Summary

High-tech crime, different crime types and perpetrators: A literature review

In this current digital era we live in, core processes throughout society are often controlled by ICT and digital technologies. The worldwide use of ICT and the internet by both private individuals and the business community has increased during the past decade. Our society has come to depend heavily on a fully operational network of digital and inter-connective systems. This dependency will continue to grow as more government bodies, companies, organisations and natural persons start to use them. The specific conditions associated with this development – such as the growing use of networks that have an open internet connection, and the anonymity and broad reach of the internet – also provide lucrative opportunities, however, for the criminal circuit (Van Amersfoort et al., 2002). The opportunities for a wide range of criminal activities – described here as *high-tech crime* – have increased significantly in recent years (NHTCC/NPAC, 2006a: 6). The financial, economic and social consequences of high-tech crime may have a deep impact on our society. Not only is it important for the core processes in our society to continue functioning well and to continue in their development, but the user's faith in a secure ICT environment is also a vital aspect. As a result, preventing and combating high-tech crime is one of the spearheads in the Dutch and European security policies. The lack of knowledge concerning the perpetrators of high-tech crime and the involvement of organised crime is an important gap in terms of developing an efficient and effective policy. As such, the Ministry of Justice felt that it was fitting to commission a *literature* inventory, mapping the status quo and existing knowledge in relation to high-tech crime and, more particularly, its perpetrators (including perpetrators of organised crime).

This study focuses on the following six research questions:
- What do we mean by the term 'high-tech crime'?
- What phenomena of high-tech crime can be distinguished?
- How can the perpetrators (or perpetrator groups) of high-tech crime be characterised?
- What is the extent of organised crime's involvement in high-tech crime?
- What gaps exist in the literature in terms of knowledge concerning the perpetrators of high-tech crime?
- What developments in high-tech crime should we expect in the near future?

For each research question, the main findings are summarised and a few points of concern and discussion are assessed for the purpose of further interpretation of the research and policy programming in the field of high-tech crime.

What is high-tech crime?

The literature shows that it is not easy to clearly define the criminal area of high-tech crime. There is no conventional norm on shared concepts and often, different definitions are used interchangeably. The scope of high-tech crime is infinite and difficult to delimit due to the close relationships between 'traditional' forms of crime (such as fraud and theft) on the one hand, and advanced ICT and digital technologies on the other. Moreover, new criminal markets are also emerging at the same time. As a result, researchers, policy-makers and law enforcement workers have a tendency to speak different languages: identical concepts used to describe a phenomenon may have widely diverging meanings to different stakeholders and vice versa (different terms that actually refer to the same problem), and some use a narrower set of definitions than others. The area of crime is also referred to differently by different people. For instance, terms like cyber crime (or cyber criminality) and high-tech crime are often used as equivalents, but terms like ICT, internet, digital, information and e-crime are also used on a regular basis. This lack of a total overview and the absence of consistency cause confusion and do not benefit the development of a good approach, knowledge exchange and collaboration in the field of high-tech crime.

This report uses *high-tech crime* as the umbrella term that refers to a range of criminal activities which make use of ICT. Such criminal activities may target persons, property and organisations (using ICT as a means), or electronic communication networks and information systems (with ICT being both the means and the objective). When compared to the term *cyber crime*, *high-tech crime* offers a wider and more dynamic perspective – a better match for the fast technological developments in time. The umbrella term also covers new forms of crime that may emerge from new ICT innovations (not just the internet), which by definition means that high-tech crime is not a static umbrella term. In order to further define the difference between traditional offences and new forms of crime that have resulted from ICT, this report distinguishes between two sub-categories of high-tech crime. Where ICT can be characterised explicitly as the means *and* the target, we use *computer crime*. For all other ICT-related (often traditional) offences we use *cyber crime*. There are different, closely related phenomena of both sub-categories, which are often committed simultaneously. A characteristic that the phenomena of computer crime (e.g. hacking and virus distribution) share, is that they are of an extremely technical, virtual nature: they have emerged from – and cannot exist without – ICT. But the phenomena of cyber crime, to the contrary, generally involve traditional offences that can be committed without ICT (e.g. child pornography and extortion) but have now emerged

in a new (more efficient) form due to the use of advanced, technical – ICT-based – resources.

