registered members.[104] Others doubted whether SL is actually attractive to jihadists.[105] The researchers in question concluded that these new, interactive, multimedia-rich types of communication are effective resources for extremists when it comes to putting across their ideas, sharing sources and communicating with each other.[106]

Rogan and Stenersen, two Norwegian researchers, observed a shift from so-called static sites to interactive sites. Discussion forums are participated in by members and sympathisers and used to distribute material, provide new information about, for example, sites that have disappeared, and to take part in discussions whose agenda is often determined by the media organisations.[107] Sageman states that these interactive sites are much more dangerous than the more static - or in his terms passive - sites[108] (see also paragraph 3.3.3).

99 Europol 2009, p. 40.
100 Hyves 2009.
101 Elsevier 2009.
102 SITE 2009b.
103 Cochran 2007a and Cochran 2007b, Nood & Attema 2006.
104 Chen e.a. 2008.
105 Cochran 2007a en Cochran 2007b.
106 Chen e.a. 2008.
107 Rogan & Stenersen 2008.
108 Sageman 2008a, p. 114-115.

3.2.3 *The disappearance of prominent international jihadist sites in 2008*

Jihadist (mother) sites regularly disappear, often to reappear elsewhere. This may be as a consequence of, for example, specific actions by intelligence bodies, by providers (whether or not as a result of pressure from certain groups), or because the owners are no longer able to fulfil their obligations. The owners of jihadist sites themselves may regularly change IP-addresses, for example for security reasons.

The prominent international jihadist site al-Ekhlaas disappeared from the Internet on the eve of 11 September 2008. Other prominent jihadist sites were no longer active at around that time or kept disappearing. Examples are al-Firdaws, al-Boraq and al-Hesbah and the websites of leading spiritual leaders and ideologists of the jihadist movement, like those of Abu Mohammed Al-Maqdissi and Abu Qatada Al-Filistini. The disappearance was the largest of its kind up to that point in time.

During the first days, weeks and months after the disappearance, jihadists sought refuge in other jihadist sites which were still operational. Once these had been found, new websites gradually started appearing, and the already existing, originally smaller jihadist sites, referred to hereafter as non-affected sites, more or less took over the role and content of the sites that had disappeared. Various forums referred to the respective links.

When compared to the period before September 2008, security awareness has increased. For example, the access procedures of the new prominent sites changed after the disappearance. In the first place, access to the newly established site was made subject to a registration procedure. In the second place, the details of the parties registering, such as IP address, stated identity, size and nature of contributions, were checked. In the third place, access to certain parts of forums on the site was restricted to parties known to the webmasters. The forums in question concerned 'preparations for the jihadist conflict' and hosted discussions of technical and operational aspects of the jihad and how to deal with weapons, ammunition and explosives. In the fourth place the contributions by members were critically examined to prevent disinformation and false reporting. Lastly, the sites and participants warned each other in time about reputed infiltration or attempts at disinformation and visitors were given advice about personal security in order to protect their identity.

The sites were given a new style, and new ways of interacting with the visitors to the site were provided. The sites were also given a uniform structure and sections, with discussion forums on political news in Muslim countries, sections with communiqués about jihadist activities, and weekly or monthly bulletins on successes in jihadist conflicts in various parts of the world. A striking feature is that the information on the jihadist conflicts and jihadist movements is provided in various languages. In addition to Arabic, information is also provided in, for example, English, German, Turkish, Urdu, Somali, Albanian, Indonesian, Filipino and Russian. Other sections are classified as the 'Islamic emirates' of that moment, namely Afghanistan, Iraq and Chechnya and key conflict areas which are relevant to jihadists, such as Palestine, Somalia, Algeria, Uzbekistan and Kashmir. These websites are used to distribute ideological, strategic and tactical publications. In addition, messages, invitations and other promotional texts are used to try and get visitors to the sites to join the jihadist conflict. The websites differ as regards their regional and local accents.

Shortly before 11 September 2009, a number of new prominent jihadist sites went *offline*, such as al-Shura, al-Falluja and Shumukh al-Islam.[109] A few reappeared a short time later while others, including al-Shura and Shumukh al-Islam, continue to be down. Both the websites referred to had developed, since the spring of 2009, into replacements of the leading al-Ekhlaas and al-Hesbah websites which had disappeared.

Various jihadist postings show that jihadists assume that the disappearance of the al-Ekhlaas site in September 2008 had to do with infiltration by intelligence services. This was also the case as regards the publication of a new version of al-Ekhlaas in September 2009. The visitors to the jihadist sites responded to this new al-Ekhlaas site with a great deal of suspicion and distrust. Later a number of detailed articles were published in which the 'return' of al-Ekhlaas was explained as an intelligence operation which was intended to trace jihadist fighters with a view to dismantling their virtual and physical organisation.[110] The visitors to these jihadist sites were warned to be on the guard for such manipulation, and they were given relevant practical hints and tips.

In a general sense the disappearance and return of the sites in the period from September 2008 to September 2009 are evidence of a considerable degree of resilience and security awareness. While jihadists were unable to respond quickly after the disappearance in September 2008 and were in a state of uncertainty, they did respond quickly to the disappearance of the jihadist sites in September 2009. In fact, many sites have remained active, or have adopted the role of the sites that have disappeared, and new ones are also appearing with different web addresses. Jihadists inform each other about new sites and web addresses and also warn each other about possible site infiltration or involvement on the part of intelligence bodies. The jihadist media organisations referred to in paragraph 3.2.1 also ensure continuity and continue to be the backbone of the jihadist Internet. They have a large jihadist archive and make that available to others, and arrange the delivery of media productions. However, the experiences of recent years have shown that jihadist sites need time to recover fully from being removed from the Internet. Moreover, there appears to be a great deal of distrust among jihadists themselves. They warn each other about sites that may have been hacked and sometimes openly question the reliability of a site.

3.2.4 *An increasing focus on a Western audience*

International jihadist sites and media, which were often Arabic in origin, are focusing increasingly on a Western audience. This is reflected in three developments. In the first place speeches by the leaders of Al Qaeda and video productions about terrorist activities that have been carried out are often accompanied by proper subtitles in Western languages, particularly in English.[111] In the second place, there is a marked improvement in the quality of translations and use of language. Some publications such as 'Jihad Recollections' have been written or narrated in perfect American English.[112] This makes the jihadist message easier to understand and more convincing. A fictitious figure is also used to reinforce the jihadist message and to show that physical people from the West and America are joining Al Qaeda. One example is 'Rakan Bin William'. This virtual person is presented as an American who has converted to Islam and who has joined Al Qaeda.[113] In the third place, influential jihadist sites are being expanded to include

109 Site 2009c.
110 Communiqué on 'Shabakat Shumukh al-Islam', 22 September 2009.
111 Lia 2009, p. 4, Europol 2009, p. 14, SITE 2009h, p. 1.
112 Hegghammer 2007.
113 Moss & Mekhennet 2007.

English, French and German sections. These contain news, communiqués, bulletins and video films about the jihadist conflict.

3.2.5 *Relationship between virtual and physical institutions, people and activities*

The link between the jihadist media organisations and sites to various organisational branches of the jihadist movement appears to be difficult to establish. The sites are usually not official bodies, nor are they a reflection of the organisational links of various jihadist groups. However, there are indications that the jihadist virtual actors, such as webmasters and forum participants, are well-informed about the various branches of the jihadist movement. For example, the jihadist media organisations have a monopoly on interviews and news scoops from the leadership of core Al Qaeda. As-Sahab has exclusive rights to interview the Al Qaeda leadership and to distribute those interviews. The same applies to Al-Fajr as regards the leadership of the 'Islamic State of Iraq'.[114] Another indication is that some participants in jihadist forums are so well grounded and informed about issues relating to the jihadist conflict, that it can be assumed that their knowledge and information position is the result of experiences in the field. A number of them appear to have left for the conflict areas. These include forum member 'asdasd99' alias 'al-Miskin al-Muhajir' of the al-Firdaws and al-Ekhlaas websites, who joined the jihadist fighters in Afghanistan in June 2008,[115] or the 'Mujahid 1988' who placed a large number of postings on the al-Ekhlaas site during the course of 2007 and then announced his departure to the jihadist battleground in a 'farewell letter' in May 2007.[116] The Al Qaeda video message, which celebrated the eighth 'anniversary' of the attacks in the US, included clips of two suicide terrorists who were involved in the suicide attacks in Pakistan in May 2009. One of these, Ali Jaleel, was a known participant on English language jihadist forums, including those at Tibyan and Firdaws. He was a key translator for that forum.[117]

According to open sources there were links between virtual activities and physical activities of those involved in the jihadist site known as Minbar SOS. Members of an alleged Belgian cell of Al Qaeda, including Malika El Aroud, were arrested in Belgium in December 2008. According to open sources, until her arrest in December 2008, Malika El Aroud was the administrator of the French language jihadist website 'Minbar-SOS'[118] [119] and is said to have posted various jihadist texts. She also translated a variety of interviews and pamphlets by prominent jihadists from Arabic into French.[120] According to open sources, she was active in August 2007 on the site in a discussion about the proposed niqab ban in The Netherlands.[121] She used to be married to the Tunisian Abdessatar Dahmane, who carried out a suicide attack in Afghanistan in 2001. In June 2007 she was convicted together with her current husband in Switzerland for running sites with pro Al Qaeda content.[122] [123]

114 Reals 2007.
115 NEFA 2008.
116 Kohlmann 2008.
117 SITE 2009h, p. 23-24.
118 Cruickshank 2009a, Vlierden 2009.
119 Minbar: platform at the mosque used to preach from.
120 SITE 2007b, Cruickshank 2009c, Israel Military.net 2008.
121 SITE 2007b.
122 SITE 2007b, Cruickshank 2009c, Israel Military.net 2008.
123 At the time of writing at the end of October 2009, the members of the Belgian cell had not yet been convicted by a court. In a formal sense, therefore, they were only suspects as regards their involvement in Minbar SOS and links with physical activities.

As time went by, it became more and more obvious, based on information from open sources, that Minbar-SOS played a key role within the 'Belgian cell of Al Qaeda'. Malika El-Aroud and her current husband are said, among other things, to have used the site to recruit people for the jihad. Her husband and six recruits went to the border area between Pakistan and Afghanistan at the beginning of 2008. Via the forum he had had contact with his followers in Belgium until the end of May 2009. He also posted a call to carry out attacks in Europe at the end of September 2008. He is thought to have logged into the forum for the last time on 24 May 2009.[124] Minbar-SOS has no longer been available since the beginning of June 2009,[125] perhaps because the individuals behind the website have been detained.

3.2.6 *Assessment of the threat of the Internet as a resource: general*

The three media organisations referred to, namely As-Sahab, GIMF and Al-Fajr, play an even more crucial role for the jihadist movement than they did at the end of 2006. The same applies to between five and ten so-called mother sites from which jihadist publications and the jihadist message are first distributed, and which host forums on all kinds of jihadist issues that contain a range of information and views.
By contrast, jihadists are distributing their publications and message more and more via numerous non-jihadist sites and 'applications' such as YouTube and social network sites, which have become very popular since 2006. This can be regarded as a kind of implanting process. Although jihadists have less control over these sites, their reach is many times greater than that of their own sites. Since the end of 2006, two large-scale jihadist sites have disappeared, presumably within the framework of a counterterrorism operation, namely on the eve of the commemoration of the attacks in the US in September 2008 and 2009. While jihadists were not directly able to respond to the disappearance in 2008, they appeared to have learned some lessons in 2009. They have become less vulnerable with regard to the removal of their prominent sites from the Internet. Other tendencies which can be referred to are continued professionalisation and improvements in quality of jihadist publications and the jihadist message, and a greater orientation towards a Western audience.

It is clear that the Internet is a factor which, as Sageman and Europol also indicate, facilitates many jihadist activities.

3.3 Use of the Internet as a resource: specific

The following paragraphs examine the specific ways in which the Internet is used as a resource, as were also dealt with in the in-depth study. First, a paragraph will review the conclusions of the in-depth study, after which new or additional insights are dealt with per issue.

3.3.1 *Review of the in-depth study*

Propaganda

The conclusion of the in-depth study was that propaganda via the Internet contributes to radicalisation. Propaganda via the Internet is professional, has considerable reach, and meets with relatively limited resistance. The propaganda is not restricted to one-way traffic, since jihadists actively try to interact with interested parties. If we combine that with the fact that it is primarily large groups of young people who

124 Site 2009d, Cruickshank 2009a, Vlierden 2009, Cruickshank 2009b.
125 Vlierden 2009 and personal observations on 2 July 2009.

have access to the Internet and use it intensively, it is clear that the result is a breeding ground for (further) radicalisation. That applies in particular to Muslim women due to the lure that the Internet has for them (demand side) in combination with the active role of radical Muslim women on the supply side.

