Cyberdaders: uniek profiel, unieke aanpak?

Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin

Eindrapportage – December 2019

Dr. W. van der Wagen[1]

Dr. E.G van 't Zand-Kurtovic[2]

S.R. Matthijsse MSc[1]

Dr. T.F.C. Fischer[1]

Met medewerking van: Sophie Keizer en Nicole Alberts

[1] Erasmus Universiteit Rotterdam, Sectie Criminologie

[2] Universiteit Leiden, Instituut voor Strafrecht en Criminologie

COLOFON

Opdrachtgever

Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Afdeling Externe Betrekkingen (EWB) Ministerie van Justitie en Veiligheid

Koningskade 4

2596 AA Den Haag

Onderzoekers

Dit onderzoek is uitgevoerd door de sectie Criminologie van de Erasmus Universiteit Rotterdam in samenwerking met de Universiteit Leiden. De betrokken onderzoekers waren: Wytske van der Wagen, Elina van ’t Zand, Sifra Matthijsse en Tamar Fischer, met medewerking van Sophie Keizer en Nicole Alberts.

Illustratie voorblad: https://tumblr.com

Summary

Background and research question

Recent developments indicate that hacking[3], DDoS attacks[4], ransomware[5] and other forms of cyber-focused crime[6] are on the rise among both adolescents and adults. The scientific knowledge about cyber offenders is limited, anecdotal, outdated and fragmented. This research attempted to generate more systematic knowledge about the characteristics and profiles of juvenile and adult offenders of cyber-focused crime, as well as to provide insight into appropriate and effective interventions for this offender group. The following research question has been addressed in this research:

"What are the differences between the profile(s) of cyber offenders and offenders of" traditional "crime and what are the implications of those differences for the nature of interventions for cyber offenders?"

Research methods

In this qualitative research a combination of different research methods was used. First, two systematic literature studies have been conducted: one focused on characteristics of cyber offenders and one concentrated on interventions for cyber offenders. The first search yielded 99 sources about characteristics of offenders of cyber-focused crime, whether or not compared to traditional offenders. The second search yielded 25 sources about interventions aimed at offenders involved in cyber-focused crime. Secondly, expert interviews were conducted (29 individual interviews, 2 focus groups, 1 expert meeting and 1 round table). A total of 52 experts from virtually all partners in the security chain (police, Public Prosecution Service, judiciary, legal profession, (youth) probation service, Child Protection Board, Halt and care providers) were interviewed as well as industry experts, researchers and freelancers who have knowledge about cyber offenders and/or interventions. Thirdly, 14 interviews with adult offenders were conducted. Of these offenders, the majority was convicted of one or more cyber-focused offences (including hacking, DDoS attacks, virtual theft[7]) and the minority was involved in those crimes, but never got caught. Hacking was the primary offence in most cases. The judicial interventions imposed on the offenders mainly concern community service orders, but some offenders also received a (conditional) prison sentence, contact prohibition, fine, compensation or electronic detention. Four offenders did not receive any judicial intervention and two offenders were still awaiting their criminal case at the time of the interview.

Limitations of the research

The research has a number of limitations. First, the literature study has its limitations. For example, relatively much literature has been found on hackers (albeit much outdated literature and usually small samples), but little information was available on offenders involved in other forms of cyber-focused crime such as DDoS attacks and ransomware. In addition, only a few (effect) studies were found in which the application of traditional or cyber-related interventions to cyber offenders was examined. Hence little systematic knowledge is available about the effectiveness of interventions for cyber offenders. Secondly,

[3] This refers to the unlawful intrusion into a computer system.
[4] This refers to disrupting or breaking down a system through overloading it with traffic.
[5] This refers to malicious software (malware) that can be used to take a system "hostage" or block it so that the victim has to pay ransom.
[6] Cyber-focused crime refers to crime in which ICT is both the means and a substantial target. In the full Dutch report we use the term 'cybercrime in the narrow sense' [cybercrime in enge zin]
[7] This refers to theft of goods in a virtual game.

regarding the expert interviews, various respondents only got involved with a limited number of cyber offenders. The answers of these experts are therefore based on a small number of cases and their perceptions are perhaps also partly influenced by stories from colleagues, images from the media or the social debate. Thirdly, the interviewed offenders form a selective group (adult, majority convicted and hacking in most cases being the primary offence). Consequently, we obtained less information about other types of offending. Finally, the results depend on the self-report of the offenders. The offenders may not have reported all their delinquent behaviour, withheld recent offences or, on the contrary, portrayed their criminal career as "more successful" than they really were.

