Summary ‘Phishing, Child porn and Advanced-Fee internet Fraud’

In this summary we will follow the connecting lines which run through the subject matter of phishing, child pornography and advance-fee internet fraud. These all result in central conclusions. Consistent with the approach in this report, they often have a hypothetical character as well. The dividing questions which are presented as points of departure for this research report, have served as denominators under which to categorize the conclusions. In the second part of the summary a number of discoveries made during this research will be dealt with. Research restrictions and the quality of the source material, a.o., will also be discussed. At the end, we will look ahead, on the basis of the questions posed, to which further steps these research results may lead. After all, hypotheses are nice but their real value will be proven only through application and testing the results of the hypotheses against their presupposed results. Realization of these activities and creating the necessary conditions are beyond the scope of this report.

Hypotheses and “darknumber” as points of departure
The relevance and therefore the presentation of this research had connotations with the nature of the “darknumber” of cybercrime and the characteristics of the responsible “unknown offenders”. It is an accepted fact that one can gather all sorts of knowledge from research documents, literature and “people’s brains”. Knowledge which, if it were accumulated, would lead to both factual, as well as presumed characteristics of the manner in which cybercrime is committed and which people are involved. To avoid that disclosed facts would be viewed as representative of the undisclosed darknumber or unknown offenders, hypotheses are used, with the indisputable advantage that not only factual insights could find a position within these hypotheses but also if suppositions about the method of operating within cybercriminality and the characteristics of its offenders could do so.
This leads us to the actual question:

*Which hypotheses concerning the cybercrime offenders and the crimes they commit(led) could serve as a basis for influencing, prevention or stopping?*

Hypotheses have no purpose of their own but are of use for the different kinds of influencing of cybercriminality. Varying from policy development in which, as far as
strategic choices go, one often has to rely on relatively vague ideas about what else could be going on besides what has become known to the police and regulatory agencies, to putting up barriers against presupposed criminal procedures.

In this study, cybercrime is translated as “internet related criminality”. The concept of criminality should be between quotation marks because it would include not only facts punishable by Dutch law, but also every other form of illegality or facilities which contribute towards illegality. Not really a watertight definition but it is adequate for the functional character of this study. The scope of internet related criminality is embedded in focussing on phishing, child pornography and advance-fee internet fraud. Three diverse forms with the common effect that they strongly encumber society as regards to psychological and/or material damage. That is also the reason they were chosen. The internet relationship is different for each of the three forms. Phishing activities (address acquisition, identity theft, mule-recruitment, etc.) are internet related per definition. This is also true for child pornography, as far as distribution and demand is concerned, but hardly for its production. In the case of advance-fee internet fraud, the relationship is even more restricted, as the internet is mainly used for massmailing of spam and the subsequent e-mail communication with the victims who responded to the temptation of the spam.

**Offenders: types, characteristics and profiles**

In literature about cybercrime and also in investigations and regulatory files, the conception of offenders is usually not much differentiated. In the process of phishing, the spammer who mailed the spam runs is often regarded as the offender, as is the money mule, on whose bank account the proceeds acquired by stolen identity data are deposited. But these are only two of the in total 17 offender roles which have been connected to phishing in this research report, not counting the offender roles of the so-called “bona fide” offenders.

In the case of child pornography, the perspective of the offender often goes together with the downloader, while there are at least 18 offender roles distinguishable. In the case of advance-fee internet fraud, the scammer (the person who sends the e-mail) is usually marked as the offender; one of the 13 malefide offender roles.

The offender perspective is strongly connected to where an offender type is located. Downloaders of child pornography, scammers and spammers are active in the Netherlands and therefore sooner subject to locating and prosecuting than if they work mainly from abroad. The perspective of the offenders is dependent on three variables: the possible range (national-international) of the authorities which are looking at a modus operandi (MO), the core business of those authorities and
who they have managed to identify at the hand of tips or by catching red-handed.

Of the three researched cybercrime offences various offender types have actually been recorded in the form of role complexes which describe the mutual relationship; roles of which the involvement has been proven or is presumed. On the basis of their responsibility or contribution to the modus operandi, the roles are divided into three types: “initiators” (those taking the initiative), “employees” (those carrying out the work), and “facilitators” (the supporters). The initiators have in common that they have initiated and/or maintained a criminal business process. Without their intrinsic motives this process would not exist. In the role complex concerning child pornography the actual perpetrator (abuser) of a child is also considered to be an initiator and on the basis of the nature of the abuse is then sub-divided into six subtypes: the “voyeur” (peeping Tom), the “breeder” (the child molester on the internet), the “choreographer” (the internet child molester who actually meets the victim and seduces him/her to pose naked), the “performer” (the masturbator in the presence of the child), the “assailant” (who has sexual intercourse with the child), and the “sadist”, who not only has intercourse with the child but also assaults it in other ways.