The influence on radicalisation
The conclusion was that Internet use supports the entire radicalisation process. A supply of jihadist material is available for each phase of radicalisation. Using the Internet, a potential jihadist can go through the processes of ideology formation, ideology reinforcement and ideological indoctrination. It also helps to form groups and networks of like-minded people. As a result, individuals and groups can turn against society, first ideologically and possibly, in time, as violent activists. The question was asked as to what extent and how the Internet actually plays a role in radicalisation and eventually leads to terrorism.

The creation of virtual networks
The conclusion was that virtual networks increase the jihadist movement's power to act. The formation of virtual networks can lead to the creation of an informal pool of people who are willing to become involved in the jihad in varying combinations, and who are able to devise violent activities with each other or individually. As a consequence, local and international elements can become more interwoven. As far as jihadists are concerned, virtual networks have advantages and disadvantages, with the question of trust being one of the most important disadvantages.

Recruitment
The conclusion was that Internet use results in more interactive types of recruitment which cannot yet be properly identified, and in conscription and autonomous radicalisation. A feature of the Internet is, above all, that potential fighters are wiling to put themselves forward for participation in the violent jihad (conscription). In relation to the Internet, the term autonomous radicalisation (spontaneous combustion) is also used to describe someone who wants to embark, or indeed embarks, on his own private jihad. While it is difficult to view the transfer from radicalisation to recruitment and conscription in the physical world, the same certainly applies to the Internet

Acquiring information
The conclusion was that acquiring information via the Internet potentially supports the performance of terrorist activities. Information can be obtained to serve a wide range of goals. As for everyone else, the Internet is an inexhaustible, low-threshold source of information for jihadists as well, which information can be combined using professional resources such as data mining. Information can be acquired legally and illegally, for example through hacking.

Fundraising
The conclusion was that fund-raising via the Internet by and for jihadists only takes place on a limited scale, but that more secretive fund-raising is to be expected.

Training
The conclusion was that use of the Internet for training purposes lowers the threshold when it comes to carrying out attacks.

Mutual communication and planning
The conclusion was that jihadists use the Internet to communicate with each other and plan.

3.3.2 Propaganda: additional or new insights

3.3.2.1 Propaganda is very diverse by nature
From an analytical perspective, a number of types of propaganda can be identified, namely:
- the recruitment or retention of close followers and (larger) grass roots support;
- the influencing of international public opinion;
- the influencing of the enemy and the enemy's audience;
- the instilling of fear;
- hacktivism.

The distinction drawn between these types of propaganda is not always clear, because one message can serve a wide range of goals and may be aimed at a variety of target groups.

Various kinds of jihadist propaganda can be found on the Internet. There is a continual stream of editions and reprints of jihadist publications, audiovisual media productions etc. These may deal with the jihadist conflict, but may also examine many other issues from a jihadist perspective. Examples are democracy, liberalism, secularism and relations between Islam and the West. Besides three prominent media organisations and a number of prominent mother sites, there are also a great number of jihadist sites, and the jihadist movement also makes use of sites which focus on Islam or Muslims in general, and neutral sites such as YouTube. It is logical, therefore, that jihadist propaganda comes in many shapes and sizes.

In particular, the three media organisations referred to earlier have published a substantial stream of propagandist messages (audio, video and text). We certainly hear frequently from the first and second in command of core Al Qaeda, Osama Bin Laden and Ayman al-Zawahiri. They comment on both current themes, for example the Israeli occupation of the Gaza Strip at the end of 2008 and the speech by President Obama to the University of Cairo in June 2009, and on the progress being made by the jihadist conflict and the situation in the jihadist battlegrounds. Conflicts like the one in the Gaza Strip can lead to threats being issued against certain countries. For example, a member of core Al Qaeda, Abu Yahya al-Libi, used the war in Gaza as an opportunity to call for revenge attacks against the United Kingdom in a video released in January 2009.[126] In the video the United Kingdom was held responsible for the fate of the Palestinians due to the historic role which it played in founding the state of Israel. Individual posters may also be used to spread a wide variety of propaganda on, for example, the mother sites.

It is difficult to acquire an overview of how the discourse in the jihadist forums is going to develop and how much value should be attached to it. Do the views or calls for action that are posted come from a single individual, a terrorist group or the entire jihadist movement? Sageman compares this with the discussions between participants at one and the same dinner. They have different discussions among themselves, at different moments in time and in different contexts. The type of discussion depends on numerous factors, including the news of that day. It is difficult to determine how the discussion is going to develop. The same

126 For the latter, see SITE 2009e.

applies to forums. These also have many participants who may be active in all kinds of different forums. A participant in one forum has an influence which is proportional to the number of messages he posts, the level of consistency of these messages with the general discourse in the forum and their added value for the other participants.[127] Another factor which determines the value of a posting is the forum in which it is placed, the number of postings by a particular contributor, the substantiation, the number of responses and the like.

A clear example of propaganda which focused on instilling fear and on influencing an audience are the threatening anti-German videos. Since the end of 2008 jihadists have posted various video messages on the Internet which criticise the presence of German troops in Afghanistan and, at the same time, warn the German people about the consequences. The reasons for the videos may have been the combination - at that time - of three congruent situations: the discussions in Germany about taking prisoners from Guantanamo Bay, the extension to the deployment of German troops in Afghanistan, and the elections being held in Germany in 2009. Jihadists may have wanted to try and influence the elections in Germany by creating a sense of fear.[128] A video message had appeared earlier, in November 2007, in which Germany and Austria were put under pressure to withdraw their troops from Afghanistan. Although there is some doubt about how real the threat referred to in the video messages was, the videos increased the sense of fear. Sometimes the jihadist movement focuses on The Netherlands as well. Both before and after the film Fitna appeared, threats were made on leading jihadist sites in the direction of the leader of a Dutch political party (the PVV party), The Netherlands in general, and the Dutch troops in Afghanistan.

In one specific case, things went beyond the posting of video messages alone. According to the 'Jihadist Brigades to Invade the Internet', one of the threatening video messages directed at Germany was actively sent to more than 40,000 German e-mail addresses. This action accompanied the distribution of that video message to as many German (neutral) sites as possible by the Global Islamic Media Front (GIMF).[129] The sending of jihadist material to citizens enables jihadists to instil fear, because citizens then feel much more personally involved. Incidentally, spam filters usually intercept many of these kinds of messages.

Something that was noticeable in recent years is that jihadists actively respond to news items from Western media for propagandist purposes. This is news which may, for example, help jihadists with their propaganda, or reinforce their morale, which they then distribute via the Internet.[130] For example, jihadists tried to learn lessons from, for example, interviews with American soldiers in Iraq and from the responses following the ultimatum distributed via the Internet to Germany and Austria in March 2007 to withdraw their troops from Afghanistan. They also monitor the counter-initiatives of governments, organisations and leading intellectuals and opinion makers which are intended to counteract the jihadist ideology. For example, the jihadist strategists, opinion makers and commentators monitored the plans of the American government to promote moderate Islam, and the initiatives of Muslim countries such as Saudi-Arabia to combat extremist forms of Islam. At the same time, they attacked new publications by liberal and critical intellectuals and opinion makers. They link the new plans, initiatives and publications to 'conspiracies against Islam and Muslims' and issue appropriate warnings.

127 Sageman 2008a, p. 118-120.
128 This is based on, for example, Hamburger Abendblatt 2009, Welt 2009 and NRC Handelsblad 2009.
129 SITE 2009f.
130 Memri 2007.

Jihadists are on the lookout for supposed affronts to Islam, and they respond in their own forums to relevant news items in Western media. They also try to affect reporting on neutral sites. For example, in the period between July and the beginning of December 2007, a call was posted in a forum of the jihadist al-Ekhlaas website in Arabic six times by different participants to take part in a vote on a proposition on the website of the Dutch Radio 1 programme called 'Stand.nl'. Issues which had to be voted on by jihadists were: the ban on the headscarf in The Netherlands (twice), the ban on the niqab, the banning of the Koran (twice) and a complaint by Muslims about the ban on the Koran. During that period a discussion was taking place in The Netherlands, based on a variety of events, of a number of issues related to Islam. Perhaps people were under the impression that the Dutch government allows its opinion to depend on the outcome of such votes. The people who posted the call probably did not realise sufficiently that the propositions changed every day and that the time difference with The Netherlands can result in the vote being cast on a different proposition than intended. The call therefore came across as amateurish. Nevertheless such calls on an Arabic jihadist website do present a picture of The Netherlands as hostile to Muslims and it also shows that jihadists monitor Western reporting closely. Incidentally, this casuistry also shows that numerous other sites adopt a call on a prominent site and that the original call can then acquire a very different meaning. In fact, incorrect information is distributed on numerous sites to the effect that the Koran was banned in The Netherlands and that the Dutch government had organised a referendum on the matter. In this way, news is "created", namely the supposed ban on the Koran in The Netherlands.

The Israeli Memri institute claimed that considerable numbers of women were being indoctrinated by websites, with regard to making a financial contribution, supporting husbands or children who are prepared to join the jihad, and even with regard to carrying out suicide attacks themselves.[131] The Internet can therefore be used in this way to reach a larger group - a group which would otherwise be difficult for male jihadists to reach - and summon them to participate in the jihad. Sageman refers to the growing role of women in Internet chat rooms.[132]

An unusual form of interactive propaganda came to light at the end of 2007 and beginning of 2008. As Sahab (see paragraph 3.2.2) announced in December 2007 that Al Zawahiri, the second man of core Al Qaeda, would answer questions from Al Qaeda supporters, journalists and critics. In two video messages, of which the first appeared on 2 April and the second on 21 April 2008, he provided hundreds of answers to more than a thousand of the questions posed. He was even prepared to answer controversial questions.[133] A game was also launched in which, among other things, President Bush and the British Prime Minister Blair were attacked for propaganda purposes. The game was what is known as a *first person shooter* entitled *'night of Bush capturing'*, aimed at *'terrorist children'*, with so-called nasheeds (see also 4.4.2.2) as background music.[134]

As mentioned earlier, the propaganda distributed via the Internet has become more professional, uses new applications, is also aimed at a Western audience, and still has a wide reach (see paragraph 3.2). Although different types of propaganda can be distinguished, 'making converts' is a key underlying goal. This propaganda creates a breeding ground for the (additional) radicalisation of individuals and groups (see also paragraph 3.3.3).

131 Memri 2008.
132 Sageman 2008a, p. 111-112.
133 Algemeen Dagblad 2008, International Herald Tribune 2008, Whitlock 2008. The number of answers and questions is taken from the latter source.
134 Jihadwatch 2006.

3.3.2.2 Jihadist/Islamic hacktivism on the rise

Hacktivism has become considerably more widespread since the end of 2006.[135] At the beginning of November 2007, for example, a campaign was announced to disrupt and or deface, from 11 November 2007 onwards, Western, Jewish, Israeli and 'disloyal' Islamic and Shi'iti news, government websites, and websites important for vital infrastructure.[136] So far as is known, the campaign referred to was not carried out but did attract a degree of (media) interest. Hacktivism was certainly prevalent in October and November 2007, in this case carried out by Turkish-speaking hackers. More than five thousand Swedish websites were attacked in a single assault, possibly in connection with the publication of a controversial Mohammed cartoon in a Swedish newspaper.[137]

Islamic or jihadist hacktivism also occurred a several times in The Netherlands as a way of expressing displeasure with situations of (supposed) anti-Islamic expressions and attitudes. From the beginning of February 2008 onwards, hackers have defaced a variety of Dutch websites as a protest against the (then forthcoming) film called Fitna and against Geert Wilders, the Dutch politician behind the film.[138] Measured over a longer period of time, an estimated 20,000 Dutch websites were affected. The altered web pages contain a clear message from the hacker in question, often including a short film or links to other web pages or files. It is therefore not the case that details are stolen, that a website is taken control of or that the website is rendered completely inaccessible. It is also quite straightforward for the owner of the page to rectify a defacement. In view of the larger number of websites affected, the defacements referred to were very probably carried out in an automated fashion.[139] The websites were therefore targeted not because of their specific content, but because they were running on vulnerable servers and because they belonged to the Dutch Internet domain (.nl). The messages consisted of a mix of Dutch, English, Turkish and Arabic texts in a variety of different guises. This is an indication that several hackers (groups) are active, and that the perpetrators probably have different backgrounds. This does not alter the fact that the majority of defacements appear to have been carried out by hackers with Turkish backgrounds.

The question is to what extent the hacker(s) operated purely from an ideological position. Statistics on hacker 'achievements' are maintained on specific websites and the mutual competition certainly plays a role.

3.3.2.3 Assessment of the threat

Various sorts of jihadist propaganda can still be found on the Internet. In particular, three prominent media organisations, namely Al-Fajr, GIMF and As-Sahab, have published a substantial stream of propagandist messages (audio, video and text). Propaganda via the Internet has become more professional, still has considerable reach, and meets with relatively limited resistance. Jihadists are actively trying to engage in interaction with interested parties, in numerous ways. Jihadists also respond actively to news items from Western media for propagandist purposes, are alert to alleged defamations of Islam, and respond in their own forums to related news items from Western media. The likelihood of hacktivism by jihadists will sooner increase than decrease, including in The Netherlands.