Findings

Part 1 Offender characteristics

The first part of the report focused on the specific characteristics of cyber offenders and the extent to which different offender profiles can be constructed based on those characteristics. Additionally, the characteristics were compared with the characteristics of traditional offenders, so that differences among them could be described. In this context we distinguished (offline and online) *criminogenic* (risk factors that contribute to the delinquent behaviour) and *protective* factors (factors that can prevent or restrain delinquent behaviour). In the analysis of the offender group, we used insights from various criminological approaches such as the differential association theory[8], neutralisation techniques[9] and the rational choice theory. [10] Concepts have also been applied that have been specifically developed to explain online and technical aspects of offending such as the online disinhibition effect[11], digital drift[12] and mastery. [13]

Profiles

During the research we came to the realisation that a simple clustering or profiling based on the presence or absence of certain characteristics does not produce a realistic picture. The offenders have different characteristics and factors (personal and contextual) and specific motivations (such as mental challenge or status) that occur in different combinations and degrees. This then leads to (a certain development in) the delinquent behaviour (criminal career). For this reason, the profiling of cyber offenders has been approached by describing the impact of various characteristics and factors on the delinquent behaviour, both individually and in their mutual coherence.

Background characteristics

Literature has shown that cyber-focused crime is relatively more often committed by young men with a non-migrant background and a reasonable to good socio-economic background. In the subgroup of financially oriented cyber offenders, the age of onset is generally higher. There are also indications that these offenders more frequently have an ethnic minority background as well as a lower socio-economic

[8] This theory assumes that delinquent behavior is taught in intimate peer groups. This involves the learning of techniques for committing crime as well as norms, values and attitudes.
[9] This refers to techniques that offenders can use to legitimise delinquent behavior.
[10] This approach assumes that delinquent behavior results from and can be understood as a rational cost and benefit assessment. This can involve both material (money) and non-material costs and benefits (fame, pleasure).
[11] This refers to the disappearance of inhibitions due to online anonymity.
[12] This refers to the way in which the internet offers both technical and social affordances that can intensify certain forms of delinquency or offer new possibilities for committing crime.
[13] This refers to the need or urge to master the technology and is accompanied by a sense of power and control.

status.

Although the level of education among cyber offenders varies, it appears that there is a relatively higher level of intelligence and education compared to traditional offenders. Sometimes offenders do not complete their education, which does not automatically entail that they end up in low-skilled work. The work and training that cyber offenders do or have done varies, but training and jobs in the IT sector are over-represented. In their leisure time, cyber offenders spend a lot of time on technology, IT, gaming and social media. In addition, they also have a wide range of other hobbies. The domestic situation (including the role of family problems) varies greatly. There often seems to be a lack of parental controls on the online behaviour of cyber offenders, both in families with and without family problems. This limited supervision is partly caused by poor knowledge of parents[14] of the internet and the online world. Finally, cyber offenders can be characterised as intelligent. More often than traditional offenders, cyber offenders appear to have features from an autism spectrum disorder (ASD) and a strong problem-solving capacity. The findings also suggest that there is a distinction between cyber offenders who experience lower levels of self-control and are impulsive versus offenders who set long-term goals and are perfectionist. According to the literature and the experts, some offenders can be characterised as introvert or socially awkward, but another part (of which many of the interviewed offenders feel they belong to) seems to be sufficiently socially competent. Whereas most offender have built up an extensive online peer network, their offline network is relatively smaller and had less impact on their offending behaviour.