In the example of the abuser, the role of the initiator coincides with that of the employee but that is not the case per definition. Employees are the performers of the primary process. They perform the activities which belong to a certain modus operandi and they also know to which offence they contributed. The last type, the supporters, indirectly contribute to an offence without exactly knowing what their contributions are used for. There are two types of facilitators: *bon fides and male fides*. The first group is actually also misused as victim because they have no concrete idea that their contributions are used for data theft, the production of child pornography or swindle. They cooperate reluctantly and as soon as they realize this they often attempt to take measures against it, even if this is difficult for the suppliers of the generic products. The second group knows that they supply the resources or render services that are most probably, or even certainly, used for illegal practices.

The consequence of differentiated offendership is that the characteristics of these offenders also differ. In this research the emphasis was put on the characteristics which could be portrayed by administrative means; a principle which logically arises from the final objective: charting the dark numbers and unknown offenders. Socially demographic characteristics such as gender, a wide age-scope or a certain level of education are less suitable as they discriminate insufficiently between the three offences and therefore too large a population is left after applying the
hypotheses: a group in which most people will answer to the hypothesis. In this study we have tried to focus the attention more on the “up front” measurable characteristics of behaviour, which differs from those based on rather general background characteristics. For example, when someone has had a higher professional education: in the role of the exchanger within a child pornography network (exchanger of material) he will show a certain download or surfing behaviour which is indicative of this role, while the level of education does not do this. The internet-related character of phishing, child pornography and advance-fee internet fraud leads to more or less specific internet behaviour for each offence and to conditional characteristics derived from this behaviour or the behaviour with connections to the internet. The behaviour-related characteristics often present an important basis for hypotheses about offenders in their various roles and their activities. It appears that a wide frequency band (the amount of data traffic up and downstream) is an important determinant for the role of exchanger in a child pornography network. Have more personal background characteristics literally disappeared to the background? No, because they remain necessary to define start populations which give meaning to the hypotheses applied to this population group. For example, the amount of data traffic only could indicate child pornography if it can be connected to a sexual interest for children. In that case, it could be chosen as start population for people with a known paedophilic inclination and to apply the hypotheses on them. For a number of hypotheses this kind of start population is important while others could be tested without pre-selection.

At the hand of this reasoning a main classification was made into two kinds of offender characteristics: actor typed (characteristics which are connected to the offender as a person), role typed (behaviour characteristics which ensue from the role taken). Social demographic, social psychological, social economic and some criminal characteristics are counted among the first main category. The second category is subdivided into offence behaviour, dynamic behaviour, static internet behaviour, dynamic internet behaviour and use of hardware and software.

Static internet behaviour recognizes as underlying dimension, among other things, whether a person does or does not have a hidden IP-address or does or does not make use of bullet proof hosting. In comparison to this, dynamic internet behaviour stands, a.o., for a rolespecific surfing, downloading and uploading behaviour. The classification has not been sufficiently crystallized but is an initiative for a functional and logical categorization of behaviour characteristics in combination with roles that appear in the working-process of cybercrime. The characteristics were developed in order to detect actual offenders of cybercrime. This does not imply that the characteristics could also indicate beforehand who
runs a greater risk of being an offender and who does not. Especially more or less real time behaviour (behaviour close to committing a cybercrime offence) is interpreted with these characteristics and not the sensitivity or the vulnerability to future involvement in criminality. Characteristics and hypotheses are not drawn up beforehand as the risk profilers defining a certain target group or subject with a potentially higher chance of becoming offenders, victims or objects of abuse. The characteristics do not have this predicting value. At most, they are usable, with the help of insights derived from the ‘stepping theory’ or ‘gateway’ theory, to indicate a following step in a criminal career, just as the photographer with debts and involvement in the regular adult industry, who stands a greater chance of getting involved with producing child pornography; or the internet marketeer for whom it is a small step, technically, towards illegality when he sees his turnover diminish. But these are not the profiles which detect large high-risk groups.

**Working methods**

Phishing, as well as child pornography and advance-fee internet fraud have their own business procedures. The acquisition of addresses and customers and the recycling of criminal proceeds overlap between the various processes. These are generic activities which clearly are not connected exclusively to the product which is generated. In the battle against criminality one could profit from those generic activities by not considering each and every offence as being an exclusive one with its own combat specialist but by bundling what is known about phishing and child pornography, on the basis of the corresponding modus operandi in both types of offences.

Evolution-wise, the working methods of the three researched offences differ strongly from each other. The phishing process has developed while coping with contra-strategies of their targets and the security industry. Phishers are involved in a kind of race in which they constantly have to go in search of different techniques in order to steer clear of new obstacles or to attack as yet unprotected targets. This manifests itself in constantly changing modus operandi of at least parts of the working method. The child pornography process and committing fraud with advance-fees knows a lot less evolution. They are also less dependent on the internet than the phishing process. The method usually stays the same, only the shielding of this working method increases so that it becomes less recognizable and traceable.

**Degree of organization**

In the phishing process, one intellectual offender (the sponsor) supervises the entire process and therefore also the other roles. It appears from investigation files that all sorts of relations run from this offender to his employees and facilitators. Family
members and confidants are called upon as members of the peer group because of the greater chance at secrecy than would be the case with random strangers. Everyone’s motive is the same: money.