What are the phenomena of high-tech crime?

This report uses a holistic perspective in order to create an inventory of as much knowledge as possible relating to the perpetrators of high-tech crime. To this end, we have categorised the different phenomena of cyber and computer crime into eight theme clusters on the basis of the literature (see also Figure 2.2 in Chapter 2):

Cyber crime:
1. legal communication and covert shielding;
2. illegal trade;
3. economic and financial crime;
4. illegal communication.

Computer crime:
5. unauthorised access to ICT;
6. ICT failure due to data traffic;
7. ICT failure due to data and system manipulation;
8. service performers.

This classification represents a preliminary inventory and serves as a basis for the further development of a typology of high-tech crime. The overview is necessary to provide a starting point for further knowledge development and policy creation in the prevention of and fight against high-tech crime. However, the classification can be adjusted and supplemented with new, complementary knowledge at all times. Each of the theme clusters and associated phenomena is summarised below.

Cyber crime

Cyber crime refers to the use of ICT as a tool to commit a range of offences. In many cases, this relates to the supporting function of ICT in communication (between perpetrators or between perpetrators and victims), but also, for instance, about using ICT to execute (voluntary or forced) transactions with goods and services, as well as financial transactions.

Legal communication and covert shielding
ICT has a great many functions. In relation to crime, for instance, the internet acts as a virtual source of inspiration, a virtual meeting place,

and a platform for knowledge exchange and secure and unsecured communication. When these functions are used for *illegal* purposes (e.g. to recruit radical youths), this report refers to cyber crime. This cluster covers three themes: radicalisation and extremism, terrorism and ideologically motivated crime, and innovative covert shielding using ICT. The internet plays a prominent part in both radicalisation and terrorism. The internet lives particularly among young people, and they are mutually inspired and motivated to make extremist statements. The internet is also used to gather knowledge (manuals or other operational knowledge) and mobilise people. The literature shows a trend towards publications focusing on the impact of Islamic radicalism (and other radical movements to a lesser extent). This may have a negative impact on knowledge development in a broader sense and lead to tunnel vision. As a result, important trends and indications may be neglected or overlooked. Radicals, terrorists and parties in the criminal circuit use innovative techniques to screen their communication from 'unauthorised' parties (including criminal investigation bodies). Their methods vary from smart ideas (such as continuously changing unregistered mobile telephones or using 'dead letter boxes', where draft e-mail messages can be viewed and modified by several users without actually being transmitted) to advanced concepts like encryption (encoding the content of messages), and steganography (hiding the existence of a message altogether by incorporating it into an image or digital clip, for instance). In some cases, experts are hired to perform these operations.

Illegal trade

The internet enables unlimited and virtually effort-free trade. It is a growth market in our modern economy, but it also means that illegal goods and services can be traded over the digital highway. Both national and international literature provides little insight into the illegal trade in drugs, arms and explosives, nor human trade and smuggling. Based on this study, we cannot determine whether this is indicative of the *extent* to which the internet is being used, or whether such knowledge is absent due to the lack of investigation, research and publications. For now, it seems that ICT plays a primarily *communication-oriented* role in such forms of trade. The relative anonymity of internet users and the lack of social control and face-to-face contact may in fact deter internet use among these criminal markets. However, there are phenomena in which the internet is an important economic market place and distribution channel for trading goods and services. Counterfeit brand drugs, non-prescription drugs, child pornography, stolen goods, illegal software (software piracy) and illegal gambling are all examples of such goods and services that are currently offered on a large scale. The internet is a popular and commonly used resource mainly because of the large market to which it offers access and the relatively low risk of being caught. The trade in child pornography

in particular, in which the material itself is offered in digital form, is being increasingly blocked with the help of advanced techniques.