Motivations and experience

The research shows that various motivations are involved in cyber offending. We also found that offenders have multiple motivations simultaneously and that motivations can change over time.

The motivation curiosity, desire for knowledge and (mental) challenge are motivations that we mainly find among juvenile cyber offenders. These motivations are not necessarily malicious. Young offenders driven by these motivations want to learn the ins and outs of systems and seek to discover how far they can go with technology. In contrast to most traditional forms of crime, learning and obtaining knowledge is a goal or motivation in itself and not just a means or instrument for committing the offence. Other motives that we encountered in the research are the kick, excitement, pleasure, boredom, the urge to collect (information) and power. These drives can also play a role in traditional crime, but with cyber-focused crime there is stronger interconnection with online skills and technology. Recognition, status, peer respect and the urge to prove yourself are also important motives for juvenile offenders. They want to prove what they can do to gain respect or fame. The difference with traditional crime is that the focus lies more on technical skills, abilities and your performance (what you are able to 'do'). Financial motives seem to play a less prominent role for juvenile (individual) offenders. In some cases, money can in a later stage play a role in the criminal career, depending also on the activities in which the offender is involved. The financial motive seems to be most prominent among (adult) offenders who are active in the context of fraud and organised cybercrime. In some cases, the offenders involved have made the transition from traditional (offline) fraud to cybercrime. In addition, cybercrime (mainly hacking or carrying out DDoS attacks) can be committed out of anger or to take revenge on friends, family, former employers or former lovers with whom an offline conflict was going on. These motivations we mainly find among adult traditional offenders who have discovered a new means of expressing their frustration. There are also offenders who act on ideological grounds. The latter two clusters of motivations have remained relatively underexposed in this study.

[14] The IT knowledge of parents may depend on their age. This aspect we did not examine in the current study.

Perceptions with regard to the likelihood of getting punished, the risk of getting caught and the damage of the committed crimes

When it comes to the perception with regard to the likelihood of getting punished, there seems to be a sliding scale. On the one side of the scale we find (mostly young) offenders who are not or hardly aware of the likelihood of getting punished and on the other end of the scale we can locate offenders who are well aware of the penalties they might face. They obtained this knowledge, for example, through online forums. The limited awareness of the likelihood of getting punished, which is present among part of the offenders, can be explained by different factors, including the absence of supervision in the online world, the invisibility of the inflicted damage and - for some of the offenders – the involvement of motivations that are not necessarily malicious in nature (curiosity, mental challenge, recognition of talents). The latter category also includes offences in which security problems are demonstrated, involving uncertainty about the legal boundaries and the frameworks of responsible disclosure[15]. The limited perception of the likelihood of getting punished is therefore a more important criminogenic factor for cyber offenders than for traditional offenders. As the career continues, the awareness of criminality among offenders increases, but according to experts, this is partly overturned by the very limited visibility of the police and the judiciary when it comes to online crime. The chance of being caught is generally very low due to limited police capacity and the possibility of anonymisation. The findings also show that the perception of the risk of being caught decreases over time, depending on the frequency of getting away with the crimes unseen.

With regard to the perception of the damage or harm, it appeared that offenders, especially young offenders, perceive the extent and seriousness of the damage their crime inflicts as minor. They also seem to downplay or deny the damage or victim (neutralisation). Although such denial can be also found among offenders of traditional crime, this aspect is reinforced online due to the distance to the victim, the hyper-reality in which the behaviour comes about (it feels like a game), the normalisation that arises from gaming (where it is both a routine and normalised practice to launch DDoS- attacks or hack each other) and the ease with which certain crimes can be committed (in high frequency). The online environment also ensures fewer inhibitions due to the absence of the judgment of others or other dreaded consequences. Due to the online anonymity of offenders and victims, a different evaluation of the behaviour of the offender takes place than when the interaction would be offline (also known as online disinhibition effect). For older offenders, the downplaying of the damage appears to play a lesser role. They acknowledge the damage but the motivations they have for behaviour (financial, revenge, ideological, etc.) are important enough for them to continue the career.