135 See also: Rogan & Stenersen 2008.
136 Debka 2007.
137 Nu.nl 2007. On 19 August, the Swedish newspaper, Nerikes Allehanda, published a drawing by the artist Lars Vilks, who had drawn the head of Mohammed on a dog's body.
138 ANP 2008 and Pers 2008.
139 In hacker circles, the defacing of insufficiently secure, vulnerable websites by means of automated scripts is an activity performed by people very low down the pecking order.

It is still the case that the primarily large groups of young people who have access to the Internet and use it intensively, in combination with the propaganda from the jihadist movement, creates a breeding ground for (further) radicalisation. The conclusion is therefore that propaganda via the Internet (still) contributes to radicalisation.

3.3.3 The influence of the Internet on radicalisation: additional or new insights

Although this paragraph focuses primarily on radicalisation, it also examines virtual network formation and recruitment, despite these being dealt with explicitly in other paragraphs. The relevant literature does not always make a distinction, neither can the analytical subdivision always be made in practice.

Sageman examines the influence of the Internet on radicalisation. According to him, within that framework, a distinction needs to be made between the worldwide web, which is a collection of websites that provides users with information, and interactive sites. The worldwide web is in essence passive, and is comparable to traditional media like newspapers and magazines. Users absorb the information offered. The instructional material that can be found on these passive websites played a role, for example, in a number of (thwarted) attacks. Examples are the attacks in Madrid in 2004, the attempt to carry out attacks in trains in Germany using suitcase bombs and the thwarted attacks in London and the failed attack in Glasgow in June 2007. According to Sageman these 'passive' websites are not, however, the motor of radicalisation, given that they only confirm and reinforce certain points of view.[140] In addition, many of the jihadist texts visible on these sites are intellectual in nature, and demand the necessary amount of patience and perseverance to be able to absorb the content.

In addition to passive sites, the Internet also offers many possibilities for communication between individuals and between individuals and groups in the form of, for example, e-mail, forums and chat rooms. This interactivity is revolutionary, and is changing human relationships in a way that we do not yet properly understand. The anonymity of the Internet means people are more likely to drop their guard. Strong ties can be created between people via the Internet, without them really knowing each other in the first instance. Contacts via the Internet can lead to marriages, and there have even been instances of young people using the Internet to agree to commit collective suicide. The downside of this is, of course, that the interaction can be halted at a moment's notice. The lack of politeness and refinement in the communications is also a downside of greater intimacy. This is the consequence of the feeling of anonymity.[141] The in-depth study referred to the issue of trust in addition to the transience of contacts and identities. Can you actually trust virtual contacts in the context of illegal activities?[142]

Dutch PhD research revealed that the Internet offers an easy way to establish new contacts, and that online communication has positive effects on the building of friendships. People disclose more personal information online and put more questions to the people they meet. According to the researcher, it is

140 Sageman 2008a, p. 114.
141 Sageman 2008a, p. 114-115.
142 NCTb 2007, p. 90.

not important whether people can see each other or not (via a webcam). She concludes from this that the above effect is not achieved by the fact that people remain anonymous. Neither is the quality of existing friendships affected by how you got to know each other. The friendships made online and continued later offline are of the same quality as friendships made offline.[143]

The interactivity of the Internet is an important factor as regards radicalisation,[144] and the interactivity of jihadist sites has increased (see paragraph 3.2.2). According to Sageman, Internet forums fulfil the same role as radical mosques in days gone by. Interaction with like-minded people or friends on interactive sites causes people to change their ideas. The interactive discussion and exchange of ideas and views inspire people, and result in radicalisation.[145] The participants get the feeling of being part of a larger community, the Muslim community or Umma.[146] In principle anyone, whether they are a leader, expert or otherwise, can communicate with others on an equal footing. People can themselves start looking for forums in which they can meet others with similar views. They can also avoid forums in which views are aired which they do not like. The interaction with others with similar views gives people the feeling they are not alone. Scarcely any attention is paid to other views, and this serves to reinforce their own personal views. The interaction can also start with a general question, such as 'where can Muslims go on holiday 'safely'?' and can eventually lead to an exchange or the formation of radical points of view. This interactive process can lead to further radicalisation.

- *'[…] the Internet can form an environment in which individuals' commitment to the 'cause', and their concept of what means are justified in defending the Ummah, are exaggerated'.*

The Internet therefore offers the possibility of networking between others with similar views. This brings people into contact with others they would not otherwise have met. In this way, interactive sites can act as a kind of recruitment magnet by which 'seekers' gain access to parts of the jihadist movement.[147] The interactive sites therefore not only influence radicalisation, but also act as a resource for recruitment and virtual network formation.

It is still not entirely clear to what extent - and in precisely what manner - the Internet plays a role in the process of radicalisation, or, for that matter, in the processes of recruitment and virtual network formation, either. However, everyone agrees that the Internet is a key factor. Opinions differ with regard to the degree to which this is the case, certainly in relation to other factors. A relevant illustration of this point is a report by the International Centre for the Study of Radicalisation and Political Violence (ICSR). This report claims that the Internet can play a role in radicalisation and recruitment, but that it is not the primary factor. Radicalisation and recruitment are also rooted in the 'real world'.[148] The argument used in the report - that the influence of the Internet is not dominant - is based primarily on the absence of human contact on the Internet and the need for 'real' social networks and group processes. Nevertheless, in a previous report the ICSR does not rule out the possibility that virtual self-recruitment is taking place, in which the Internet has indeed been the dominant or even the only radicalisation and recruitment factor. Within this

143 Antheunis 2009, UvA 2009.
144 Sageman 2008a, p. 116-117.
145 Sageman 2008a, p. 116-117.
146 Sageman 2008a, p. 116-117, ICSR 2007, p. 51.
147 ICSR 2007, p. 50-52.
148 ICSR 2009.

framework, the ICSR also refers to two examples, namely the Irhabi007 referred to in the in-depth study and this update, and Irfan Raja from Ilford in England.[149]

In the earlier report, the ICSR refers to three ways in which the Internet can support recruitment. First and foremost, the Internet reinforces the ideological message that recruits receive during study sessions. They discover that they are not alone, but are part of a virtual jihadist movement. Secondly the Internet offers the possibility to create networks, as indicated above, and thirdly the Internet can reinforce involvement in the jihad and remove obstacles to involvement. However, the researchers do indicate that *'armchair jihadis'* can still adopt radical points of view without ever having actually to engage in action. On the basis of their research, the researchers believe that the support that Internet provides for recruitment will increase.[150]

The fact that radicalisation and/or recruitment do not occur exclusively via the Internet is shown, for example, by the case of a German convert who is suspected of being the leader of what is known as the Sauerland Group. This group prepared attacks in Germany in 2007, stood trial in mid 2009 and were sentenced in March 2010. The convert in question stated in court that his choice to become a Muslim had been a rational one. He became radicalised after the attacks of 11 September 2001 in the US. He searched the Internet for information on Islam.[151] In the case of what was referred to as the Belgian cell of Al Qaeda, the jihadist site Minbar SOS is thought to have played a role in identifying individuals who are prepared to become involved in the armed struggle with a view to recruiting them physically later on (see paragraph 3.2.5). One of the people arrested by Turkish police in the summer of 2008 is said to have declared that calls to join the jihad were constantly being made on Minbar SOS. The propaganda videos which he saw there were the reason for him to put himself forward.[152]

Europol states that the role of the Internet as regards radicalisation is rarely clear, but that there is no doubt that the Internet has played a role in the radicalisation of suspects identified by criminal investigations in the United Kingdom. Europol has also identified recruitment via the Internet as a source of concern, although it states that the Internet can never replace the personal interaction between potential recruits and the recruiter. On the other hand, Europol makes it clear that a convert in the United Kingdom who had placed a bomb in a restaurant in Southwest England in 2008 had become radicalised independently and was encouraged to act by literature and other material on the Internet. The bomb exploded prematurely and only he himself was hurt.[153]

According to Sageman, the Internet has changed the nature of terrorist interactions. Up until 2004 networks were usually the result of physical interaction between friends. This later changed into interaction via the Internet.[154] Nevertheless, he also states that terrorist networks are a mix of online and offline elements and of virtual and physical networks and mutual contacts.[155]

149 ICSR 2007, p. 50-54.
150 ICSR 2007, p. 50-54.
151 Haegens 2009.
152 Cruickshank 2009a.
153 Europol 2009, p. 17-21.
154 Sageman 2008a, p. 109-110.
155 Sageman 2008a, p. 121.

3.3.3.1 Assessment of the threat

The insights into the influence of the Internet on radicalisation have not changed substantially. A supply is available for each phase of radicalisation. Using the Internet, a potential jihadist can go through the processes of ideology formation, ideology reinforcement and ideological indoctrination. The threat is greater from interactive sites, including social network sites or forums, than from static sites from which, for example, only documents can be downloaded. It is precisely the interactivity of jihadist Internet use that has increased, and with that the influence of the Internet on radicalisation. As a consequence of this increased interactivity, it is becoming more and more difficult to distinguish between propaganda, recruitment, virtual network formation and the influence of Internet use on radicalisation as a whole. The Internet influences radicalisation, but opinions in the literature differ regarding the degree to which the Internet is the only or the deciding factor. The conclusion is still: Internet use supports the entire radicalisation process.

3.3.4 Creation of virtual networks: additional or new insights

Social networking sites such as Facebook and Hyves are popular. Jihadists also use the possibilities offered by social networking sites for the creation and/or maintenance of networks. According to Sageman, terrorist networks are a mix of online and offline elements, and of virtual and physical networks and mutual contacts.[156] As indicated above, a debate is going on about the extent to which radicalisation and recruitment can only occur via the Internet. The same question applies to network formation as well. The fact that interaction via the Internet can contribute to network formation, can be deduced from the fact that, in general, new contacts are easy to establish, friendships can be formed or people can collectively decide to commit suicide via the Internet (see paragraph 3.3.3).

3.3.4.1 Assessment of the threat

It is still likely that the formation of virtual networks can lead to the creation of an informal pool of people who are willing to become involved in the jihad, and who, in varying combinations, are able to devise violent activities with each other or individually. As a consequence, local and international elements can become more interwoven. The conclusion is that the Internet offers possibilities for forming virtual networks, and these increase the jihadist movement's power to act.

3.3.5 Recruitment: additional or new insights

As regards recruitment via the Internet, the picture continues of a permanent and interactive mix of the top-down and bottom-up provision and acquisition of information, mixed with online encouragement, control or network formation. As a result of this, it is not always possible to make a clear distinction between propaganda, radicalisation and recruitment. Neither can a proper distinction always be made between recruitment in the strict sense of the word, conscription or self-recruitment (see also paragraph 3.3.3).

As regards Internet and recruitment, the ICSR states:

- *The Internet has come to play an increasingly important role. The main function is to support 'real-world' recruitment (by reinforcing religious ad political themes; by facilitating networking; and by creating a climate of exaggeration).*

156 Sageman 2008a, p. 121.

In recent years, however, new forms of Islamist militant online activism have emerged, which rely less on human contact and can be described as 'virtual self-recruitment'. [157]

Two examples can illustrate the way in which recruitment takes place. At the time of the repeated publication of the Danish cartoons in September 2007, an appeal was posted for a suicide brigade in a forum of the above-mentioned al-Ekhlaas.

- *'We are registering a suicide brigade here, which is on the way to Denmark (…) I ask you to register your names in order to spread fear among the Danish people and show them how much we love Allah's messenger (…) For me it would be an honour to be the first suicide bomber.'*[158]

Although al-Ekhlaas was a prominent jihadist website, as already mentioned it is by no means always clear how much value should be attached to a posting on a website like this. At the time, the then head of the Danish intelligence service (PET) refused to comment.[159] In addition, this appeal does not appear to be a professional recruitment method, but rather a spontaneous action. Of course, recruiters can also take advantage of this by approaching precisely these people. A second example of 'recruitment' is the supporting role played by the French language jihadist site Minbar-SOS (see paragraph 3.2.5).

Examples of self-recruitment or autonomous radicalisation, also referred to as 'lone wolves', continue to be rare, but they do exist.[160]

The ICSR researchers report that the Internet will become a battleground for European policy-makers with a view to counteracting the growth of militant jihadist recruitment.[161]

3.3.5.1 Assessment of the threat

It is unlikely that someone from The Netherlands can be recruited via the Internet directly and through one-on-one contact by recruiters from international terrorist groups. However, the interactive jihadist sites can provide an ideal recruitment location. After all those sites are visited by people who have a far-reaching interest in the jihad. It is also true that young people feel attracted to scenes of jihadist action and use the Internet to search for a way of getting there. On the Internet, a very interactive form of recruitment has been observed which is strongly linked to interactive propaganda methods. However, due to the diversity in casuistry, no general pattern can be identified other than that recruitment takes place interactively via the Internet and that usually the people involved have presented themselves rather than being recruited in the classical sense of the word. The conclusion is therefore that recruitment via the Internet primarily takes place in an interactive manner.