The supervision within the professional production of child pornography is divided according to the sequence of that process. This is not the result of explicit agreements but of the divergent characteristics and the necessary skills of the process phases: production, distribution and consumption. These are successively supervised by the producers, distributors and moderators. This implicit division of tasks seems to be determined historically, in which the printer of the sex books was always someone else than the salesman selling them from under the counter, and the original producer. With the arrival of internet this division seems to be sooner confirmed than outmoded. Under the influence of internet development, distribution and consumption of child pornography have evolved much more than its production. Even on the “set” itself it has happened in this same way for a long time with, as most important evolution, the change from analogue to digital and from photographs to video. Not until the last few years, and also the coming years, are more fundamental changes in this field becoming visible with certain consequences for the recording studio, such as “life view” (watching, interacting and intervening on the set during the abuse), integration with the actual game environment, and increasing video interaction between the consumer and the footage. The producer has the most classical organization with a group of freelancers around him. His motive is chiefly money and less his sexual predilection for children. The distributor mostly makes use of internet facilities originating from facilitators. The relationship between them is more of a customer-supplier one than that of a boss/employee. His sexual predilection is not, or not exclusively, for children and his distribution activities are broader than only directed at child pornography. The moderator operates within a relatively tight network structure which is, in fact, organized on the internet as a news group, chat room or private forum for members with a sexual predilection for children. His status was acquired by the many exchanges of new footage. His supervision is based on the literal possibilities to refuse or remove members of the news group or the forum. Owing to his position, he knows a lot about the members and their backgrounds.

In the scope of advance-fee internet fraud, the organization is even more disintegrated and the job owners operate more and more for themselves or in small combinations. They probably do make use of the same facilitators, such as translators, script writers and counterfeitors. In literature, financial associations with the much more organized drug business and human trafficking are also insinuated. Others suspect supervision from ostensibly lose cells by Nigerian
directors. The usually somewhat primitive working procedure within advance-fee internet fraud points to a limited knowledge of ICT and internet applications. The working procedure is organized more classically with a lot of direct fax and phone contact with victims and knows no “sophisticated” use of internet functionalities. Not yet; as it appears that swindlers also increasingly find their way to social network sites in order to find the lead to specific target groups who they can ‘target’ with a specific story with a higher chance at success. This development shows similarity to the working procedure of phishing: more and more specifically tuned to a limited target group (spear phishing).

Specialization
From research of investigation files and internet research it appears that the various contributions by accomplices and partners in crime may often be used in more than one offence. A counterfeiter can offer his services to more than one criminal who is occupied with various forms of criminality. It remains to be seen whether the counterfeiter himself is occupied by more than one form of cybercrime but his services are exploited in various forms. The same is true for the addresses which are hacked or harvested: they are immediately snapped up by offenders of advance-fee internet fraud as well as by phishers and the distributors of child pornography spam. It takes place according to the same economic principles as in the “real world”: offenders who are only concerned about financial gain try to sell their products as often as possible or use the techniques which have led to one product for other products. Precisely because certain parts of the working procedures in cybercrime are multi-functional as MO-elements, we come across them in various places. The general assumption is that people who have at their disposal and also make use of illegal internet practices wish to earn a return that is as high as can possibly be for these practices by adding crime domains wherever possible, for which this same knowledge can be put to use.

In the phishing process more specialist roles are involved than in child pornography or advance-fee internet fraud. This can be traced back to the high level of technical operations which, for one reason or other, are necessary to make a success of a phishing operation. Phishing also makes use of the internet in nearly all its steps of progress, contrary to child pornography and advance-fee internet fraud. This implies that many more roles are also related to the internet. During the production process of child pornography and advance-fee internet fraud fewer of these kinds of cybercriminals are involved than in phishing.

In advance-fee internet fraud it is more or less limited to providing the addresses onto which the swindlers can release their fantastic scripts. In child pornography the internet specializations are involved especially during distribution of the material and the hiding of said material. But in that case it is not only the experts
who are used but also the generic products that specialists put on the market. One could think of encrypting techniques or the hiding of illegal footage in legal material (steganography).

When we look at the specialization of the offenders it seems as if the trend of parts of the MO’s becoming more generic is also of influence. The universality increases especially with activities which are not connected to the specific offence and will probably increase even more. These are precisely the activities or services which coincide with the contribution of facilitators and that also correspond with their supporting role; they have no idea to which offence or which irregularity their services or products contributed. Activities which initially asked for high-grade knowledge, we now see appearing on the market as DIY-kits, as the demand increases. Activities which initially were specific for one certain offence now also become available for other offences (recruitment for money mules, massmailers, bullet proof hosting, the use of proxy servers, etc.). One could call it a development of “outsourcing”, where initially, offence by offence, specialized tasks were taken over by generally operating facilitators whose services are suitable for a number of offences, as well as legal processes. This development occurs amongst the services of the facilitators but will possibly universalize a number of activities of the employee in the same way. For phishing it is true that under the influence of increasing protection by potential victims, the development of the phising part increases in such a manner it is no longer worth the trouble for the individual enthusiast. One must make use of the results of a spectacular hack of an address-server because the know-how within their own role complex is simply lacking. At this moment still specialist gaming tasks in the production of child pornography, on the other hand, are probably becoming more computerized, which is also facilitated by the increasing demand. With advance-fee internet fraud the need for specific target addresses shall increase, or the attention will move to countries and victims with lower “awareness”.