Criminal careers

In order to map the criminal careers of cyber offenders, we looked at factors that contribute to the onset (initiation), the development of the career over time and to what makes offenders (independent of an intervention) desist.

When it comes to the initiation, we observed that, like traditional crime, factors such as the maturity gap (the discrepancy between biological and social maturity), the influence of delinquent peers and certain motivations (such as money, challenge or thrill) play a role. In addition, we found factors that play a specific role in the initiation of cybercrime such as interest in or affinity with IT, gaming, spending a large amount of time on forums and/or easy access to (ready-to-use) tools. When it comes to the development and maturation of the criminal career, we presumed that offenders go through (in part or all) four phases: 1) affection for computers (phase where an interest in computers/IT arises), 2) curious exploration (phase in which an interest in hacking emerges), 3) illegal excursion (phase in which illegal

[15] Responsible Disclosure (RD) concerns the "disclosure of IT vulnerabilities in a responsible manner and in joint collaboration between the person reporting and the organisation on the basis of a responsible disclosure policy established by organisations for this purpose within the ICT world (...). (National Cyber Security Centre, 2013, p. 5).

activities are explored) and 4) criminal exploitation (phase in which offences are systematically committed). The findings suggest that there is quite some variation with regard to which phase (s) the offenders go through. This can vary from offenders who do not go further than "curious exploration" and (usually adult opportunistic) offenders who almost immediately end up in the "criminal exploitation" phase to offenders who go through all phases.

We can also observe variation among offenders who go through the same phases when it comes to how the development of the delinquent behaviour looks like and which factors influence it. These variations are largely related to factors that play a role in the initiation as well as the motivations, skills and degree of professionalisation. At the same time, other factors play a role in the course of the criminal career, including changes in moral perceptions (either towards pro-criminal or towards pro-social behaviour) and changes in motives (for example, a transition from recognition to financial drives). In the case of desistance (ending the criminal career) we also see that various factors play a role. Just as with traditional offending, maturing and getting employed and another half influence quitting. In this regard, it is assumed, mainly by the experts, that cyber offenders have relatively more chances of finding a (good) job due to the social need for digital talent. The findings also show that other costs and benefits can play a role over time, which is also related to age and social ties. In addition, we also see that the motives that initially contributed to the onset of committing these offences (such as challenge, kick and excitement) eventually also led to desistance for the reason that they fade away or disappear over time. In the context of desistance, the research also drew attention to factors that make this process more difficult. Apart from having a criminal record, offenders can be completely absorbed in the online (delinquent) world, both in terms of status and identity and (the fast) money, leaving too much (material and immaterial) benefits or incentives not to stop.

PART 2 Interventions

In the second part of the research, we focused on the extent to which existing interventions[16] adequately correspond to the characteristics and factors outlined in part 1. Since interventions for specific cyber offenders are scarce and, moreover, little (evaluation) research has been carried out into both traditional and alternative interventions for cyber offenders, the findings are mainly based on *expectations* about the effectiveness that could be derived from the literature and the interviews.

For the analysis of potentially effective interventions we firstly looked at interventions aimed at deterrence and situational crime prevention, involving interventions that directly aim to influence the perception of the cost-benefit ratio of offenders when committing cybercrime (rational approach to choice). Secondly, interventions were discussed that are directed to the involved criminogenic and protective factors for perpetrating cybercrime, taking into account the individual and the different contexts in which the individual finds himself (based on What Works and the desistance approach[17]). A distinction is made here between *risk-based* interventions, which target characteristics that influence the delinquent behaviour (criminogenic factors/needs) and *strength-based* interventions, which aim to provide assistance in the process of developing pro-social behaviour and a pro-social identity. In part, this assistance can also contribute to the elimination of risk factors. Yet, they mainly seek to focus on the protective factors (*strengths*), such as the development of talent, which offer opportunities for the future

[16] In this research we maintain a broad definition of interventions. Alternatives such as hacker competition are also termed 'intervention' since they can contribute to behavioural change.