3.3.6 Acquisition of information: additional or new insights

Numerous applications appear on the Internet offering detailed information. These may, for example, provide information on possible targets, vulnerable locations, people, organisations and security measures.

157 ICSR 2007, p. 55.
158 BBC Monitoring 2007.
159 For the latter, see BBC Monitoring 2007.
160 See, for instance, the examples referred to in US Senate Committee 2008, p. 12-15, ICSR 2007, p. 52-54 and Europol 2009, p. 17-21.
161 ICSR 2007, p. 55.

This paragraph examines a number of applications and the (possible) use of these by jihadists.

The Internet offers more and more possibilities for viewing satellite images and aerial photos of every conceivable location on earth via the computer. Following the example set by Google Earth, Microsoft has also published a maps application known as Microsoft Live Maps (Microsoft Virtual Earth), which is now part of Bing. This application offers more or less the same quality photos as Google Earth and includes a facility for viewing a number of towns and landscapes in three-dimensional form. The number of providers of detailed satellite and aerial photos is increasing all the time. The resolution of satellite images is also continually increasing and the images are updated more often, sometimes to a maximum of four times a year.

Besides satellite and aerial photos, quite a few street level images are also available via the Internet. Using a street view application which is linked to Google Maps it is possible to click a desired location on a map. That location is then portrayed in a panoramic manner (360 degrees). The satellite images and aerial photos are often also linked to other information such as street names, photos and companies or places of interest. Via the site Panaramio, photos of the environment, which Internet users can themselves upload, can be downloaded for each location on a digital map. The possibilities offered by other kinds of photo sites like Flickr, where people can post their everyday photos, are also increasing all the time. For example, Flickr can now paste together photos that have been submitted via the labels which people attach to the photos. In this way three-dimensional walks can be made across, for example, the San Marco Square in Venice and other famous locations. The expectation is, therefore, that, in the future, more and more recent street level image material (photos and videos) will be available on the Internet, coupled to a certain gps location on a digital map. This means that an accurate and recent image can be acquired via the Internet of both the top and the exterior of sensitive objects. Many other details of buildings will become available via the Internet, for example in the form of live images of the breakfast room of a hotel or in the form of government information, such as building permits. This kind of information can also be useful when planning attacks.

A great deal of information about people can also be found on the Internet. Many people have a personal profile on a social networking site such as Hyves, LinkedIn, Facebook or MySpace. In addition, some people also keep blogs or use real time communication sites like twitter. There are also Internet applications which provide information on people's (actual) location. An example is Google Latitude, an application which enables you to track people's movements via the Internet.

The expectation is that the amount of information about people which is available on the Internet will only increase in the future, as well as the accessibility of this information. An example is the recent indexation of Hyves pages via Google. Combining different details generates a sharper image of people and their locations. People provide a great deal of information about themselves but poorly protected computers can be an unintentional and unwanted rich source of information about someone. Personal information on the Internet can be used to prepare for attacks when gathering specific information about, for example, the security of objects and people and about who is involved.

Google Earth is a subject that is being discussed by jihadists. For example, a message was posted in a jihadist forum on 8 March 2007 along with a detailed map of the Abu Graib prison in Iraq. In the message, readers were directed to a website where they can download 'hacks' for Google Earth which would enable them to add operationally-tinged comments and symbols to the satellite maps.[162] It was not the first time that references had been made in jihadist forums to using Google Earth to select Western and Israeli targets and to prepare for trips to jihadist conflict areas.[163] In videos produced by the North African branch of Al Qaeda (AQIM), the group showed how Google Earth had been used to prepare for attacks in Algeria.[164] Members of the Iraqi resistance use Google Earth to carry out attacks on British military bases.[165] The perpetrators of the terrorist activities in Mumbai at the end of 2008 were also said to have used Google Earth images to analyse the target area beforehand.[166] A message was posted on an extremist website in January 2007 with a link to a webcam at an airport in Alaska, which could be operated remotely. Users were able to zoom in on the terminals and the freight areas.[167] There is no evidence as yet that terrorists used street level photos and videos to prepare a terrorist attack. A special form of information gathering is the use of Twitter during attacks. At the time of the attacks in Mumbai at the end of November 2008, the Indian police also warned that the perpetrators had access to information which was important to them about police numbers, people present in the building and the like.[168]

The availability of satellite images, aerial photos and other image material and (or combined with) personal information via the Internet makes it easier for terrorists to prepare attacks. Nevertheless, physical reconnaissance still appears to be essential in order to be properly prepared. After all, images may be outdated, meaning, for example, that recent changes or roadwork are not visible, that issues such as the level of security are often only visible locally, and that the images are insufficiently sharp. Moreover, looking at images via the Internet is different to operating in a hostile and physical environment without getting noticed.[169]

3.3.6.1 Assessment of the threat

Internet applications offer many possibilities for obtaining information, and terrorists are discussing those possibilities or are already using them. The possibilities offered by those applications make it simpler for terrorists to prepare their terrorist actions. The applications provide information in an easy and anonymous way about a certain object, location, organisation or person, and they reduce the need to carry out reconnaissance locally. The information is accessible because organisations or people are insufficiently security conscious, and divulge too much information about themselves and their surroundings online. Nevertheless, some of the information is also available in another way, for example as aerial photos obtained from commercial sources. In addition, physical reconnaissance still appears to be essential in order to be properly prepared. The expectation is that the possibilities for obtaining information will only increase in the future. Moreover, in the future the Internet will be available at even more locations than is currently the case. More than used to be the case, applications for acquiring information via the Internet potentially support the carrying out of terrorist activities.

162 Site 2007c.
163 Site 2007d.
164 Burton 2007b.
165 Daily Telegraph 2007.
166 Blakely 2008, Weizhen & Singh 2008.
167 Canadian Press 2007.
168 Nu.nl 2008, Friesch Dagblad 2008.
169 The comments on the use of virtual applications when preparing attacks come from Burton 2007a, Burton 2007b and Stratfor 2007.

3.3.7 Fundraising

Potentially there are many possibilities for fund-raising by and for jihadists. An initial variant concerns direct and open fund-raising via sites. A second variant involves the use of profiling, e-commerce tools and (online) fraud. A third variant is that of exploitation and improper use of charities. The authors of a great deal of, if not almost all, literature on the use of the Internet by terrorists or jihadists refer to fund-raising. Nevertheless, there are few new examples of fund-raising via the Internet. In Germany, appeals were said to have been made on a site to donate to the jihad that was being carried out by the Taliban. Any amount, no matter how small, was welcome. The primitive site referred to two email addresses from which additional information could be obtained, one for men and one for women. The site was linked to the above-mentioned GIMF.[170] Although Second Life could be misused as a financial money laundering resource (see paragraph 3.2.2), the NCTb is not aware of any examples. The Internet does offer advantages as regards jihadist fund-raising, but also disadvantages. It is still likely that jihadists use the Internet for the three fund-raising possibilities referred to. The possible shift referred to in the in-depth study from more open to more secretive fund-raising does not appear to have taken place.

The expectation is that fund-raising via the Internet may increase as a consequence of new digital and anonymous means of payment. At the end of 2006, the SITE Intelligence Group reported that in the preceding months the use of CashU had been the subject of increasing attention in jihadist forums on the Internet and that there were indications that Iraqi resistance groups are also actually using this resource. As regards other more classical payment and transfer methods, there are many additional ways of ordering goods more or less anonymously via the Internet, or paying for the hire of web space. However, sending goods to a physical address does make them easier to trace. Other actions are also required if the recipients want to spend the money in ways other than via the Internet, and such actions can make it easier to trace transactions. After all, in such cases, money will have to be transferred in cash or from an account. Moreover CashU, for example, requires users to provide personal details, thereby making the transaction no longer anonymous.[171] Fundraising and anonymity are therefore not easy to achieve. In addition, the new payment options are often linked in some way to regular money transfers. There have been no known examples of digital and anonymous means of payment having been used. The expected increase in their use has not, therefore, materialised and, at the moment, there is no reason to assume it will do so either.

3.3.7.1 Assessment of the threat

Potentially there are still a great deal of possibilities for fund-raising by and for jihadists. A number of examples of these variants are known, but are still seldom used in practice. The expected increase in abuse of Internet banking and the expected shift from more public to more secretive fund-raising have failed to materialise. The conclusion is that fund-raising via the Internet by and for jihadists (still) only takes place on a limited scale.

3.3.8 Training: additional or new insights

Many people have indicated that the Internet has assumed, or was able to assume, the role of physical training camps. In the meantime it has become clear that the jihadist movement is still keen to use physical training camps, and that these exist primarily in the border area of Afghanistan and Pakistan, and

170 Example from BBC Monitoring 2008.
171 For the latter, see Katz & Devon 2006, Holahan 2006.

in Somalia. Those training camps are also still attended by people from, for example, Europe, the US and Australia.

Rogan and Stenersen argue that there is an abundance of military and tactical training handbooks on jihadist web pages. Handbooks can be found on almost all subjects which might be relevant for training and preparation purposes. The sources vary from English language open sources to material from experienced jihadist commanders or trainers. Around fifty Arabic instruction videos are also circulating on all kinds of jihadist sites. Approximately twenty of these are of a high quality. These videos have been made by the Lebanese Hezbollah, who are strictly speaking not the jihadist movement (see Annex 1). In the midst of a large quantity of material it is difficult to find material which is of a high quality. The training materials usually originate from lower down the scale much sooner than from the top. In other words, the material is not really from core Al Qaeda.[172]

Besides being a source of training material, the Internet also acts as a kind of classroom. Interested parties can discuss training-related issues, exchange personal experiences and communicate with virtual trainers who can explain and clarify problematic subjects. However, the jihadist forums are an arena for beginners and trainee jihadists. They are not an instrument which experienced jihadist groups can use to distribute the latest insights on a large scale. They are aware of the fact that such forums are closely monitored by numerous intelligence organisations worldwide. The Internet is therefore more of a library or classroom for the jihad than the jihad university frequently often referred to. This does not alter the fact that more up-to-date and advanced training material can be exchanged outside the public part of the Internet, for example using e-mail.[173]

The fact that publicly available training material is not always of a high quality, is no guarantee of success or can lead to dangerous situations, is demonstrated by the following case. On 31 July 2006, two Lebanese men tried to blow up two regional trains in Germany using explosives they had made using an online handbook. However, the suitcase bombs failed to go off because the perpetrators had deviated from some of the instructions in the handbook.[174] Just as the online acquisition of information cannot take the place of a physical investigation, online training cannot fully replace physical training. Reading about how to operate in a hostile environment is very different to actually doing it. The experience of teachers is also important.

Nevertheless, the material can help to make the process of radicalisation and terrorist actions more accessible, certainly if real training in a camp is not feasible. The material also contributes to the jihadist macho culture which can be attractive to young people. It can also help with the preparations required before trainee jihadists leave for training camps or conflict areas.[175] However, there has been no known confirmed case of a successful attack being carried out using online training material alone,[176] although material was used in the case of the failed attack in Germany and the same can be assumed to apply to a case in the United Kingdom in 2008.

172 Rogan & Stenersen 2008.
173 Rogan & Stenersen 2008 and Europol 2009, p. 21.
174 ANP 2006 and Schofield 2007.
175 Jane's Terrorism and Security Monitor 2008, Europol 2009, p. 21.
176 Jane's Terrorism and Security Monitor 2008, Rogan & Stenersen 2008.

Every now and again messages appear that claim that online games can be used for jihadist training purposes. However, there is no known example of terrorists or jihadists actually having concocted attacks in virtual 'game worlds'.[177] Of course, games can provide insight to a certain extent in certain tactics which lead to success in the game. However, the reality value of this for real attacks is debatable. Nevertheless, it is a fact that in July 2009 a forum member of an English language jihadist website advocated the use of realistic video games, such as Battlefield 2, as a good way of preparing for the jihad. Others responded with additional suggestions or questions. However, some disagreed, claiming that physical activities are a better preparation.[178]

3.3.8.1 Assessment of the threat

The fact that the Internet can take over the role of physical training camps has now been shown to be misplaced by the practical reality of the existence of numerous physical jihadist training camps, to which, moreover, people (are) still (trying to) travel. The Internet is sooner a library of training material and, to a certain extent, a virtual classroom for budding jihadists. Someone still has to be able to understand the instructions or manuals properly themselves and then practise, apply and execute what is in them. In addition, the discipline required to carry out a large-scale attack can be developed much more effectively in an actual training camp. The 'ease of use' and safety of certain instructions can certainly be questioned. Nevertheless, the training material and the sites where experiences and insights are shared are not harmless. They can be used, certainly by home-grown terrorists, and thereby lower the threshold with regard to carrying out attacks. The conclusion is that use of the Internet for training purposes (still) lowers the threshold when it comes to carrying out attacks, but that physical training and training camps pose a greater danger.