Economic and financial crime
Economic and financial crime involves making an illegal profit by means of fraud, deception and embezzlement. Internet embezzlement in particular is a common problem that is threatening Dutch society. People are made to pay money under false pretences (advance-fee fraud), or ICT is used to obtain confidential information illegally (identify theft) that is subsequently used to commit bank and credit-card fraud. Identity fraud by means of phishing – which is a criminal tool rather than an objective – is seen as one of the fastest growing forms of non-violent crime. The literature contains less information on the other themes (fraud through market manipulation, extortion and blackmail, and money laundering). Money laundering using ICT might increase significantly in the future due to the growing virtual money flows in social and economic traffic (via online auction sites, electronic and mobile commerce). Another potential threat is the extortion of companies that depend heavily on the internet for their operations (e-commerce), or companies and citizens which receive threats that important files and data will be damaged or made publicly if they do not comply with the demands being made. We should note the close relationship between phenomena of cyber crime and computer crime in this context. Internet fraud (cyber crime), for instance, uses a variety of methods and techniques like phishing, spamming, malware and pharming (computer crime). The cyber variant of blackmail and extortion is often related to system hacking and threats of a dDoS attack that may corrupt entire systems (see also computer crime).

Illegal communication
The many uses of ICT and the internet can also be used to convey messages with *illegal content*. This mainly involves activities that actually affect public morale, or the personal life of victims (e.g. stalking, discrimination or grooming). In this report, such crimes are called illegal communication. In terms of their content, these digital behavioural crimes differ little from their variants in the 'physical world'. Discrimination (or inciting hatred) via the internet in particular, in which different groups continuously provoke each other in discussion forums and chat boxes, has become a trend. Another growing problem that is causing a lot of outrage in society is grooming, in which chat sites are used by adults with dishonourable sexual intentions to approach children. In some cases, grooming results in an actual meeting where minors are physically abused and raped. Illegal communication is also involved when third-party computer and telephone data are intercepted illegally, i.e. without authorisation (espionage). Criminals use methods and tools like hacking, spyware and malware to do this, as well as service

performers (e.g. corrupt employees). Here, too, we see a close relationship between cyber crime and computer crime. In this context, the use of spyware (software installed unnoticed on a computer that collects data and transmits it to a third party) and keyloggers (where keystrokes and mouse clicks are transmitted to a third party) in particular may expand in the future.

Computer crime

In this report, the term *computer crime* refers to all new forms of criminality that would have been impossible if ICT did not exist. ICT is used not only as a tool in such criminal activities, but also as the explicit target. In most cases, computer crime is about breaking into, disturbing, manipulating or changing systems and/or developing and providing tools and resources to do so. We distinguish four theme clusters that are described below.

Unauthorised access to ICT
There are two central elements in providing unauthorised access to ICT (in fact, breaking into systems): hackers and botnets. Hackers increasingly have criminal intentions, are increasingly often financially motivated, and engage in multifunctional activities that can be used for multiple phenomena of computer crime. They can break into secure and unsecured systems, develop tools to cause ICT failures, and provide tailor-made customisations that require a high level of expertise and technical knowledge. There is an 'underground' sub-culture that resembles the underground criminal circuit: it has its own identity, status as an important acquirement, and its own standards and values. Hackers are increasingly hired by traditional criminal networks, and, in some cases Dutchmen are also members of organised (Eastern European) criminal networks acting as service performers.[153] One of the main criminal tools that hackers can provide is a botnet. This is a collection of remote-controlled computers that is instrumental in committing several phenomena of high-tech crime, especially spamming, phishing and (extortion with the aid of) dDoS attacks.