[17] Risk-based interventions closely correspond to insights from the What Works approach, which places the emphasis on the treatment of criminogenic factors. Strength-based interventions mainly correspond to theories about desistance. However, the approaches and their insights about effective interventions also partially overlap. In the current research, we therefore do not oppose them, but we regard them as complementary. It should also be emphasised that some interventions have both risk-based and strength-based elements.

and thus offer perspective and hope. The responsiveness of offenders to the intervention offered is an important theme in both approaches.

Interventions that correspond with deterrence theory and situational crime prevention

According to the rational choice approach, interventions are effective if they either increase the costs of committing a crime or reduce the benefits. Situational prevention strategies[18] (such as warning banners[19] and the disruption of digital markets) can play a role in increasing the risk and the necessary efforts for committing the crime. Of all the interventions described in the research, disruption (measures aimed at disrupting the criminal executive process) is the intervention that most directly affects the efforts that must be made to commit these offences and thus increases the costs of committing the offence. Subgroups for whom this intervention may be effective are offenders with financial motives in all phases of their criminal career and offenders (regardless of their motives) who commit their crimes with the help of purchased tools.

Other interventions aimed at increasing perceived costs are interventions directed at raising awareness of the risks that come along with committing the offence (such as the risk of getting punished) or awareness of the damage inflicted (awareness of this damage might affect the moral perception). Whether such interventions are effective depends on the extent to which the offenders are responsive to the information transferred in the interventions (responsiveness). It can be assumed that these interventions are not effective for the more experienced offenders and offenders for whom the likelihood of getting punished is actually part of the benefits that come along with the offending (for example, thrill or status).

The interviewed experts also point out that these interventions can have potential adverse effects, such as generating even more thrill (which is precisely why some offenders commit these offences) and taking extra measures for anonymisation by the offenders. On the other hand, the visibility (of law enforcement) that is achieved by means of interventions that are aimed at raising awareness of the risks, can also make the sense of inviolability disappear. Consequently, an adjusted cost-benefit outcome may arise, which may make them abandon cybercrimes.

From the findings it can further be concluded that still much could be gained in respect to the certainty, severity and speed with which punishment follows the crime (conditions for a deterrent effect). Both the perceived and actual chance of being caught is considered very low by experts as well as by offenders. In addition, according to the experts, the process of investigation, prosecution and trial appear to be longer in cyber cases than in "traditional" cases, which is partly due to the fact that the investigation and the provision of evidence is more complex.

According to experts, the answer to the question of how 'severe' the penalties should be in order to have sufficient deterrent effect depends mainly on the motivation of the offender, whereby a distinction is made between offenders driven by financial motivations and offenders who are young, first offender and driven by curiosity. For the latter group of offenders an arrest or even the threat of an arrest by means of a warning conversation with the police (knock and talk[20]) can often be sufficiently deterrent and raise awareness of the likelihood of getting punished and the inflicted damage. If an intervention is still imposed a long time after the offense has been committed (and the juvenile offender may be much further in his or her development and may have already desisted), the intervention may, if resocialising aspects are not taken into account (e.g. in the case of high fines or imprisonment), have a counterproductive effect for this group. At the same time, the literature and experts point out that – as

[18] This refers to preventative strategies aimed at taking away the opportunity to commit crime and thus increasing the perception of risk (and costs) of the offender.

[19] This refers to digital warning messages to prevent someone from displaying online crime behavior

[20] This intervention is also known as 'cease and desist'.

the likelihood of getting caught (especially for more serious cybercrime cases is relatively lower), an example should be set towards society by also imposing a serious punishment. This could produce a general deterrent effect (signaling function).