3.3.9 Mutual communication and planning: additional or new insights

An indication that the Internet can be used for operational communication is shown by, for example, the fact that a terrorist wearing a bomb belt blew himself up in an Internet café in Casablanca. According to reports he had wanted to receive the necessary instructions there for a series of (suicide) attacks via the Internet. When this did not work out, and after the owner of the café had called the police, he blew himself up.[179] According to open sources the husband of Malika el-Aroud reportedly maintained contacts from the border area of Afghanistan and Pakistan with his wife by e-mail and Skype, a form of Internet telephony. He also placed postings on the jihadist site Minbar SOS (see also paragraph 3.2.5). In 2008, the jihadist website al-Ekhlaas made the encryption software 'Mujahideen Secrets 2' available which can also be used to encrypt chats.[180] Chats are, of course, more suitable for operational communication than websites.

According to media reports, the perpetrators of the attacks in Mumbai at the end of November 2008 used VoIP (voice over IP telephony via the Internet) to communicate with their leaders in Pakistan and to receive specific instructions. As such, there is of course no difference between this method and, for example, communication via mobile telephones, although VoIP is more difficult for some countries to monitor.[181] Incidentally, the Indian police were said to have been able to trace no fewer than ten IP addresses with the help of the FBI. Five of these came from what is referred to as a proxy, which means the IP address is ultimately untraceable. Five addresses were traceable.[182] Nevertheless it is far from likely that members of core Al Qaeda communicate via the Internet. For them the risk is great.

3.3.9.1 Assessment of the threat

It is very likely that jihadists still use the Internet to communicate with each other. Logically, this will largely take place in a protected manner. Strictly speaking it does not make any difference to the threat whether jihadists communicate by telephone or via the Internet. As is the case with other means of communication, intelligence bodies and the police can also intercept Internet traffic. Jihadists are aware of this and warn each other accordingly. The conclusion is that jihadists (still) use the Internet to communicate with each other and plan.

3.4 Concluding observations

Jihadists still make extensive use of the Internet as a resource. In line with the general use of the Internet and the emergence of web 2.0, jihadist use has become more interactive. That increased interactivity makes it easier to spread propaganda, set up networks and 'recruit', and to communicate and plan with each other. As a consequence of the interactivity, the effect on radicalisation of Internet use by jihadists is greater, certainly as regards propaganda. Nevertheless, the extent of this influence is still unclear. Is it *a* factor or is it *the* factor? It can be concluded that the use of the Internet as interactive means of communication constitutes a threat.

In addition, the fact that the Internet fulfils a supporting role for jihadists as regards (the preparation of) terrorist activities also constitutes a threat. Besides fund-raising and communication and mutual planning, that threat is primarily the result of using the Internet to create virtual networks, acquiring information and for training purposes. However, the Internet cannot fulfil the same role as training camps, and that means that camps are a greater danger. Neither is the Internet a replacement for physical reconnaissance.

It can be concluded that the Internet is, and will continue to be, a crucial resource for the jihadist movement.

177 Shachtman 2008.
178 SITE 2009g.
179 AFP 2007.
180 Webwereld 2008a.
181 Business Line 2009.
182 United News of India 2009, Times of India 2009.

4 Jihadism on the Dutch Internet

4.1 Introduction

The in-depth study included an overview of the manifestation of jihadist expressions on the Dutch Internet. With regard to Dutch jihadist websites, it transpired that there are three, partially overlapping, categories which can also be regarded as periods:

- foreign-oriented jihadist sites in The Netherlands (2000 - 2001);
- Dutch jihadist sites with a foreign orientation (2002);
- Dutch jihadist sites focused on The Netherlands (2003 - 2006).

Dutch jihadists focused primarily on the ordering, offering and distributing of jihadist information and material, often via free websites, such as tk.domains, geocities and freewebs. This information concerned, among other things, literature translated into Dutch about the waging of the violent jihadist conflict, statements by Al Qaeda, and the required way of dealing with 'unbelievers' (non-Muslims). These websites are characterised as jihadist 'material websites'. The use of free web space appeared to be attractive because it scarcely required any registration and administration, and offered anonymity. In the period 2003 to 2005, Microsoft Network (MSN) groups appeared to be very popular among jihadists. As regards content, the various MSN groups and sites focused on both the theoretical and dogmatic aspects, and on the practical and operational aspects of the jihadist conflict. The jihadist MSN groups were mainly popular among young people, including members of the Hofstad Network. The MSN groups, often with explicitly jihadist names, disappeared for a short period only to reappear elsewhere under a new name and with a new look. After developments that included media reports that MSN contained a great many jihadist messages, the administrators of MSN communities decided to close the jihadist MSN groups in question.[183] Once that had been done, more or less all the jihadist material disappeared from MSN.

The jihadist information offered via the different sites was used primarily for propaganda purposes. It turned out to be possible to trace these expressions of virtual jihadism and the related discussions to jihadist websites and to some neutral web forums. It also transpired that it was primarily Muslim women who had a key share in the translation and distribution of jihadist material on the Internet.

At the time, the online activities also appeared to link up with an active period of local autonomous jihadist networks in The Netherlands. Recent editions of the Terrorist Threat Assessment Netherlands *[Dreigingsbeeld Terrorisme Nederland]* (DTN) show that the local autonomous jihadist networks in The Netherlands have lost strength and become less active in recent years[184] It also applies that the attention of these people is now focused on the activities in classic jihadist conflict areas and not on terrorist activities in The Netherlands. This chapter examines whether these changes also occurred within the jihadist movement in The Netherlands after 2006 in the context of jihadism on the Dutch Internet.
It is important to emphasise that Dutch jihadists can, of course, also use Arabic and/or English language jihad websites, but that this falls outside the scope of this chapter. This chapter also analyses whether any changes regarding jihadism on the Dutch Internet have consequences for the jihadist threat against The Netherlands or Dutch interests.

183 Novatv.nl.
184 NCTb 2009.

4.2 Dutch jihadist sites since 2006

4.2.1 The growth in the number of jihadist 'material sites' has stagnated since 2006

Many of the jihadist material sites referred to under 4.1 have now disappeared or have not, or have scarcely, been supplemented with new (jihadist) material. The websites that did remain operational therefore have largely the same appearance as three years ago. A few new jihadist material sites have appeared. The material offered is a mixture of translated literature by radical ideologists on the one hand and home-grown Dutch material on the other. Most of the jihadist texts on the jihadist material sites are not very accessible, and assume that the reader has some prior knowledge of jihadist ideology. It is therefore difficult to make exact statements about the reach of the jihadist material sites, partly because these sites have no communication functionalities (such as a forum) from which conclusions can be drawn about the responses made.
However, the static, one-sided way in which jihadist material is offered no longer seems to fit in with the current Internet trend Web 2.0, whereby the emphasis is on the interactivity between *content* provider and user.

4.2.2 Few activities on weblog sites

The use by jihadists of (free) weblog sites on which an author can post a message (blog) to which readers can then respond, has continued to a limited degree in recent years. The blog contributions are often shorter and more personal in comparison with the long jihadist articles posted on the above-mentioned material sites. Despite the fact that it is technically possible to respond to the jihadist messages posted, this rarely happens. Jihadist-oriented blog sites often include various hyperlinks to similar websites, meaning that users can quickly consult a substantial part of the Dutch jihadist material online. This creates what is referred to as a 'snowball effect' for those with jihadist interests. Nevertheless, the number of such Dutch 'jihad blogs' continues to be limited to around five.

4.2.3 Thabaat.net (2007-2009): the professionalisation, isolation and internationalisation of jihadism

Besides the above-mentioned free jihadist websites, there have also been two new jihadist websites since 2006 with their own domain name, including Thabaat.net which has already been offline for some time now. The servers of the two websites were located abroad. The Thabaat server was in the United States, possibly due to the less strict legislation and regulations that apply as regards Internet postings.

In June 2007, the professionally designed website www.thabaat.net was set up and registered in Brussels. It was used to post numerous videos produced by the main jihadist media organisations (see 3.2.1). In April 2009, the website has a total of 286 registered forum members, including user name and password, who engaged in various discussions in the web forum regarding the desirability of the violent jihad and related political-religious issues. Current issues were dealt with in the 'Ummah News' section. This made Thabaat.net the only large-scale interactive Dutch jihadist web forum. According to the Internet tool Statbrain.com, the website was visited by an average of 1,300 visitors per day up to that moment. Despite its professional design, the website turned out to be offline much of the time, for example in periods in 2007 and 2008. The website has been offline - perhaps definitively - since May 2009. In the Spring of 2009 a Thabaat.net administrator declared on the forum that 'Jews and non-believers were carrying out [digital] attacks on the website.' Whatever may have been the case, this long-term offline status brought about an abrupt interruption to the jihadist discourse on the Dutch Internet.

A striking detail is that the English language website Revolution.thabaat.net, subtitled 'The ignored puzzle pieces of knowledge' was also being maintained from the same IP-address. From December 2007 onwards, the website in blog format was supplemented on an almost daily basis with jihadist topics, including messages of admiration for mujahadeen fighters in Pakistan, Al Qaeda and the introduction of the sharia. The design and content of this international version of Thabaat was very similar to other English language jihadist websites, meaning that the latter may have been used as a source of inspiration. The fact that Revolution.thabaat also attracted the attention of other leading English language jihad sites, was apparent from the various hyperlinks on these sites which refer to Revolution.thabaat. Revolution.thabaat shared the same IP address as Thabaat.net and has therefore also been offline since May 2009.

4.2.4 New jihadist website: centralisation of jihadist information

A few months after Thabaat.net had disappeared from the web, a new Dutch jihad website was set up. The emphasis of the new website is primarily on providing jihadist literature and videos that have been translated into Dutch, some of which date from the period 2004-2007. Only a very limited number of communication facilities for the website visitors are offered, as was the case at the time on Thabaat.
The goal of the website administrators appears primarily to be to combine all Dutch jihadist information and offer it at a central location. As in the case of Thabaat, the information focuses primarily on the foreign jihadist conflict areas.

4.3 Jihadism on Salafist sites

In contrast to the limited number of jihadist websites on the Dutch Internet, the number of Salafist websites on the Dutch Internet increased in the period 2006-2009. A critical examination of the Salafist websites present in The Netherlands reveals that, in the first place, the websites have an ultra-orthodox religious orientation, with a focus on gathering knowledge on the Salafist aqiedah (religious doctrine) and manhadj (religious methodology). No sections relating to (violent) jihad have been found on known Salafist websites. Leading Salafist scholars and imams also speak out against jihadist ideology via online sermons. However, a number of jihadist forum members appear to be active on the most important Salafist-oriented web forum Ansaar.nl, although they are in the minority by a long way. In some cases they post translated jihadist articles like the article entitled '44 ways to carry out the jihad' by the radical American-Yemeni spiritual leader Anwar al-Awlaki, or issue death wishes and threats to people who are said to have insulted Islam. In general such comments result in heated internal Salafist discussions on the different meanings of the jihad, for which there are also non-violent interpretations.

4.4 Jihadism on Islamic mainstream sites since 2006

4.4.1 A decrease in jihadist expressions on Islamic mainstream sites

In the period 2004-2007, a large number of jihadists were active on Marokko.nl, the largest Islamic young people's website in The Netherlands. Forum members with jihadist online pseudonyms post appeals both in the news section and the 'Islam and me' subforum to join the violent jihad and (translated) jihadist propaganda was frequently distributed. As a result, many unsuspecting visitors came into contact with jihadist ideology. However, the number of jihadist expressions has decreased sharply since 2007. There are probably a number of reasons for this. Firstly the moderation policy on the website has increased and improved. If detected, radical expressions are removed faster than used to be the case. Secondly, the number of Islamic critics on Marokkko.nl has increased. The consequence of this is that Islam is criticised

during many discussions and this has, in turn, probably been the reason why jihadists no longer actively engage in the discussions. Thirdly, jihadists now realise that investigation services are monitoring what is being said, and this has resulted in jihadist intentions being communicated less openly.

Incidentally this does not mean that jihadists no longer try at all to disseminate their ideas via Marokko.nl. For example, in June 2008, a message was posted on Marokko.nl about the launching of the Dutch branch of a jihadist radio station, known as Sana-Al-Islaam, which could be listened to in Dutch via Profilepitstop.com. The posting included information to the effect that the broadcaster belonged to the 'Qaidat al-Tawheed and Al-Jihaad' organisation.[185] This forum contribution appealed to readers to distribute the hyperlink on other web forums. Incidentally, the Dutch online jihadist radio station Sana turned out to be no more than a short-lived phenomenon and had vanished without trace by mid 2009.

Maroc.nl, as well, has not had to deal with any, or scarcely any, jihadist messages posted by forum members. Islamic forum members on this website speak out explicitly against violent interpretations of Islam, and there is criticism of, for example, terrorist attacks in name of Islam by Al Qaeda.