ICT failure due to data traffic
Criminals can disturb the operation of systems (e.g. websites, e-mail services or computer networks) in several ways. (d)DoS attacks and spamming are two important phenomena that have shown enormous worldwide growth. A (distributed) Denial of Service or (d)DoS attack involves intentionally sending massive quantities of data to systems,

153 We use the term service performer to avoid confusion with the term 'service provider' (ISP).

overloading them and making them unavailable. It is a tool that is deployed to blackmail companies, for instance, but may also represent an expression of protest, revenge, competition and vandalism. Spamming in the form of mass e-mails can also cause system failures, but this is mainly a side-effect of digital marketing and advertising (e.g. for lifestyle products and non-prescription drugs), rather than a concrete objective. Internet fraud involves sending massive quantities of phishing e-mails in order to obtain confidential information from people. That information is then used to extort their money. Hackers provide support for both dDoS attacks and spamming, or execute sub-tasks with the aim of causing targeted failures.

ICT failure due to data and system manipulation
Failures can also be caused directly by the actual manipulation of (damaging, deleting, changing or destroying) data and systems. Malware is the umbrella term for dubious '*…computer programmes that run on a computer without authorisation from the owner or administrator and cause the system to do something an outsider wants it to do*' (KLPD, DNRI, 2007a: 15). Such programmes are tailor-made by experts and, entirely unnoticed, collect confidential user information, damage data and systems (the infamous viruses), or grant external access to computers (via the modern viruses called Trojan horses). It is also possible to block or change entire websites (defacing), among other things, as a way to swindle (e.g. internet fraud by means of fake websites) and extort money from people or to express one's discontent (hacktivism). Only when ICT systems that control vital infrastructures (such as transport systems, control systems in the chemical sector or important crisis and information services) are damaged for political reasons in order to cause large-scale social disruption, this report refers to a cyber-terrorist attack. While no concrete attempts have been made to date, (vengeful) insiders with knowledge of and access to the operating systems represent a significant threat in particular (see also service performers).

Service performers
The use of ICT service performers has a direct relationship to organised crime. Criminals and terrorists hire the knowledge of experts to, for instance, protect their communications against criminal investigation or develop tools to facilitate criminal or terrorist activities (such as the intentional creation, sale, distribution or availability of a technical tool, password or code to gain access to an automated system). This report distinguishes between three types of service performance: corruption of ICT personnel, infiltration by criminal ICT workers, and hiring ICT experts. People with ICT authorisations that have access to sensitive company data may render assistance (through bribery or threat) to criminal parties from inside an organisation. This is called corruption

and mutual involvement of the upper and underworlds. While the threat of corrupt IT workers seems limited in the Netherlands at this time, criminal infiltration by ICT consultants and hiring experts for certain tasks (e.g. hackers) constitute a significant security risk.

What is known about the perpetrators?

Systematically mapping perpetrator characteristics in the form of risk indicators (the prototype offender profile) is called *profiling*. In terms of development and usability, however, profiling techniques are still in their infancy. This technique does not lead directly to the identification of the perpetrator(s) of a crime, but provides a description of *combinations of properties* that perpetrators are likely to have. At this time, insufficient research data is available about the effectiveness of using risk profiles (see also Van Donselaar and Rodrigues, 2006: 43, 58). It is clear that a combination of general and specific perpetrator characteristics that are sufficiently distinctive is required.

The disadvantage of risk profiles is that they confirm prejudices about certain people and groups. Both prevention and investigation will devote a disproportionate amount of attention to known risk groups, which may lead to stigmatisation of innocents (that just happen to match the characteristics) whilst simultaneously allowing real criminals to remain 'invisible' and untouched if it just so happens that they do not match the profile. As such, the profiling technique is certainly not perfect; its use requires a certain level of caution and nuance. As a preventive and investigative tool, risk profiles must be used with great care and restraint. However, an understanding of perpetrator characteristics may offer a starting point in both the prevention and tracing of high-tech crime. Further research will have to demonstrate this. Since perpetrator characteristic mapping onto profiles is not yet supported from an empirical perspective and validated instruments are lacking at this time, this report speaks of understanding the type of people that commit high-tech crimes instead of using the term 'offender profiles'.