Indications for these presupposed developments are especially derived from the internet itself. By mirroring the developments within legal branches (marketing, gaming, regular porno) in illegal working methods in the scope of phishing, child pornography or advance-fee internet fraud, by the demand and supply of personnel, apparent in the many websites and, for example, the supply of products offered by tool suppliers such as massmailers, phishing kits or nude patches. Besides, it also appears from research dossiers, for example, that there is rumour of recurring MO’s in various offences or address files which appear to originate from the same sources. Unification of working methods or, in this case, of addresses, means that it concerns a relatively new file which, as yet, has not been copied again
or distributed. The professionals will be able to afford such a virginal file and purchase it from insiders.

Resuming, two general developments arrest the attention when, for convenience sake, we sweep working processes, degree of organization and specialization of the researched crime processes into one big pile. The first one concerns outsourcing: what was formally considered an element of a certain offence is now organized more and more generically. For example, in a number of offences, false identities are necessary, so why go through the trouble of filling that need as initiator yourself when you can also just purchase them according to the latest state of the art. (False) credit card data form the basis for renting server space in the framework of phishing but also for hosting child pornography. Tool suppliers do not deliver their massmail programmes or encrypting tools exclusively to one offender within one type of offence but sell them wherever they are needed. Depending on specific modus operandi, it could concern phishing, as well as child pornography and advance-fee internet fraud. Mass mail occurs in all three business processes as an important way of obtaining customers or employees. In short, for the organization of criminality the same principles apply for division of work as for those we encounter in regular organizations. Among facilitators, out-sourcing leads to specialization. Considering the increasing size of the market it is becoming profitable to concentrate on professionalism/know-how and study it in depth, as much as possible. Specialization in a content related domain such as porn with a subsequent broad offer of services is replaced by the offer of specific functionalities for several functional domains.

The second development concerns the increasing encryption at the basis. Not only are certain MO procedures encrypted but, where, in regular software, encryption has become ingrained, this is also true for the MO’s. For example, when it concerns concealing authentic identities, accepting false, falsified or stolen identities, organizing money transfers and choosing methods of money laundering.

**Concurrence of various forms of (cyber) criminality**

It so appears that cybercrime hardly ever stands on its own. With the help of occasional theory it is assumed that when criminal activities, which belong to the skills of an offender in a certain role, are also suitable for other forms of (cyber) criminality (cross-over crime), there is a big chance that this will actually take place. It does not matter much to the money mule whether he is brought in on a phishing operation or to complete a credit card fraud. In this way, the tool supplier who produces software development kits for malware will not limit himself to just phishing. The connection between offender roles within respectively phishing, child
pornography and advance-fee internet fraud have been divided into support offences, which are preconditioned to execute certain cyber offences; embryonic offences, which function as nurseries for the committed cybercrime and supression offences, which arise from competition between offenders who are at cross purposes. Besides, we determine association offenses which are committed by the same offenders, but not part of the described offenses.

Support offences are necessary for the primary criminal process. One has to stay involved in order to complete this process. Phishing does not only consist of one offence and that is also true for child pornography and advance-fee internet fraud. Identity fraud, hacking, credit card fraud, forgery, spreading spam and money laundering all occur, virtually per definition, in the production chains of the researched offences. Specifically in connection to child pornography, violent support offences occur in two ways: as a means of exerting pressure on the child or its surroundings and as intrinsic theme which is incorporated in photo’s or films. As another kind of support offence, corruption represents a part of advance-fee internet fraud in the case of customs officials.

Association offences are individual offences which are committed by the same offenders parallel to other offences and not just as part of an offence. The Timeson line showed a connection between child pornography and terrorism. Steganographically manipulated pictures of child pornography were said to contain secret messages and supposedly served as means of communication between the members of a terrorism cell. A certain terrorist mindset was suggested where the privacy of the networks in which child pornography is exchanged is also considered safe for the exchange of other information which also has to remain hidden. Actually, these kinds of messages were not discovered in the pictures involved, at least none of the consulted sources showed any indications. Also, certain offences are more likely to being committed when one is more acquainted with phishing techniques. The Greek case “Avanture” is an example of that, where the phisher was after obtaining a game still in the making with the accompanying entrance codes. In this kind of intellectual ownership fraud (piracy) phishing has become more or less synonymous for hacking. Other examples are hacking and cracking of regular software.

Numerous other kinds of criminality (association offences) are ascribed to perpetrators of advance-fee internet fraud, among which various frauds, drugs trafficking are, human trafficking and trafficking of stolen cars or other goods. Nigerian gangs are called “poly crime organizations”. Considering the similarities between the working procedures and the various kinds
of fraud, a connection to advance-fee internet fraud could be expected in the present internet era. Concretely, it concerns mortgage fraud, insurance fraud and identity fraud. In pre-internet times Nigerians in the U.S.A. were already known as master counterfeiters.