4.4.2 Jihadism on neutral websites since 2006

4.4.2.1 Hyves.nl does not appear to be popular among jihadists in The Netherlands

It is conceivable that Hyves.nl can be a suitable resource for jihadists within the framework of propaganda or communication between jihadists themselves. However, hardly any jihad-related material can be traced on Hyves. Neither does Hyves.nl appear to be a suitable means of communication between jihadists themselves. This is presumably due to the very public character of Hyves.nl which makes it difficult to communicate anonymously. It is easy for investigation and security services to monitor. Moreover, Hyves.nl is actively moderated, meaning that unwelcome material can quickly be removed from the website.

4.4.2.2 YouTube sometimes used by Dutch jihadists as a means of propaganda

Jihadist image and sound material in Dutch or with Dutch subtitles has also been found on YouTube. A number of jihadist videos with Dutch subtitles were originally found on international jihadist websites, including translated propaganda films by Al Shabaab, the radical-Islamic movement from Somalia.

A unusual phenomenon, which has been apparent since the end of 2008, is that a number of clips of jihadist nasheeds (Islamic non-instrumental songs) in Dutch have been posted on YouTube. These nasheeds include the full text of Al Qaeda's ideological-political theories, including those relating to the 'occupation by the Americans of the sacred Saudi-Arabia'. Perceived evils are also supplemented with images and numbers of Muslim dead caused by the West's actions in Afghanistan, Iraq, Chechnya and Palestine. The purport of the songs is that Muslims must rebel against the oppression by the West (referred to as 'apes and pigs' and the 'Jews and crusaders'). At the same time, the majority of the ummah are said to have been perverted by worldly (dounia) matters. Jihadists are portrayed as an advance-guard movement which is actively fighting for the superior honour and glory of Islam against the 'unbelieving invading armies' in the jihadist theatre of conflict of Afghanistan. These elements are interspersed in a technically skilful way with dramatic video images of mujahadeen fighters in desolate areas, presumably in Afghanistan.

It appears that such jihadist nasheeds on YouTube have been viewed thousands of times and have often been greeted with positive comments. Only a few of the readers who have responded on these web locations were critical about the violent, jihadist message. The musical adulation of the jihad in The Netherlands appears to be a jihadist tactic designed to appeal to Islamic young people in The Netherlands who do not all have a command of standard Arabic. Jihadist songs and videos appear to reach more people than the above-mentioned, 'dry' ideological-religious articles on the jihadist material sites. The traditional Islamic background to the nasheed can also be regarded, from the perspective of jihadist ideology, as a legitimate means of communication. What is more, the videos show that the interest of the video makers is directed primarily at the classic jihadist conflict areas in the world and not The Netherlands. This 'international outlook' in the virtual world corresponds to the conclusions about the primarily international orientation of Dutch jihadists in the physical world.[186] First and foremost, the material is related to jihadist propaganda. No instructions about recruitment or handbooks for making weapons can be found on YouTube. Moreover, the quantitative scope of these Dutch, jihadist propaganda films is not that great, and remains limited to less than ten.

4.4.2.3 MSN groups not used by jihadists since 2006

As of February 2009, the services of MSN have been taken over by Multiply (suitable for large groups) and Windows Live Groups (suitable for groups of up to a thousand people). No explicit jihadist activities of a Dutch nature appear to have taken place on these sites. Neither does there appear to be (much) discussion about the desirability and/or need for a violent jihadist conflict in other discussion groups such as Yahoo and Google.

4.5 Conclusions and threat implications

Jihadist expressions can still be found on the Dutch Internet, but their number has decreased since 2006. This can probably be explained by the active moderation policy pursued by the administrators on the mainstream sites, the decrease in the activities of local autonomous jihadist networks in The Netherlands itself, and the increased security awareness among jihadists that they are being monitored by investigation agencies and security services in The Netherlands. Nevertheless, jihadist material in Dutch is still available on the Dutch web. In addition, since 2006, a number of jihadist websites appear to have repeatedly had technical problems and have been frequently offline.

As was also observed in 2006, Dutch online jihadism is aimed almost entirely at spreading propaganda. The propaganda on the Dutch Internet varies considerably as regards content and style. On static websites, (translated) jihadist literature can still be found, with some of this dating from the time of the Hofstad Network. This literature, by leading international jihadists, legitimises the violent jihad. In addition, there are more modern, Web 2.0 based interactive knowledge exchanges on the jihad. In comparison with the situation in 2006, interactive knowledge exchanges are increasingly taking place in isolation, and sometimes via protected websites (requiring user names and passwords) and, to a lesser extent, in neutral

185 'Qaidat al-Tawheed and Al-Jihaad' (also known as Al Qaeda in Iraq) was a jihadist terrorist organisation in Iraq led by Al Zarqawi. The organisation is now part of the umbrella organisation called the 'Islamic State of Iraq'.

186 NCTb 2009.

web forums. The jihadist songs on YouTube primarily try to stir up a feeling of anger against the West among Muslims, and to incite them to take action. In addition, these nasheeds project a romantic image of the violent jihad.

The jihadist focus on the Dutch Internet is mainly on international aspects of the jihad, namely the traditional conflict areas in Afghanistan and Pakistan, as well as - and this is relatively new - Somalia. No examples have been observed on the Dutch Internet of direct recruitment and/or the distribution of (Dutch) manuals on explosives and the use of weapons. Of course it is perfectly possible that direct recruitment is taking place outside the public Internet.

The observation that the extent of jihadist propaganda on Islamic (mainstream) web forums has decreased, means in theory that in 2009 fewer people came into contact with jihadist ideology online than in 2006. The chance of radicalisation using jihadist websites therefore appears to have decreased. The criticism of the violent jihad which is often expressed on Salafist websites can have positive effects in the medium to long term.

Of course, as mentioned in the introduction, jihadist information can also be obtained from Arabic and/or English language jihad websites. However, anyone who wants actually to acquire knowledge about the violent jihad can still find enough material on the Dutch web. Another source of concern are the various positive responses observed in connection with the Dutch *nasheeds* on YouTube. There still appears to be interest among certain sections of the Dutch population for the violent jihadist message.
The fact that various individuals in The Netherlands are still active, possibly in groups, with online propaganda related to the violent jihad, means that it is conceivable that certain people are becoming (more) radicalised.

Annex

Jihadism, jihadist movement, jihadist terrorism and online jihadism

Islam has become an increasingly important political factor in many Muslim countries in recent decades. Numerous political parties and movements derive their goals and activities from Islam. Within that framework people refer to 'political Islam' or 'Islamism'. Islamism can be both Sunni or Shiite in nature. Salafism and jihadism, two movements within Islamism, are Sunni, as are the Muslim Brothers, the Hizb-u Tahrir (HuT)[187] and Hamas. Hezbollah is Shiite.

Within Islamism, a distinction can also be made in the way in which changes are aimed for: through either violent or non-violent means. A characteristic of the non-violent movement is that it does not practice or advocate violence to achieve the realisation of the intended changes. Jihadism falls under 'violent Islamism'.

Jihadism is made up of extremist and violent elements of primarily the Salafist doctrine (see List of Terms) and the ideas of Sayyid Qutb, the most important ideologist of the Muslim Brothers. Jihadism regards the armed struggle, which is defined as jihad, as the ultimate means for achieving a global dominion of Islam and the re-establishment of the Islamic State. The point of departure for this endeavour is the jihadist interpretation of the model of the Prophet's religious community. 'Jihadism', like 'jihadist', is therefore derived from the term 'jihad'. The term 'jihad' in Islam, however, is a complex and wide-ranging term which also has an explicit spiritual and 'peaceful' meaning (see List of Terms). Whenever one talks of jihadism or jihadist, this always means jihad in the sense of an armed struggle, also referred to as 'small jihad' or 'holy war' by some. This means jihad by individuals, groups and freedom fighters and not by countries.

Although in the case of the term 'jihadists' the accent is on the actors who make up the jihadist movement, when using the term 'jihadist movement' the accent is on the collectivity of those actors.

The element of 'movement' can be stated specifically as being the entirety of networks, groups, cells and individuals with similar views and goals. It should be noted that there is no homogenous whole in this case; within the jihadist movement there are differences of opinion regarding certain issues, and other differences. Neither is there any central control or authority. Nevertheless, a movement does exist, which is bound together by ideology. It can be compared to the Communist movement, within which there were also differences of opinion, trends (and the like) and no global control and authority. Al Qaeda fulfils a key role within the jihadist movement. A distinction is also made between 'core Al Qaeda', 'Al Qaeda related' and 'Al Qaeda inspired' (see List of Terms).

'Jihadism' can be described as a movement within political Islam whose aim, based on a specific interpretation of the Salafist teachings and the body of thoughts of Sayyid Qutb, is to achieve global dominance of Islam by means of an armed struggle (jihad) and the re-establishment of the Islamic State (Caliphate).

187 The HuT is a political-activist group that operates worldwide. The ideology is focused on the (re) establishment of a Caliphate state, run according to the rules of the shari'a.

On the basis of the combination with the definition of jihadism, the definition of jihadist terrorism is then as follows:

- Jihadist terrorism is terrorism based on jihadist goals. A feature of this category of terrorism is:
- The use of the term jihad for the threat of, preparation of or perpetrating of serious violence against people, or deeds aimed at causing socially-disruptive material damage.
- The carrying out of activities which are commensurate with the aim of achieving global dominion of Islam and the re-establishment of the Islamic State.

Criteria for online jihadism

A site is labelled as jihadist if it preaches and spreads jihadism by means of articles, audiovisual documents, postings and other Internet functionalities (mailing list, chat or Paltalk room).

The jihadist ideology consists of a mix of closely related theological, dogmatic, liturgical, ethical, legal and political terms or doctrines. They can be classified as follows:

1) The oneness of God [Tawhied].
2) Belief and unbelief [Imaan and Kufr].
3) Worshipping God [Ibada].
4) The duty to apply divine legislation and regulations [al-Hukm bi-ma Anzala Allah].
5) Loyalty and disownment [al-Walaa wa al-Baraa].
6) The community of Muslims [Jamaat al-Muslimin].
7) The preaching and missionary work [ad-Da'wa].
8) The armed struggle [al-Jihad].
9) Re-establishment of the Islamic State (Caliphate).

The first eight terms correspond to the key notions of Salafism. Jihad, within the meaning of armed struggle, ensues in both Salafism and in jihadism from all the key terms/doctrines. However, jihadism assigns a radical and activistic clarification to those terms and links them to activistic consequences. In addition, jihadism broadens the circumstances in which jihad may or must be carried out and ignores certain limitations.

Jihadism has four main themes, namely the end time, the global dominion of Islam, the re-establishment of the Islamic State and, last of all, dawa and jihad carried out by the vanguard, as a means to achieve these goals. The end time, which means the end of the world and the subsequent 'day of judgement', is the ultimate goal. Prior to that, the aim of jihadism is to achieve global dominion of Islam and the re-establishment of the Islamic State. Dawa and jihad by the vanguard, meaning jihadists, is the only suitable means to achieve these goals. Dawa has to be based on jihad, and Hijra[187] - by analogy with the journey the prophet Mohammed undertook from Mekka to Medina - constitutes a link between dawa and jihad. Jihadists reject everything that contradicts those ideals.

Additional background information on jihadism can be found in: Ideology and strategy of Jihadism, National Coordinator for Counterterrorism, December 2009.

187 Hijra means emigration or departure from a country and settlement in another country for religious and political reasons, but also a temporary or permanent establishment in a country to which Muslims have moved to.

Bibliography

AFP 2007
'Suicide attack in Casablanca kills bomber, wounds three', AFP, 11 March 2007.

AFP 2009
'US security braced for 'cybergeddon', AFP, 7 January 2009.

Agence 2009
'Singapore - Backroom cyber warriors trawl web for extremist threats', Agence France Press, 16 August 2009.

Algemeen Dagblad 2008
'Al-Qaeda houdt 'spreekuur' en beantwoordt 100 vragen', Algemeen Dagblad, 24 April 2008.

ANP 2006
'Mohammed-spotprenten motief voor kofferbommen', ANP, 2 September 2006.

ANP 2008
'Website Willem II gekraakt tegen Wilders', ANP, 1 February 2008.

Antheunis 2009
M.L. Antheunis, *Online Communication, Interpersonal Attraction, and Friendship Formation*, Amsterdam 2009 (http://dare.uva.nl/document/129138).

Australian Financial Review 2007
'Media proves a powerful vehicle for terrorists', Australian Financial Review, 22 March 2007.

Automatiseringsgids 2007
'DoS-aanvallen gevaar voor internet',Automatiseringsgids, 26 September 2007.

Automatiseringsgids 2009a
'Beveiliging kern internet vertraagd', Thijs Doorenbosch, Automatiseringsgids, 12 October 2009.

Automatiseringsgids 2009b
'Angst in VS voor stralingswapens', Automatiseringsgids, 19 August 2009.

BBC Monitoring 2007
'Website linked to al-Qa'idah reported seeking suicide bombers to attack Denmark', BBC Monitoring, 22 September 2007.

BBC Monitoring 2008
'German paper says Islamists collecting Internet donations', BBC Monitoring, 11 April 2008.