The lack of knowledge concerning the perpetrators in a so-called 'intelligence database' is one important reason for the failure to develop perpetrator or offender profiles. One of the aims of this study was therefore to compile an inventory of existing knowledge about people and groups that commit high-tech crimes on the basis of national and international literature. In Chapter 3 we mapped perpetrator characteristics for a selection of high-tech crime phenomena whose threat and risks to Dutch society are considered most urgent:[154] (1) radicalisation

154 The perpetrator characteristics for the other phenomena of high-tech crime are described in Annex 4.

and extremism, (2) terrorism and ideologically motivated crime, (3) child pornography, (4) grooming, (5) software piracy, (6) internet fraud, (7) money laundering, (8) cyber terrorism, (9) hacking, (10) malware, and (11) ICT service performers.

Among other things, this inventory demonstrated that *internet fraud* and *hacking* in particular are criminal phenomena that are often committed in combination with other forms of high-tech crime. Terrorism, child pornography, grooming, software piracy and internet fraud mainly involves male perpetrators. Most sexual offences (child pornography and grooming) are committed by white perpetrators, whilst terrorism and internet fraud primarily involve perpetrators of African and/or Asian descent. While a significant proportion of high-tech crimes is financially motivated, hackers and malware authors in particular have a range of motives for their criminal activities (they also do it because of the challenge, their ideology, power, revenge or vandalism). It is notable that corrupt ICT workers and criminals who are active in the field of terrorism, internet fraud, child pornography and hacking tend to have a criminal record. The diversity of phenomena and (limited) clues as to the perpetrators make it clear that it is impossible to speak of 'the' high-tech criminal, but rather of criminals that specialise in a certain field. However, because certain offences are facilitated by the same digital techniques it becomes easier for the criminal to realise larger profits by deploying the same techniques to commit multiple crimes at the same time.

We are forced to conclude, however, that fairly little knowledge on individual perpetrators of high-tech crime is available in the literature. The literature inventory offers nothing more than rough and incomplete perpetrator sketches based on a limited number of characteristics. If we compare the profile sketch with indicators such as those developed for the FBI (see also Annex 5), there is a clear lack of specific perpetrator knowledge in the literature, in terms of organisation (e.g. recruitment), execution (expertise), behaviour (including personal characteristics) as well as the resources used. Moreover, for most phenomena of high-tech crime we also lack an understanding of the criminal career of perpetrators and the overlap between the various forms of high-tech crime. The information that *is* available in the literature is generally superficial, unstructured and limited, and in some cases based on anecdote and hypotheses of which the reliability and validity are difficult or impossible to establish. In short, there is a lack of empirical scientific research into perpetrator characteristics which clarifies the distinction between the separate phenomena of high-tech crime. A more elaborate understanding of perpetrators can be achieved by means of more problem-targeted research (e.g. case studies). A literature inventory alone

is clearly not enough to make well-founded statements about people and groups that commit high-tech crimes.

Can we speak of organised high-tech crime?

There are indications that organised crime exists for some phenomena of high-tech crime. In this report, we speak of organised crime if: '*…groups focus mainly on illegal [financial or material] gain and systematically commit crimes with serious consequences for society*' (Parlementaire Enquêtecommissie Opsporingsmethoden, Annex VII, 1996; Fijnaut et al., 1998; Kleemans et al., 1998: 22-23). While little is known in the literature about perpetrator groups committing high-tech crime (the understanding of perpetrators is relatively limited), there are clues that both traditional criminal networks (such as the Russian and Eastern European mafia) are involved that hire the required expertise externally, and that new fluid high-tech (HT) criminal networks are involved in which experts (such as hackers and malware authors) perform sub-tasks and bundle their forces. The KLPD (Boerman and Mooij, 2006) speaks of a trend towards *diversification* in which various forms of crime are committed simultaneously (e.g. hacking, botnets, spamming, malware, pharming, dDoS attack, internet fraud, extortion) and a trend towards *specialisation of tasks* in which criminals deploy experts that are responsible for certain sub-tasks in committing an offence (e.g. developing the tools or creating fake websites).