Circle patterns are noticeable, as well, when a product of phishing (address data, credit card data, log-in data, and identities) is used in other kinds of cybercrime. On average, little is know about the preceding careers of cyber offenders in their various roles. We suspect that a case like that of the Russian Leo Kuvayev is not unique in its sort. As Russian/American spammer for illegal software, illegal medicine and porno, he and his accomplices were also involved in developing botnet viruses. He bought wide bullet proof hosting in Brazil, China and Russia and used an enormous number of domains (with false information) which rotated in order to prevent detection by filters.

That little is known about embryonic offences does not imply that is does not exist. We know, for example, to what extend the statistics probably mirror the focus of the criminal investigation authorities. In the case of child pornography they are especially about known paedophiles and little about the populations which, helped by the internet and the great amount of sent child pornography spam, have joined the devotees of child pornography. Without a controlling group one does not know to what extend conclusions are exclusively true for the category of paedophiles. The arrested offenders of advance-fee internet fraud could also just have been taken in as “first offenders” because of their oafish working methods, while the actual hard core frauds and perpetrators of other offences remain out of reach.

The research conclusions, in any case, do not rule out that there may be unknown historic offender behaviour among “known” or “unknown offenders”.

Finally, a fourth group of offences may be distinguished which is not necessary to complete a cybercrime but is incited by that offence, as it were. The rip deal, of which the so-called Sneker botnet appeared to be a member, is an example, as is the murder of the Russian spammer Vardan Kushnir in 2005, or the competition between the botnet herdres who attempted to steal each other’s zombies. We have classified these forms of related criminality as suppression offences.

If we are to believe some dark sources intellectual ownership fraud also takes place within the porn business. Precisely in countries with a low tolerance towards porn (Korea, for instance) one could be found guilty of this. This research did not find any concrete examples of competition between those concerned with the production and purchase of child pornography resulting in committed crimes against each other. This does not mean to say that suppression offences do not
occur in that world. The internet related character of the material certainly induces frequent copying and sending. Moreover, (DVD) compilations are composed from it. It could be that this leads to “copyright” conflicts. On the other hand, the hidden character of the circuit, the mutual illegal character, plus the mutual dependency on new material also creates a sort of balance. The, on its own, illegal character of the business perhaps is the cause that little is exposed: mutual interdependence or conflict regulation as a foundation for avoiding conflicts. The same line of thought also applies for phishing. In the environment in which these kinds of offences take place, there are also alternative measures available against competitors or those who have made a faux pas, in which one can keep one’s hands clean and minimize the risk of discovery within the enclosed group of producers and devotees. Measures such as, for example, tipping the investigation authorities about activities of the competing groups. For that matter, the markets for phishing, child pornography and advance-fee internet fraud seems to be enormous and not easily saturated.

**Knowledge gap: perpetrators and modus operandi**

Certain elements of modus operandi, such as the technical ins and outs of an often recurrent phishing operation or of the downloading of child pornography, are very well-known. Of others, such as the production of child pornography or the managing of the many Nigerian scammers, there is, at the most, just talk of presumptions which have little or no connections. The degree of insight into MO’s and roles does not depend so much on the secrecy of certain criminal activities but on the subject on which the Dutch criminal investigation authorities have directed their spotlight. If one were to look more carefully at the front of the production of child pornography, without being restricted by a national perspective, then more of it would be visible.

This conclusion is limited to the areas of phishing, child pornography and advance-fee internet fraud. Knowledge about the offenders has a classic dimension only, where one actually does not wonder enough of what use this knowledge is. On the internet, a new dimension could be added, besides the general social-demographic characteristics, namely the behaviour. Internet behaviour is easier to follow, to a certain degree, than behaviour in the real world. Unfortunately, there are a number of blanks when describing the behaviour before the investigation. For example, phishing is observed mainly by banks in the form of increased traffic to the website, increased downloads of certain logo’s and website frames and, afterwards, by reports. We are familiar with the proces of a phishing attack but it could take place in peace and quiet. Offenders do not have to be conspicuous yet. The importance of banks in recognizing phishing attacks is mainly directed towards
stopping the attacks. That is to say, the bank is already satisfied when the security leak has been sealed or the spoof website taken off the air. The actual detection part is of minor importance for them because limiting the damage, as soon as possible, has priority.

As far as child pornography and Nigerian fraud are concerned, we are especially interested in the Dutch offenders within the entire roles complex. However, we do not know which offenders, or even which offender roles, can be found in the Netherlands. It is clear that the Netherlands offers possibilities for all the facilitator roles, the “initiator”, or organizer of 4.1.9-fraud and the producers of child pornography.

Current research is aimed especially at social-demographic factors. It is very difficult to make them operational. It is not very differentiating when we realize that 86% of child pornography purchasers are men above the age of 26, usually higher educated, single or married and have an above-average income. They still denote a large group of people. Steering towards suspicious (internet) behaviour does not have this disadvantage because those that do answer to the suspect behaviour profile can be distinguished from the masses. This does demand that we cannot only describe suspect behaviour but also make it operational within internet use.