Blakely 2008
R. Blakely, *'Google Earth accused of aiding terrorists'*, Times Online, 9 December 2008 (http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5311241.ece).

Burton 2007a
F. Burton, *'The Secrets of Countersurveillance'*, Stratfor, 6 June 2007.

Burton 2007b
F. Burton, *'Surveillance in the Information Age'*, Stratfor, 14 June 2007.

Business Line 2009
'E-World falling short on security', Business Line, 12 January 2009.

Buxbaum 2008
Peter Buxbaum, *'Cyberterrorism, Inc.'*, ISN Security Watch, 11 Februay 2008.

Canadian Press 2007
'Terrorists eyeing webcams as means to assess vulnerabilities, says FBI', Canadian Press, 11 January 2007.

Chen e.a. 2008
Hsinchun Chen, Sven Thoms, T. J. Fu, *'Cyber Extremism in Web 2.0: An Exploratory Study of International Jihadist Groups (Forthcoming, IEEE International Conference on Intelligence and Security Informatics)'*, 2008.

Cheong 2008
Lee Kwok Cheong, *'Must we wait for crisis to strike?'*, Business Times Singapore, 14 July 2008.

Cochran 2007a
A. Cochran, *MetaTerror: The Potential use of MMORPGs by Terrorists*, Counterterrorism Blog (http://counterterrorismblog.org/2007/03/print/metaterror_the_potential_urse_0.php)

Cochran 2007b
A. Cochran, Part II of "*MetaTerror: The Potential use of MMORPGs by Terrorists*, Counterterrorism Blog (http://counterterrorismblog.org/2007/03/print/part_ii_of_metaterror_the_pote.php)

Computerworld 2008
'CIA says hackers pulled plug on power grid', Computer-World/ IDG News Service, 18 January 2008.

Council of Europe 2007
Council of Europe, *'Cyberterrorism - the use of the internet for terrorist purposes'*, Council of Europe Publishing, December 2007.

CRS2008
CRS Report for Congress, *'Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress (update)'*, 29 January 2008.

Cruickshank 2009a
P. Cruickshank, *'The Belgium Cell and FATA's Terrorist Pipeline'*, CTC Sentinel, volume 2, issue 4, April 2009.

Cruickshank 2009b
P. Cruickshank, *'Italy arrests linked to Brussels 'al Qaeda' recruiting network'*, CNN, 15 May 2009.

Cruickshank 2009c
P. Cruickshank, *'Love in the Time of Terror'*, Marie Claire (updated 18 May 2009) (www.marieclaire.com/print-this/world-reports/news/interntional/malika-el-aroud...)

Daily Telegraph 2007
'Terrorists 'use Google maps to hit UK troops'', Daily Telegraph, 13 January 2007.

Debka 2007
'Al Qaeda declares Cyber Jihad on the West', Debka.com, 7 November 2007.

Denning 2007
Dorothy E. Denning, *A View of Cyberterrorism Five Years Later*, in Internet Security: Hacking, Counterhacking and Society, K. Himma ed., Jones and Bartlett Publishers, 2007.

District Court 2009
Indictment 'Unauthorized Impairment Of a Protected Computer', US District Court for the Central District of California, February 2009.

EETimes 2009
Rick Merrit, *'Congress debates how to holster RF weapons, Electromagnetic pulse attacks: impact high, probability low'*, EETimes.com, 25 August 2009.

Elsevier 2009
'Terroristen prediken terreur op Facebook', Elsevier.nl, 17 March 2009.

Europol 2009
TE-SAT 2009, EU terrorism situation and trend report, Europol, 2009.

Forbes 2007
Andy Greenberg, *'America's Hackable Backbone'*, http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html, 22 August 2007.

Foxnews 2008
'How to Hack Into a Boeing 787', Foxnews.com, 18 February 2008.

Friesch Dagblad 2008
'Twitter eerste bron bij terreur', Friesch Dagblad, 1 December 2008.

Global Risks 2008
Global Risks 2008, A Global Risk Network Report, World Economic Forum, January 2008.

GOVCERT 2008
Trendrapport 2008, GOVCERT.NL, June 2008.

GOVCERT 2009
Trendrapport 2009, GOVCERT.NL, June 2009.

Graham 2004
Dr. William R. Graham et al, *'Report of the Commission to Assess the Threat to the United States from Electromagnetic pulse (EMP) Attack'*, Volume 1, Executive Report, 2004.

Haegens 2009
K. Haegens, *'Hoe Fritzi Abdullah werd'*, De Groene Amsterdammer, 19 August 2009.

Hamburger Abendblatt 2009
'Videos: Terroristen starten eine Propagadaoffensive', Hamburger Abendblatt, 29 January 2009.

Hegghammer 2006
T. Hegghammer, *'Global Jihadism After the Iraq War'*, Middle East Journal, Vol.60, No.1 (Winter 2006): pp.11-32.

Hegghammer 2007
T. Hegghammer, *Jihad Recollections*, 07 April 2007 (www.jihadica.com/jihad-recollections/).

Holahan 2006
C. Holahan, *'Policing Online Money Laundering'*, BusinessWeek.com, 6 November 2006.

Hyves 2009
Raymond Spanjer over de echte statistieken van Hyves, Hyves.nl, persbericht, 22 July 2009.

ICANN 2007
ICANN Factsheet root server attack on 6 February 2007, ICANN, 1 March 2007.

ICSR 2007
Recruitment and Mobilisation for the Islamist Militant Movement in Europe, ICSR, 2007 (www.icsr.info).

ICSR 2009
Countering Online Radicalisation. A Strategy for Action, ICSR, 2009 (www.icsr.info).

inSITE 2008
'Inside the Online Jihadist Network', inSITE, September 2008.

International Herald Tribune 2008
'Al-Qaida deputy Al-Zawahri says group is still targeting Western countries', International Herald Tribune, 22 April 2008.

Israel Military.net 2008
'Something about Malika', Israel Military.net, 16 December 2008, (http://www.israelmilitary.net/showthread.php?t=7978).

ITAC 2006
'A Framework for Understanding Terrorist Use of the Internet', Trends in Terrorism Series, ITAC, Canada, 2006.

Jane's Terrorism and Security Monitor 2008
'Finding Nemo', Jane's Terrorism and Security Monitor, 4 July 2008.

Jihadwatch 2006
'New "jihad" videogame targets Bush, US Forces, Shi'ite leaders', Jihad Watch, 19 September 2006.

Katz & Devon 2006
R. Katz, J. Devon, *'Jihadist Use Online Remittance System to Fundraise and Transfer Money'*, SITE Intelligence Group, 26 October 2006.

Katz & Devon 2007a
R. Katz, J. Devon, *'The Online Jihadist Threat'*, (Testimony before the House Armed Services Committee Terrorism, Unconventional Threats and Capabilities Subcommittee, United States House of Representatives), Washington: SITE Intelligence Group, 14 February 2007.

Katz & Devon 2007b
R. Katz, J. Devon, *'Web Of Terror; Al Qaeda and its allies are exploiting the Internet to recruit and plot havoc. Here's how we can stop them'*, Forbes, 7 May 2007.

Kohlmann 2008
E.F. Kohlmann, *'Al-Qa'ida's "MySpace": Terrorist Recruitment on the Internet'*, CTC Sentinal, January 2008 http://counterterrorismblog.org/2008/01/alqaidas_myspace_how_suicide_b.php

Kravets 2009
David Kravets, *'Feds: Hacker Disabled Offshore Oil Platforms' Leak-Detection System'*, http://blog.wired.com/27bstroke6/2009/03/feds-hacker-dis.html, 18 March 2009.

Lachow 2009
Irving Lachow, *'Cyberterrorism: Menace or Myth'*, in: Cyberpower and National Security, Franklin D. Kramer e.a, National Defense University Press en Potomac Books, 2009.

Leppard 2007
D. Leppard, *'Al-Qaeda plot to bring down UK internet'*, The Sunday Times, 11 March 2007.

Lia 2009
B. Lia, *'Does al-Qaida Articulate a Consistent Strategy? A Study of al-Qa'ida Leadership Statements, 2001-2009'*, Paper to be presented at the International Studies Association's 50th Annual Convention, New York City, February 2009.

Luiijf 2008
H.A.M. Luiijf, *'Cyberterrorisme'* in: Terrorisme, Studies over terrorisme en terrorismebestrijding, Muller e.a., Kluwer, 2008.

Mansfield 2006
Laura Mansfield, *'His Own Words. A translation of the writings of Dr. Ayman aL Zawahiri'*, TLG Publications, 2006.

Memri 2007
'How Islamist Internet Forums Are Used to Inform Mujahideen of News from Western Media', Memri Special Dispatch Series - No. 1615, 8 June 2007.

Memri 2008
'Women's forums on islamist websites; tools for preparing women to carry out jihad and suicide operations', memri.org, 1 February 2008.

Moss & Mekhennet 2007
M. Moss, S. Mekhennet, *'An Internet Jihad Aims at U.S. Viewers'*, New York Times, 15 October 2007.

Nationalterroralert 2007
Video Shows Simulated Hacker Attack of Power Grid, http://www.nationalterroralert.com/updates/2007/09/26/video-shows-simulated-hacker-attack-of-power-grid/, 26 September 2007.

NCTb 2007
'Jihadisten en het Internet', Nationaal Coördinator Terrorismebestrijding, January 2007.

NCTb 2009
'Aanbieding Samenvatting Dreigingsbeeld Terrorisme Nederland 18', http://www.nctb.nl/Images/Samenvatting%20DTN_tcm91-216361.pdf, 11 September 2009.

NEFA 2008
'Report: "Supervisor of Al-Firdaws Forum Joins Jihad in Afghanistan', NEFA Foundation, 29 June 2008 (www.nefafoundation.org).

Nood & Attema 2006
D. de Nood, J. Attema, *Second Life. Het Tweede Leven van Virtual Reality*, EPN: Den Haag, 1 October 2006.

Novatv.nl
http://www.novatv.nl/page/detail/uitzendingen/3213/MSN-groepen+staan+vol+met+radicale+uitingen, Novatv.nl, 8 February 2005.

NRC Handelsblad 2009
'Duitsland vreest grotere kans op terreuraanslag', NRC Handelsblad, 2 February 2009.

Nu.nl 2007
'Zweedse sites doelwit van Turkse hackers', Nu.nl, 8 October 2007.

Nu.nl 2008a
'Indiase politie waarschuwt Twitteraars', Nu.nl, 28 November 2008.

Parool 2008
'Link hackers tegen Fitna', Het Parool, 13 September 2008.

Pers 2008
'Duizenden sites kraken als reactie op Fitna', Dagblad De Pers, 29 August 2008.

UvA 2009
'Communicatie via internet heeft positief effect op vriendschap', Persbericht, Universiteit van Amsterdam, 2009 (http://www.uva.nl/actueel/agenda.cfm/24764780-1321-B0BE-6840CC1036F6BC54).

Reals 2007
T. Reals, *'Was London Bomb Plot Heralded On Web'*, CBSNEWS, 29 June 2007 (http://www.cbsnews.com/stories/2007/06/29/terror/main2997517.shtml).

Rogan & Stenersen 2008
H Rogan, A. Stenersen, *'Jihadism online. Al-Qaida's use of the internet'*, Norwegian Defence Research Establishment, May 2008.

Sageman 2008a
M. Sageman, *'Leaderless Jihad. Terror Networks in the Twenty-First Century'*, Philadelphia: University of Pennsylvania Press, 2008.

Sageman 2008b
M. Sageman, *'Radical web of Islam's Terror'*, National Post, 8 July 2008.

SANS 2008
'CIA Confirms Cyber Attack Caused Multi-city power outage', SANS NewsBites - Volume: X, Issue: 5, 18 January 2008.

Schofield 2007
M. Schofield, *'New generation of terrorists cyber-inspired, -trained'*, McClatchy Newspapers, 7 February 2007.

Shachtman 2008
N. Shachtman, *'Pentagon researcher unveils warcraft terror plot'*, Wired.com, 15 September, 2008.

SITE 2006a
'First Issue of Technical Mujahid by al-Fajr', SITE Intelligence Group, 28 November 2006.

SITE 2007a
'Large Arabic Compendium of Hacking and Cybersecurity Documents Distributed through Al-Firdaws Jihadist Forum', SITE Intelligence Group, 14 November 2007.

SITE 2007b
'SITE Monitoring Service on European Jihadist Websites Malika El Aroud: Internet Jihadist', SITE Intelligence Group, 31 Augustus 2007.

SITE 2007c
'Detailed Google Earth map of Abu Graib prison provided to jihadists, in addition to available hacks for the Google Earth software', SITE Intelligence Group, 8 March 2007.

SITE 2007d
'Jihadist forum member suggests method of joining al-Qaeda and striking western and Israeli interests', SITE Intelligence Group, 11 January 2007.

SITE 2008a
'Jihadist Forum Member Suggests Mujahideen Sever Underwater Fiber-Optic Cables Providing Internet to European Countries and America', SITE Intelligence Group, 6 February 2008.