An inventory was made in Chapter 4 on the involvement of organised crime in the phenomena of high-tech crime that were qualified as a threat to Dutch society (see also section 5.3). Of the phenomena prioritised in Chapter 3, child pornography, software piracy, internet fraud (advance-fee fraud and identity theft), money laundering, hacking and malware in particular, are financially lucrative fields of operation for both traditional and new fluid HT criminal networks. The profits are significant, especially when you consider the small amount of investment and risks involved. ICT service performers also increasingly have criminal intentions and become involved in organised crime. Young people with ICT knowledge are recruited at universities, computer clubs and via the internet to provide support to the malicious practices of criminals; as are graduates and IT employees. However, this does not necessarily mean that the criminal circuit itself may not possess adequate technical knowledge to commit serious crimes without outside help. Botnet trading in particular is an important market for organised crime. In the Netherlands, HT criminal networks operate mainly in the field of internet and advance-fee fraud. Moreover, the Netherlands is an important supplier of botnets (that are rented out at very high prices) and an

important target of dDoS attacks. Creators of viruses (malware and Trojan horses) in particular play a prominent part in this context to gain control of, and spy on, the systems of others. Modifying or destroying websites (defacing), and developing fake websites to which people are rerouted (pharming) are increasingly becoming crimes from which perpetrators also achieve considerable financial gain.

While in relation to radicalisation and terrorism, activities occur on a (locally) organised basis, traditional criminal networks are not involved. Nor does grooming (which is generally committed on an individual basis) involve organised high-tech crime; and no concrete cyber-terrorist activities have been detected as yet. Furthermore, KLPD research has not yielded any clues on collaboration between criminal and terrorist networks (Boerman and Mooij, 2006: 86). We should note, however, that terrorist networks *are* involved in a range of criminal activities, including high-tech crime as a means to finance their terrorist operations.

We can only conclude here that, as yet, too little can be said about organised high-tech crime based on this literature study. The inventory offers a general overview of the criminal activities (that are sometimes committed in combination), the level of expertise required, experts and service performers hired, and the transnational nature of high-tech crime with its international connections. It is expected that organised crime will increasingly move towards high-tech crime, implementing ever new trends and innovative techniques. However, specific knowledge concerning perpetrators and collaborations is lacking in the literature, and additional research (e.g. studies on criminal files and cases) is necessary to map organised crime in the field of high-tech crime more adequately.

What are the knowledge gaps concerning perpetrators?

Based on this literature inventory, we have established that little specific knowledge is available concerning perpetrators and criminal collaborations. The overview below classifies the findings in terms of current perpetrator knowledge on a scale from 1 (very limited knowledge) to 4 (very good knowledge). The prioritised high-tech crime themes are printed in bold type. The rows (from left to right) refer to the knowledge position concerning individual perpetrators; the columns (from top to bottom) list the knowledge as it relates to organized high-tech crime. As such, the overview provides a direct understanding of what is known, in the literature, of individual perpetrators and HT criminal networks for each variant.

Literature-based high-tech crime perpetrator knowledge

	Individual perpetrator characteristics			
HT criminal networks	Very limited	Moderate	Good	Very good
Very limited	**Animal rights activism** **Extreme right terrorism** **Software piracy** **Identity fraud** **Pharming (internet fraud)** **Money laundering** **Grooming** **Cyber terrorism** **Hacking** **Novice hacker** **Petty thief hacker** **Old guard hacker** **Virus writer hacker** **Professional criminal hacker** **Information warrior hacker** **Political activist hacker** **Malware** **ICT service performers** Medicine trade Arms/explosives trade Human trade Drug trade Fencing Illegal gambling Market manipulation Espionage Spamming dDoS attack Defacing	**Right-wing radicalism** **Islamic radicalism** **Islamic terrorism** **Cyberpunk hacker** **Internal hacker** Cyber stalkers Discrimination	-	-
Moderate	Shielding Extortion and blackmail	**Child pornography** **Advance-fee fraud**	-	-
Good	-	-	-	-
Very good	-	-	-	-