The contribution of hypotheses to influencing cybercrime

Behavioural characteristics of offenders are not only useful but also necessary for a pro-active battle. Rather simple and much simpler than the more general offender characteristics, they may be applied in hypotheses and accompanying search-strategies. Internet has a big advantage in this. It forces perpetrators of various offences into the same sort of format. That format works as a sort of “extruder”: that which enters in the front as absolutely incomparable motifs and behaviours, leaves through the back as organized manners of a similar nature that fits the demands of internet usage. Offenders who use the internet in their offender roles convert their behaviour into the same internet dimensions, so that, in theory, it is possible to line them up next to each other (classify them as equals) but one does have to know how to make them operational beforehand by means of the hypotheses and afterwards by the means of the test results of these hypotheses. That asks for mobilization of the sources at the hand of which application and testing of these hypotheses can take place. For the time being this may turn out to be the biggest problem. A number of generally functional “helping hands” could be suggested. In so far as the offence, which is to be tested at the hand of hypotheses, is considered to be a more serious one, the chance of co-operation with those tests by non-judicial source managers, increases. In the case of the afore-mentioned photographer, whose purchase behaviour of software and hardware, in
combination with several other identifiers, made for a higher chance of involvement in child pornography, the chances are higher that, for example, the software supplier Adobe co-operates with identification than would be the case with only spam. Approval by the representatives in the field of the hypotheses has an important psychological effect. By endorsing a hypothesis one says, in fact, that there is truly something the matter with these activities which/people who fulfil the hypotheses. Meaning that there is only a little chance of there being activities/people among this group with whom/which nothing is wrong and this causes the barrier for really sharing information to disappear for the greater part. More timely endorsement of these hypotheses will therefore not be without obligations.

If a hypothesis is not only a presupposition but is so sharply defined that people who appear to fit the hypothesis are faulty by definition (even without having to determine this from the population arising from the hypotheses), then the chance of co-operation increases.

Precisely because it is mostly not known how offenders operate in regards to certain forms of cybercrime and how they participate in various related roles, the ideas dealt with in this report have a presupposing character, per definition. The applied research approach originates from the investigation into blank spaces or ‘dark number’. Actually, it is remarkable that, after all these years of supervision and investigation, there still is very little factual knowledge available about general offenses and that so much still has to be presupposed. Cybercrime seems to be a positive exception here, which is mainly due to the technical platform to which it can be traced, more (phishing) or less (advance-fee internet fraud). This platform registers a large part of the behaviour for which the platform is important, however this behaviour is hardly explored. The demand for ‘which hypotheses’ has supplied descriptions of modus operandi and role complexes. Parts of this are already known: they have actually been encountered in practice. Other parts came into being on the basis of estimates and the opinion of specialists. But could these hypotheses also be used as a basis for influencing? We found that the hypotheses have not come any further than a “sheet of patient paper”. Application of the hypotheses and an analysis of what surfaces after the application is a condition for judging their final strength and whether they are (accurately) able to separate the Bad (and their behaviour) from the Good. On the other hand, not infrequently are policy choices based on weaker ideas about connection and behaviour and criminality than are presented in the hypotheses. So, on its own, a simple hypothesis can already emanate a certain power of persuasion, which could give an impulse to the various policy processes. The hypothetical character of the MO-
descriptions and of the role complexes already has an influencing effect, in spite of the fact that testing has not even taken place.
Their effects arise from the plausibility of what is stated in the hypotheses. This development is not limited to the policy process. At the time of the research, the field had already started working with these various ideas, eager as professionals are to try out new things and eager as they are to want to get a grip on the capricious reality of cybercrime.

Besides this direct influence on policy and implementation, it seems that this type of thinking in MO-elements, the variations involved and thinking in role complexes of offenders and victims contributes to ordering the many fragmented insights. It could be seen as a form of cumulative knowledge. Every new case or manifestation could be compared to it and, as far as newly proven MO’s are concerned, they could be incorporated.
The same is true for associations which arise, as a result, about alternative MO’s or as a result of the possibilities of misusing new internet related developments. It is easy to use an MO-scheme or role complex to literally post the ideas one has about barriers or interventions, so that one can also see on which parts of the process these sort of measures have a grip and on which they do not. To prevent these ideas becoming arbitrary, they have to be based on other hypotheses, at least; namely, on the assumed relationship between measure and effect.
The second part of the methodology, which was not carried out in full, supervises the forming, the application and testing of these kinds of intervention hypotheses.

Research restrictions
The lack of actual international contact has proven to be a handicap for the research. As often as possible, an attempt was made to compensate for this by tapping human interfaces within the Netherlands for their knowledge of the situation and the developments elsewhere. But that has its restrictions. Not everything is known and, moreover, the knowledge was acquired from a Dutch perspective. Direct contact with sources is therefore of essential importance, also because the ability to change the original source data into hypotheses useful for problem solving in an inventive way, is not everyone’s gift. Because of this cases were missed which should certainly have been completed in a testing phase. The Dutch perspective will also work restrictively towards the future because how responsible does the Netherlands feel and could it feel for those parts of MO’s which do not entirely belong to the Dutch territory?