Interventions that correspond with the What Works and the desistance approach

Risk-based interventions

Based on the literature study and the expert interview, we can conclude that still little is known about the (effectiveness of the) use of interventions aimed at the criminogenic factors of cyber offenders (risk-based interventions). An important observation is that there is hardly any validated risk assessment for this group of offenders. First of all, it turned out that there is only limited insight into how the criminogenic factors of cyber offenders should be measured precisely (for example when it comes to the quality of parental supervision and the way in which personal and psychological characteristics can be related to delinquent behaviour in the online context). As a result, existing diagnostic instruments still appear to be insufficiently validated with regard to criminogenic and protective factors on which interventions must be specifically deployed for cyber offenders. In addition, various experts indicate that there is insufficient evidence of (timely) risk assessment with the necessary in-depth analysis by experts in this offender group. In order to accomplish this, a correct "routing" seems necessary in the settlement process.

When it comes to the question of which interventions could be effective for cyber offenders, experts often refer to existing interventions for traditional offenders. These are aimed at various areas of life such as improving the relationship with parents, learning social skills, tackling a pro-criminal attitude and working on debts or addiction. These interventions could be effective in tackling the relevant criminogenic factor in offenders of different ages and in different phases of the criminal career, only in case the motivation for change is present or can be created. However, it is expected that cyber offenders generally will not be sufficiently responsive to (most of) these interventions because they take little or no account of the online context in which the offences take place (in which damage is less visible and the victim is very 'abstract'). To take this aspect more sufficiently into account, experts put forward that a method such as ‘mentalising’, involving empathising with another person, can be useful. Experts also expect, despite very limited experience, positive effects of contact with the victim through recovery mediation.

The only interventions specifically targeted at cyber offenders that we found, are the imposition of restrictions on computer and internet use and the use of serious gaming. In serious gaming, young people are taught good and bad manners of hacking in a playful way and at the same time they are encouraged to think about ethical issues. Such interventions can, among other things, ensure that contact with online criminal peers does not take place (an important criminogenic factor). However, preventing such contact is complex to achieve and will always be temporary. This intervention must therefore be seen as an intervention that creates a momentum for other interventions that can trigger desistance on the long term (by, for example, changing the pro-criminal attitude and offering alternatives). The use of serious gaming is potentially effective for young, non-malicious offenders who playfully get aware of good and bad aspects of hacking. This is therefore a relatively light intervention that can contribute to knowledge about ethics and awareness among young hackers. Although no negative effects can be expected from this intervention, the question remains whether the effects that are generated in a game setting also have a *real-life* effect. On the other hand, serious gaming takes place in a context of guidance and ethical boundaries are most likely discussed. Still, the question remains to what extent offenders are responsive to this information and thus susceptible to adjusting their moral compass. More research needs to be done to provide answers to these issues.

Strength-based interventions

In addition to interventions aimed at reducing criminogenic factors (needs), the literature and experts also focus on strength-based interventions, interventions that are primarily aimed at strengthening the pro-social identity. More than offenders of traditional crime, a part of the offenders of cyber-focused crimes have talents (technical skills) that are of great value to society, only in case they are used in a pro-social manner (ethical hacking). Interventions can respond to this by providing more information to offenders about what they could achieve on the labor market with these skills. Preventative interventions mentioned by experts in this context are cyber workplaces[21] and hacking competitions. [22] These interventions are aimed at increasing IT skills and teaching ethical hacking. Such interventions also give young people recognition, enable them to meet like-minded people (that share the same interest in IT) and build on (both technical and social) skills and future prospects. Another form of a strength-based intervention (component) is guidance by role models. [23] Both the experts and the literature identify this as an important element in building a new prosocial identity and relationships. Role models can also have a signaling function, because any deviant behaviour can be noticed and corrected.

A specific (reactive) intervention aimed at cyber offenders is the recently developed *Hack_Right* intervention. This intervention among others aims to strengthen talent and to learn offenders to hack ethically through a working/learning trajectory at an IT company. In this context, experienced hackers are used as coaches (role models). The intervention seems to correspond well with insights from the desistance approach, because it assists young cyber offenders in developing a pro-social identity and role in society. Although the intervention still needs to be formally recognised by the Judicial Interventions Recognition Committee[24], experts have high expectations about what the intervention can achieve for the target group (young, first offender, technically skilled, no serious offence, pleading guilty and motivated). There are, however, also some critical notes, for example with regard to the question whether such an intervention actually rewards criminal behaviour. Viewed from the perspective of deterrence, such an intervention may generate insufficient special and perhaps also general deterrence.