The overview shows that there is a *moderately good* understanding of child pornography and advance-fee fraud perpetrators (both in terms of individual perpetrators and for HT criminal networks); that there is *moderate* knowledge, for extreme-right and Islamic radical and terrorist movements, of individual perpetrator characteristics (but not HT criminal networks); and that there is also a *moderately good* understanding of individual perpetrator characteristics – but not for HT criminal networks) for several hacker variants (cyberpunk and internal hacker) and

behavioural offences (cyber stalking and discrimination).[155] While there may be some knowledge of HT criminal networks for some techniques (shielding, extortion, pharming), the individual perpetrators behind them are relatively invisible. Perpetrator knowledge is not qualified as good or very good for any of the phenomena of high-tech crime. It is notable that very limited knowledge is available in the literature on the perpetrator characteristics for most of the phenomena (the top-left cell in the table contains most of the phenomena). And for many of the phenomena characterised as a threat to Dutch society (animal rights activism, extreme right terrorism, software piracy, identity fraud, money laundering, grooming, a number of hacker types, malware creators and ICT service performers),[156] we can conclude that there is a lack of knowledge all together. This does not necessarily imply that such knowledge is unavailable to the law enforcement and intelligence services. After all, the conclusions of this report are based on a study of mostly public literature.

Expectations for the future

Increase in high-tech crime
In terms of high-tech crime, it is expected that both the number of victims and criminal profits will continue to grow over the next few years. Perpetrators change methods quickly and the trend of diversification (in which criminals focus on various activities at the same time) and task specialisation (in which specific expertise is deployed for criminal sub-tasks) will continue (NHTCC, quoted by KLPD/DNRI, 2007a: 36). It is also expected that criminal activities will focus more on specific targets (i.e. an individual or organisation); and especially on victims that have little or no technical knowledge of digital communication structures (e.g. the elderly) and have implemented inadequate security will be duped in particular (NHTCC, 2006b: 10-11).

The internet as a crime scene
Due to increased use of the internet (causing the market to grow) and the limited risk of being caught, illegal trade on and via the internet may expand further. Moreover, the increasing virtual money flows give rise to the expectation that internet fraud (and identity theft) will cause the greatest number of victims and the most important financial damage (Taylor et al, 2006: 357-383). The V-NDB2006 also described identity fraud

155 In relation to cyber stalking, collaborations are irrelevant due to the nature of the offence.
156 It is self-evident that there is no knowledge concerning the perpetrators of cyber terrorism since no such attacks have been made to date.

with the aid of phishing as going through a tumultuous development (Boerman and Mooij, 2006: 21, 30). The high ADSL density, which means that computers are connected to the internet virtually permanently, makes the Netherlands a particularly attractive area of operations for phishers. This involves not just cyber criminality but also phenomena of computer crime, such as spamming (Ianelli and Hackworth, 2005). More recently, phishing on the internet is based in part on botnets (networks of malware-infected computers that are then controlled by third parties from external locations). Botnets also play an important part in many other high-tech crime phenomena, thereby representing a significant threat (Europol, 15 June 2006). Since botnets are created on a smaller scale and focus on specific target groups, they are becoming more difficult to trace.[157]