Critical success factors of the research methodology
As it is, the applied research methodology is nothing but a basic form of conducting
research. What is extraordinary and difficult about it is that an attempt has been made to give a hypothetical answer to what is considered as intangible/incomprehensible, not just an arbitrary answer but one that fits in or connects to the knowledge one already has and which could, at least, be given the predicate “plausible”. One first obvious condition is that one is able to coherently present the knowledge acquired, for example, from the many investigation studies which were executed in probably different surroundings. This research has proven that this is what is lacking. Judicial, as well as non-judicial organizations usually have a casuistic attitude. The moment one case is solved they are off to the next case.

Moreover, not every case is suitable to base hypotheses on. Investigation services understandably tend to publish extraordinary cases, especially those with which they also illustrate their own expertise: we managed, again, to round off a case with so many (new) aspects, successfully. The FBI press releases are a very clear example of this attitude. It is especially the extraordinary or a-typical character which makes these cases so unique that they cannot be generalised, while that is really the intention of the followed methodology: investigating cases which answer to a certain generic pattern and not just investigating the one case with that very specific pattern. Without any exceptions, working with hypotheses seems to be welcomed profusely by representatives in the field because of their characteristic as the accumulation of knowledge. One recognizes one’s own casuistic attitude and sees great advantage in accumulating knowledge from various cases, to be able to end up at the front of cyber problems (pro-active).

Everyone who contributes to the forming of the hypotheses should also have the final hypothesis at his disposal in order to be able to experience the feeling of exchange. But the question sent along with the respondents is also very clear: who is going to do it?

**Research and action research**

The research started as an *action research*, in which a limited number of hypotheses serving as starting points would rapidly proceed to the actually applying and testing of these hypotheses in daily practice, in order to, afterwards, reject the proven insights of the hypotheses or extend them into other hypotheses founded on new insights. In the end, the research had more consequences than was originally accepted because of which the actual application and testing of the hypotheses did not took place. Postponing the application and the testing carries the risk of hypothesis after hypothesis being piled up and the insecurity, as the pile grows higher and higher, keeps increasing. If, in the end, it appears that the first hypothesis has to be rejected, than this also has far reaching consequences for all
the hypotheses based on this first one. Moreover, reality just keeps on developing, certainly in the case of cyber space, with the risk that once we are at the point of applying and testing a hypothesis, the MO has already evaluated. That is why the hypotheses in this rapport are, as often as possible, presented as start hypotheses on an equally low level in an imaginary hierarchy, with a slight mutual dependency. Shortcycle development, application, testing and continuing to develop the hypotheses is a very important recommendation for the use of this methodology.

**MO-description and role complexes**
The use of descriptions of actual and/or imaginary presupposed modus operandi and of role complexes is essential for the methodology. As more hypotheses are applied and have actually been tested, the MO- and role models adopt the form of knowledge. When this knowledge is subsequently made operational in investigation methodologies, it will be advantageous to the battle against criminality. MO-models and role complexes in their ultimate form are not only a reflection of cumulative knowledge (evidence based), but also a conditional necessity for developing new hypotheses. To be able to assess whether hypothetical interpretations of blank spaces in the process of criminality are plausible, one will want to review the entire process. The same holds true for certain presupposed roles and behaviour characteristics of offenders who one will also want to place within the perspective of a total role complex, in order to get some feeling for relevance and merit of investigation. For one who is entirely unfamiliar with the business process of a phisher, a hypothesis about internet marketeers will also come entirely out of the blue.

The use and keeping up-to-date of an MO-description (as complete as possible) and of role complexes prevents, moreover, that the focus is only on parts of a modus operandus which take place in the Netherlands. By looking at the complete story one also gets a different perspective of one’s own territorialism. Perhaps (other) ideas will arise about how the battle against criminality could be served with a certain approach in a certain country of source, and vice versa. The length of one’s own criminal justice arms is most probably a lot less decisive than the early signalling or intervention by private parties abroad.

**Hypothesis application and hypothesis testing**
The moment a hypothesis is applied and a number of people or activities appear to fit, does not mean that it has been tested. Not until it is determined, at the hand of the elements of that population, whether and to what extend they actually relate to what the hypothesis means to indicate, can we speak of testing, with the rejection and/or support of the hypotheses as a final result. When using the
methodology it is of the utmost importance to differentiate between application and testing. Is the result of an application of a hypothesis of little use on its own? No, because when one realizes on what many of the choices for policy or measures are based, then those are, more often than not, vaguer ideas than those that are the result of the development of a hypothesis. For police purposes, that could be of great importance.

The “National Infrastructure against Cybercrime”
The ideas about the National Infrastructure Cybercrime, such as were placed on the horizon as a vision by the NPAC (Faber, Mostert & Oude Alink, 2006), are geared (freely translated) towards three questions:
- Does sharing information between parties have added value? And, if so,
- Is institutionalization of this sharing of information while retaining the added value, necessary, and if so
- In what way should this institutionalization preferably take place?

In the core, The NICC action research could be traced back to these questions. To see whether by already acting, temporarily, according to the perspective on the horizon, answers to these questions could also be generated. This report is about the phase in which the factual action has not taken place yet. Nevertheless, there are a few connotations to be made on the basis of the results of the research.