When imposing strength-based interventions, it is of course important that the right target groups are selected, whereby the motives for the delinquent behaviour appear to be an important criterion. After all, only working on enhancing IT skills and offering a network or career opportunities without working on the moral awareness and turning a possible pro-criminal attitude can lead to more cybercrime. If the various components are combined in the intervention, strength-based interventions not only offer new opportunities to cyber offenders, but they could possibly also lead to a decrease in future offending and thus result in a positive outcome for society.

Conclusions and recommendations

In this research we analysed the (unique) characteristics of cyber offenders and the extent to which available interventions correspond to these characteristics. The research shows that we are dealing with everything but a homogeneous group of perpetrators. There is a lot of variation, both in terms of motivation and criminogenic and protective factors for committing cyber-focused crime. In a more general sense, it can be concluded that a number of criminogenic factors contribute both to traditional and cyber offending, such as family issues, downplaying the severity and damage of the crime committed and certain

[21] This refers to a place where IT-skilled young people can go to, for example, attend workshops or work on IT projects.

[22] This refers to hacking competitions that are (commonly) sponsored by private parties in which hackers hack systems on request.

[23] This concerns people from the hacker world (for example, ethical hackers) who play an exemplary role and/or mentor role.

[24] For more information about this commission and the procedures see: https://www.nji.nl/nl/Databank/Databank-Effectieve-Jeugdinterventies/Deelcommissie-Justitiele-interventies.

motives (kick, pleasure and money). However, due to the online environment and (technical) nature of the offences, they can be expressed differently. We have also found characteristics that seem to occur relatively more often with cyber offenders than with traditional offenders or characteristics that are quite unique for this offender group. This concerns, for example, personality or psychological characteristics that contribute to the necessary talents for the occurrence of the offences (curiosity, eagerness to learn, self-control, perfectionism, need for recognition and the urge to prove oneself of technical skills) or personality or psychological characteristics that make offline social interaction more difficult (such as introversion, characteristics of an autism spectrum disorder and social awkwardness). Based on our findings, we present three recommendations with regard to how interventions for cyber offenders must be designed.

In the first place, it is important that more and more tailored in-depth diagnostics take place for decisions about (criminal) interventions for cyber offenders. Since there is great diversity among cyber offenders, a tailor-made approach is important, and, to that end, the criminogenic and protective characteristics and the way in which they influence the delinquent behavior in the online environment must be mapped out. The current instruments still appear insufficiently capable of measuring these specific cyber-offender-related characteristics. In addition to criminogenic needs, specific attention is also needed for responsiveness to interventions (learning styles and motivations) of cyber offenders who commit their offences in an online environment. For cyber offenders, it seems appropriate that specific supplements to existing diagnostic tools become available.

Secondly, interventions that combine awareness, mentalising (empathising with others), moral reasoning (in combination with ethical hacking) and offering opportunities offer great potential to be effective, especially for young technically skilled offenders. However, these interventions also appear to produce unwanted effects, because they can unintentionally inspire potential offenders to explore these crimes or increase the status of cyber offenders with their peers. It is therefore important to thoroughly investigate both the intended and unintended effects of these interventions and to describe clear target groups for whom the interventions are potentially effective.

Thirdly, it appeared that traditional interventions are potentially suitable for both younger and older perpetrators in different phases of the criminal career, but with motivations other than curiosity and seeking mental challenge. This concerns interventions that focus on specific criminogenic factors (such as addiction, lack of social skills or supportive relationships). However, these interventions do not yet take into account the responsiveness of cyber offenders in the online context, so that effectiveness for this target group is probably disappointing. Our final recommendation is therefore to find out what adjustments are needed in these existing interventions to reflect the responsiveness of cyber offenders.