The emergence of hackers as service performers

The deployment of ICT service performers and experts must be qualified as the most important development in the field of organised and high-tech crime. There are indications that criminal networks from Eastern Europe and Russia in particular hire hackers originating primarily in Western Europe. Through the years, hackers discovered that they can make a lot of hard, fast cash with their expertise. As a result, they have attracted attention from criminal networks and, in some cases, are likely to be members of such organisations. Many criminals who are interested in high-tech crime have an interest in botnets, for instance, putting the hackers that have access to such zombie networks in a special position. This has made hackers into important facilitators for criminal groups. They deliver a range of technical tools, such as back doors (to gain access to systems), Trojan horses and bots (to control computers externally), and complete botnets (armies of zombie computers that can be remote-controlled) to order. The multifunctional applications of *malware* and *botnets* in particular are strong drivers in the criminal market of high-tech crime: they are tailor-made and facilitate a range of criminal activities, such as dDoS attacks, phishing, spamming, internet fraud, and the distribution of child pornography. Particular causes of concern are the recruitment of young students (who are approached at universities, computer clubs and/or online forums), the corruption of highly qualified ICT personnel,[158] and the infiltration of criminals in ICT companies or e-commerce. A lack of knowledge concerning the perpetrators and the ways in which criminal groups deploy ICT in their operations cause considerable obstacles in criminal investigation and prosecution,

157 Because many botnets can be active simultaneously, their impact is not necessarily reduced.
158 Introducing a professional code for ICT workers has been a subject of discussion for several years (Rogers, 2001: 132-133).

which means that controlling this phenomenon causes serious concern (NDB2004, KLPD, DNRI).

Young people as a high-risk group
The younger generation and students with solid ICT knowledge and skills, as well as a sound understanding of the internet can be qualified as a particular high-risk group for high-tech crime. This applies especially for the possibility of being involved in organised crime, not just for criminal but also for terrorist collaborations (Europol, 2003; McAfee, 2006; Neve, 2007). Research has shown that computer crime (and some associated forms of cyber crime) perpetrators are becoming younger and are engaged in ever more complex activities (Europol, 2003: 116). Apart from the 'thrill' and the challenge, high-tech crime helps them make a lot of money. This may cause young people that may initially be qualified as part of a type of 'youth gang' to enter a criminal spiral from which it is difficult to escape.

Corruption within companies
The vulnerabilities that are created in companies when employees are careless about security measures or block or derange them intentionally is another phenomenon requiring attention. Because key processes in companies and government bodies are increasingly controlled by ICT, these organisations are forced to rely on experts with the skills and expertise to develop, manage and secure their systems. Persons with high-level ICT authorisations (engineers, system and data administrators) or access to sensitive and confidential data (e.g. customer and payment files) and employees of companies or organisations that are responsible for vital infrastructures and security (SCADA systems, criminal investigation services) represent a particular risk. This involves not just people who may be sensitive to corruption, but also vengeful (ex-)employees (internal hackers and CITIs) that can potentially cause serious damage. Companies also increasingly hire external IT consultants to build systems or software. If these people have criminal intentions or if criminals offer ICT services on the market as independent entrepreneurs, this may constitute a serious security risk.

Sub-cultures
Part of the social activities that used to be part of the 'physical world' now make use of ICT and digital technology. Virtual communities that use discussion forums, for instance, can sometimes be qualified as sub-cultures (hackers, scientists, youth gangs, paedophiles). These communities have their own identity, standards, values and interests, and in some cases even their own 'language' (the use of acronyms and symbols). This applies to young people with radical (Islamic or extreme right) ideas, for instance, as well as youngsters who have become part of the underworld of the hacker community. According to Turgeman-

Goldschmidt (2005), what starts as a form of entertainment may easily devolve and escalate into a criminal phenomenon. The increasing shift towards a digital society also means that some behaviour will result in excesses on the internet, for instance. We must devote attention to assessing a number of phenomena of high-tech crime that involve young people (radicalisation and extremism, software piracy, discrimination, hacking) in relation to sub-cultures and youth criminality. Social-psychological factors and group processes that are linked to the internet (e.g. moral development, family problems, social influence and sub-cultural group formation) are special areas of concern in this context (cf. NCTb, 2006b: 10; Yar, 2005b).