SITE 2008b
'Jihadist Informs of Possibility to Attack a Nucleair Reactor Via the Internet', SITE Intelligence Group, 10 April 2008.

SITE 2009a
'Permissibility of Cyber Jihad' in: Western Jihadist Forums', SITE Intelligence Group, June 2009.

SITE 2009b
'Facebook Invasion Jihadists continue campaign', SITE Intelligence Group, 5 February 2009.

SITE 2009c
'Jihadist Forums Go offline, Online Community Frustrated and Confused', SITE Intelligence Group, 11 September 2009.

SITE 2009d
SITE Intelligence Group, *'SITE Monitoring Service on European Jihadist Websites Covering the Period of April to May 2009'*, June 2009.

SITE 2009e
'Al Qa'ida Urges Gaza Reprisals in Western, Arab Capitals', SITE Intelligence Group, 22 January 2009.

SITE 2009f
'Internet Invasion Brigades Spreads German al-Qaeda Video', SITE Intelligence Group, 17 April 2009.

SITE 2009g
SITE Intelligence Group, *'SITE Monitoring Service on European Jihadist Websites. Covering the Period of Early Summer 2009'*, September 2009.

SITE 2009h
SITE Intelligence Group, *'INSITE'*, The official Newsletter of Site Intelligence Group, Volume 2, No. 9, November 2009.

Spangers 2007
Chris Spangers, *'Het onkwetsbare net: Kunnen terroristen het internet platleggen?'*, Intermediair, 11 May 2007.

Special 2007
'Islamist Website Instructs Mujahiden in Using Popular U.S. Web Forums to Foster Anti-War Sentiment among Americans', Special Dispatch-Jihad &Terrorism Studies Project, nr.1508, 20 March 2007.

Spiegel 2005
Yassin Musharbash, *'What al-Qa'ida Really Wants, The Future of Terrorism'*, Spiegel Online, 12 August 2005.

Stenersen 2008
Anne Stenersen, 'Al-Qaida's Quest for Weapons of Mass Destruction, The History behind the Hype', VDM Verlag Dr. Müller, 2008.

Stohl 2007
'Cyber Terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?', Michael Stohl, Springer Science + Business Media BV, 30 March 2007.

Stratfor 2007
'U.S.: The Role and Limitations of the 'Dark Web' In Jihadist Training', Stratfor, 11 December 2007.

Techworld 2009
Michel van Blommenstein, *'Hackersite Milworm is dood! Leve Milworm?'*, www.techworld.nl, 9 July 2009.

Times 2008
'Thousands of cyber attacks each day on key utilities', The Times, 23 Augustus 2008.

Tweakers 2007
'ICANN verklaart falen ddos-aanval rootservers', Tweakers.net, 12 March 2007.

United News of India 2009
'Mumbai Cyber cell traced IP adressess of 26/11 terrorists', United News of India, 2009.

US Senate Committee 2008
'Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat', United States Senate Committee on Homeland Security and Governmental Affairs, 8 May 2008.

US Senate Select Committee 2009
'Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence', Dennis C. Blair, Director of National Intelligence, 12 February 2009.

Vlierden 2009
G. van Vlierden, *'Terreurforum van internet gegooid'*, Het Laatste Nieuws, 11 June 2009.

Wall Street Journal 2009
'FBI Suspects Terrorists Are Exploring Cyber Attacks', The Wall Street Journal, 18 November 2009.

Washington Times 2009
'Hoekstra: 'Stand up to N. Korea'', The Washington Times, 9 July 2009.

Webwereld 2008a
Martin Gijzemijter, *'Al-Qaida verbetert encryptiesoftware'*, Webwereld.nl, 3 February 2008.

Webwereld 2009
Jasper Bakker, *'Vandalen saboteren glasvezelnetwerk Silicon Valley'*, Webwereld.nl, 10 April 2009.

Weimann 2008
Gabriel Weimann, *'Al-Qa'ida's Extensive Use of the Internet'*, CTC Sentinel, Volume 1, issue 2, January 2008.

Weimann 2009
Gabriel Weimann, *'Econo-Jihad, a new Al-Qaeda priority'*, Daily Star, 10 August 2009.

Weizhen & Singh 2008
Tan Weizhen & Khushwant Singh, *'Concerns over use of Google Earth by terrorists'*, Straits Times, 8 December 2008.

Welt 2009
'BKA: Terroristen wollen Bundestagswahl beeinflussen', Die Welt, 2 February 2009.

Whitlock 2008
C. Whitlock, *'Al-Qaeda's Growing Online Offensive'*, Washington Post, 24 June 2008.

Wolfe 2008
'The internet's vulnerability', Adam Wolfe, ISN Security Watch, 19 February 2008.

ZDNet 2008
'Cyberattacks target UK national infrastructure', ZDNet News, 30 October 2008.

ZDNet 2009
Merijn Gelens, *'WPA in zestig seconden gekraakt'*, ZDNet Nederland, 28 August 2009.

List of Terms

Amsterdam Internet eXchange (AMS-IX): The exchange to which the networks of almost all Internet providers in The Netherlands are connected. It is used for national and international data exchanges. The AMS-IX is the largest Internet exchange in The Netherlands.

Anycast: This is a routing scheme for networks whereby data packages for a certain address can be sent to physically different locations. In this way, a large quantity of traffic can be spread over various servers at different geographical locations.

Defacement: Defacement (or defacing) relates to the unapproved changing, replacing or destroying of a website or the rerouting of Internet traffic to a different website by means of a DNS hack or spoofing.

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

Distributed Denial of Service (DDoS): The restricting or frustrating of the operation of one or more networks, systems, or applications thereon, through improper use of a large number of computers. A 'controller' arranges a mass and simultaneous computer attack on a network, system or application.

Domain Name Server (DNS): The Internet cannot carry out its tasks without support services. There is, therefore, a link between the IP address (a number) which is usual on the Internet and the name known to the user assigned by a hierarchically organised service. This is the Domain Name Server (DNS). This services works like a telephone directory. Services such as the www, file transfer and e-mail depend heavily on the proper functioning of this service.

Encryption: Encryption is the process by which data is protected using an arithmetic algorithm and a key comprising a series of numbers, so that it cannot be read by unauthorised parties. This enables parties to communicate with each other confidentially.

Firewall: Protection between the Internet and an internal (company) network. A firewall blocks unauthorised access and prevents the spread of viruses.

Internet as a target: In the event of the Internet being a target, the violence or the causing of serious socially disruptive material damage is directed at (the infrastructure of) the Internet itself. This can take a number of different forms:

- A cyber attack by using computers via the Internet.
- A physical attack based on using conventional weapons against computer hardware or communication lines.
- An electromagnetic attack by using, for example, electromagnetic energy (EMP).
- Other indirect attacks, for example against the electricity supply so that (the infrastructure of) the Internet is unable to function.

Internet as a weapon: In the event that the Internet is used as a weapon, attacks are carried out against physical targets using the Internet. Examples are the taking over of air traffic systems or control systems of vital installations in the chemical sector. Another example is the shutting down of emergency centres or crisis organisations, for example by hacking or by causing overloading.

Internet Service Provider (ISP): An organisation that offers its customers access to the Internet. To do this, the ISP maintains one or more POPs, which are access points to the Internet for subscribers to the ISP. These days many ISPs also offer other services in addition to providing access. Examples are news services, transaction solutions and entertainment services.

IP: IP means Internet Protocol. IP is similar to the postal system. A package of data can be addressed (using an 'IP address' or 'IP number'), sent via the Internet and then 'delivered' to the right computer system. IP addresses are distributed by authorised bodies, for example providers. Every domain name has a corresponding IP number.

Jihad (in this framework within the meaning of armed struggle): The development of violent activities against perceived enemies of Islam in order to realise a world which is as true a reflection as possible of that which one believes is referred to in the first sources of the Islamic faith.

Jihadism: A movement within political Islam whose aim, based on a specific interpretation of the Salafist teachings and the body of thoughts of Sayyid Qutb, is to achieve global dominance of Islam by means of an armed struggle (jihad) and the re-establishment of the Islamic State (Caliphate).

Jihadists: Contraction of jihadist terrorists and jihadist radicals.

Jihadist movement: The jihadist movement is the entirety of networks, groups, cells and individuals whose aim, based on a specific interpretation of the Salafist teachings and the body of thoughts of Sayyid Qutb, is to achieve global dominance of Islam by means of an armed struggle (jihad) and the re-establishment of the Islamic State (Caliphate).

Jihadist terrorism: Terrorism based on jihadist goals. A feature of this category of terrorism is:

- The use of the term jihad for the threat of, preparation of or perpetrating of serious violence against people, or deeds aimed at causing socially-disruptive material damage.
- The carrying out of activities which are commensurate with the aim of achieving global dominion of Islam and the re-establishment of the Islamic State.

Malware: Contraction of the words 'malicious' and 'software'. A generic term for viruses, trojans, spyware, adware, browser hijackers, dialers, etc.

Phishing: A generic term for digital activities whose aim is to extract personal information from people. The swindler (fisher) uses a fake site or e-mail to acquire personal details such as credit card numbers, pin code, social security number, etc.

Radical Islam (or Islamism): The political-religious aim, if necessary using extreme means, to create a society which is as true a reflection as possible of that which one believes is referred to in the first sources of the Islamic faith.

Radicalisation: A mentality which indicates a readiness to accept the ultimate consequence of a way of thinking and to turn it into deeds. Those deeds could mean that differences, which in themselves are manageable, actually escalate to a level at which they disrupt society, due to the use of violence, or behaviour that hurts people deeply or affects their freedom, or due to the fact that groups become alienated from society.

Recruitment: The identification of - and the subsequent controlling and manipulating of - people, so that they adopt an internalised radical political-Islamic conviction, with the ultimate goal being the participation of these people in some way in the violent jihad.

Root server: This is a server at the highest level of the hierarchical Domain Name System (see DNS) which therefore fulfils an essential role in the Internet's 'address book'.

Router: A machine that sends packages of information via a network to the right address.

Salfism/Salafists: Wherever this study refers to Salafism, this means the non-jihadist oriented form of Salafism, with 'Salafists' being the supporters of this variant. This is in contrast to the jihadist form which we regard as being covered by the term 'jihadists'.

SCADA: A process control system that covers the entirety of IT, electrotechnology and information and communication technology used to supervise, control and monitor processes, and to acquire data.

Single Point of Failure: A singular part of a system that affects the operation of the entire system in the event of downtime.

Spoofing: A technique to disguise or change the source of messages. Spoofing can be used to assume the identity of an entity (e.g. a person or system) to facilitate the abuse of a(n) (existing) relationship based on mutual trust.

Terror: Feeling of fear created by a state against its own subjects, often with the aim being to retain the power of the ruling political, religious or ethnic elite.

Terrorism: Terrorism is threatening to commit, making preparations for or perpetrating, for ideological reasons, acts of serious violence directed at people or other acts intended to cause property damage with the aim of disrupting society, for the purpose of bringing about social change, creating a climate of fear among the general public, or influencing political decision-making

URL (Uniform Resource Locator): A clear designation of a place or a file, web page, programme, service or some other arbitrary element on the Internet in which refers not only to the location but also the protocol which can be used to access the file, the web page, the programme, the service or the 'other arbitrary element'. Often the term URL is used to indicate the web address, for example http://www.surfopsafe.nl/.

Violent political activism: The difference between this and terrorism is the absence of a deliberate endeavour to cause human victims or the explicit factoring in of casualties into actions.

Weblog: Pages on which the owner (the weblogger) reports his findings while surfing the web. This usually takes the form of short messages, possibly accompanied by a short comment or description by the weblogger. This produces a list of interesting links which makes it easier for inquisitive surfers to find specific sites. A weblog does not generally contain any links to main pages or domains, but instead direct links to pages within a site.

World Wide Web (WWW): The world wide web and surfing the web have now become household terms. From the protocol technical point of view, the most important service that this is based on is the hypertext transfer protocol (http), which facilitates the transport and the consultation of web pages. Over the years, web functionality has been extended to include dynamic content and more detailed graphic layout (Java, ActiveX, Flash, etc.) and data object-oriented presentation and exchange (XML).

COLOPHON

Publication
National Coordinator for Counterterrorism (NCTb), May 2010

Translation
Amstelveens Vertaalburo B.V., Amstelveen, The Netherlands

Design & coverphoto
Richard Sluijs, The Hague, The Netherland

Print
Koninklijke De Swart, The Hague, The Netherland

Number of copies
400

National Coordinator for Counterterrorism (NCTb)
P.O.Box 16950
2500 BZ The Hague
The Netherlands
Telefoon +31(0)70-315 03 15
E-mail info@nctb.nl
Website http://english.nctb.nl

The NCTb helps to make the Netherland a safer place to live

The task of the National Coordinator for Counterterrorism is to minimise the risk and fear 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.

Publication
National Coordinator for Counterterrorism (NCTb), May 2010
http://english.nctb.nl