In the first place, it appears that the willingness to actually co-operate (sharing knowledge and information) on the technical executing level and with the people who are directly involved, is high. The realization that this co-operation could result in something, is more than present, also because the professionals (on this level) see the concrete result of this co-operation in terms of caught offenders, prevention of attack or less financial disadvantage for victims. Institutionalization of this co-operation is not what it is primarily about, on that level. The wish to co-operate does not seem to be determined so much by the social or organizational return either, but rather by two factors especially:
- the professional drive to want to sink one’s teeth into ever renewing, technically challenging questions,
- indignation about the fact that there are criminals who dare to dirty the domain of the respective professional.

The strength of the co-operation on the basis of interest and indignation is that it happens as a matter of course, even if the parties involved have only known each other for a short time. Structuring the co-operation at this level will probably shy people off, also because, in doing so, the formal accountability for what one must
do within this co-operation and what one should not do is broadened. Moreover, this responsibility goes much further and is much broader than the context of one’s own function or organization. Structuring will turn out to be a result of the co-operation which increased through practical experience, rather than that it is about a yet to be designed start situation.

In the second place, we found that, with hardly any exception, all parties with whom we spoke and co-operated quite intensively viewed the virtual world from their own (somewhat small) perspective. This study proves that, for example, insight into the MO’s of spam and phishing could be of greater use in the battle against advance-fee internet fraud and that, in reverse, knowledge about identity theft and fraud within this form of cybercrime could be of importance in the battle against phishing. The limited perspective of the involved parties, strongly coloured by their own core task and underlying interests, prevents that knowledge from various domains and criminality themes is actually gathered in this way. In or above the parties, there is no active function from which one could have a holistic view of the total field of cybercrime (and non-cybercrime) and from which one could find the connections, indicate the overlaps or know how to generate the generic and exchangeable knowledge.

In the third place, we approach the three questions in a more abstract-philosophical way. Both the real world and the virtual world are the result of the years and years of interacting action and interaction without there being any central direction. Our society apparently stays “in control” in the same way as it was created and is being created: as sum of all sorts of actions and interactions which, collectively, lead to a certain level of well-being, usually without aiming at express control; often in such a way and so interrelated that it causes the daily continuing process of interaction. Their exact contribution to “control” can no longer be traced but it certainly has effect. It is only a small shift of paradigm to not only see the entire picture of interactive mechanisms as the reason for which way the wind will blow in the Netherlands but also as condition for maintaining this situation and its continuous development. In present society there is no longer one exclusive party which can completely control the developments, even if we make it appear as if this is so. In order to maintain this state of “control” the function of the investigation is actually no longer designated to the police only. This function has been distributed across society, often implicitly and sometimes explicitly, even if specific tasks are, of course, also designated to and reserved for specific organizations. When we connect this view with the above mentioned third question, particularly, then the institutionalization of the approach towards cybercrime, in the gist of designating certain information to a specific group, will
have little effect. A choice like this would not be contingent with the underlying analysis. In the mean time, we also stated, that there are a few functions which view the world of connection within the domain of cybercrime, for example, from a more holistic perspective. When we add this to the experienced feeling of the added value of sharing information on the professional level, in any case, then a more fitting idea, closer to the characteristics of cybercrime, is obvious. A few people are necessary (and that is not the same as an organization) who focus continuously, from a holistic point of view, on the connection between mutual forms of cybercrime and classic criminality, doing nothing but generating hypotheses by which executing professionals in the various, more focussing, organizations are triggered and take off with the idea. Apart from inventiveness, the strength of these few people should be, especially, that they are able to translate the holistic points of view into the core tasks of the organizations which should, and probably have to, be able to do something with them. In the functional approach of this study it is fitting to state that the organizational positioning of these people is not really important. It is the actual function which matters and which, for example, can also be proven from everyone’s individual anchoring in the various organizations in the field.

‘The proof of the pudding is in the eating”
Even if hypotheses are also useable independently they are meant to be utilized in the form of search strategies and to be tested on the basis of the acquired results. The HDI67-methodology goes further than the five taken steps and includes the testing of the hypotheses in actual practice and the continued bringing up to date of the developed hypotheses by means of feed-back, as well as the development and the application of matching interventions. It is actually part and parcel of the forming of hypotheses that these steps are taken. Contingent with the characteristics of the internet and internet related criminality, it is recommended to do this from a simple flexible structure consisting of a core of holistic and inventive hypotheses developers and making use of the professionals in the field. This can take place via the information interchange idea of the NICC, though the parties should not only be brought together on the basis of similar vulnerabilities or threats but also around hypotheses and the available arsenal for investigation and intervention. The involvement of these parties could vary with the content described by the respective hypothesis and the necessary sources of data needed for testing.
In order to avoid that all sorts of preconditions need to be fulfilled and that a lot of

67 Hypothesis Directed Intervention

340
data has to first flow though the internet before application can take place, perhaps an experimental base will offer the Police and Public Prosecution a chance to hitch a ride, with the condition that the orientation from these experimental projects is broader than just on criminal investigation and persecution exclusively, because otherwise they will not be able to handle a large part of the hypotheses which explore private domains.