9 Interventions for cyber offenders

Elina van ’t Zand, Sifra Matthijsse, Tamar Fischer & Wytske van der Wagen*

9.1 Introduction

Criminologists are not only faced with the question of whether traditional theories of crime can be applied to cybercrime, but also whether traditional interventions suffice to deal with (potential) cyber offenders. There may be a need for customised or new interventions. This final chapter sheds light on interventions that may be effective in dealing with cybercrime. To do so, it builds on the insights provided of various types of cybercrime (Chapter 3), various offender characteristics and contextual aspects related to cyber offending (Chapters 4 and 5) and various criminological explanations (Chapter 7). In this chapter, we focus specifically on cyber-dependent crime. We assume that offenders of these ‘true cybercrimes’ differ more from offenders of traditional crimes in terms of their characteristics and motivations. Whereas offenders of cyber-enabled crime differ less from traditional offenders, as for them IT is merely a new tool. For offenders of cyber-dependent crime, the question of suitable and effective interventions is therefore considered most relevant.

In this chapter, interventions that may be suitable and effective for these types of offenders are analysed from three perspectives: (1) the rational choice approach; (2) the ‘What Works approach’ and (3) the desistance approach. These perspectives mainly aim to target offending behaviour and related motivations, risk and protective factors. Other types of interventions are not discussed in this chapter, for example interventions that specifically target the environment, such as target hardening (e.g. firewalls or antivirus protection) (see Section 7.2.1). The interventions we address in this chapter are, on the one hand, *reactive* interventions, involving for example formal punishments

* Dr. E.G. van ’t Zand is assistant professor of criminology at the department of Criminal Law and Criminology of Leiden University. S.R. Matthijsse MSc, Dr. T.F.C. Fischer and Dr. W. van der Wagen are associated with the criminology section of Erasmus University Rotterdam (Erasmus School of Law) and work as lecturer, associate professor, and assistant professor, respectively.

or measures that can be imposed in response to criminal behaviour. On the other hand, *preventive* interventions are addressed, for example educational interventions aimed at the general public, students or parents. Of these, we will primarily focus on interventions aimed at preventing (repeated) criminal behaviour among (potential) offenders of cyber-dependent crime. We will focus on both traditional interventions and interventions developed specifically for cyber offenders.

First, Section 9.2 briefly discusses the three central approaches – rational choice, What Works and desistance – of interventions and how they relate to each other. Subsequently, current interventions that fit within each of these approaches are discussed in detail in Sections 9.3, 9.4 and 9.5. Section 9.6 briefly summarises the findings of this chapter and Sections 9.7 and 9.8 identify points for discussion and key concepts.

9.2 Perspectives on interventions

9.2.1 Three approaches

Interventions can be classified according to three different main approaches, each of which has different assumptions about how interventions can be effective (van der Wagen et al., 2019). First, the rational choice approach considers interventions to be effective if they address the cost-benefit calculation offenders make before deciding to commit crime (Cornish & Clarke, 1986). This cost-benefit ratio underlies both the theory of deterrence and situational opportunity theories of crime (Cohen & Felson, 1979). Second, the What Works approach (Andrews et al., 1990; Andrews, Bonta, & Wormith, 2006) assumes that in order to be effective, interventions must take into account specific characteristics that are central to the 'Risk-Need-Responsivity model' (e.g. Lipsey & Cullen, 2007; Lowenkamp, Latessa, & Holsinger, 2006). Third, the desistance approach considers desistance from crime to be a dynamic and complex process that is characterised by trial and error, so interventions should connect to the offender's individual process (McNeill et al., 2012). Since these three approaches are based on different criminological perspectives, each takes a different angle from which to tackle (cyber) offending and preventing recidivism.

Before looking at these approaches in more detail, it is important to note that they were not developed separately, but in response to each other. The What

Works approach arose from the idea that an exclusive focus on deterrence, based on a purely rational, calculating offender, does not work. The What Works approach aims to contribute to the resocialisation of offenders by focusing on risk, criminogenic needs and responsivity. The desistance approach subsequently emerged from criticising the What Works approach for its emphasis on 'intervention programmes' and 'treatment' of criminogenic factors. The desistance approach puts less emphasis on treatment but rather on facilitating and supporting the dynamic process of desistance from crime. The underlying assumption is that individuals should initiate the change themselves, and should be stimulated to do so. By paying attention to the offender's *agency*, interventions could contribute to this process of change.

In this chapter, we assume that all three approaches offer valuable insights into what could be potentially effective interventions for offenders of cyber-dependent crime. Moreover, a strict distinction cannot always be made and interventions often contain elements of various approaches.

9.2.2 Applicability of the approaches to cyber offenders

The rational choice, what works and desistance approaches all aim to reduce crime and prevent the development of criminal careers. The approaches are, however, not developed for offenders of cyber-dependent crime in particular. Consequently, we have knowledge about how interventions can target and take into account the risk and protective factors that play a role in committing traditional crimes, such as violent, drug or sex offences, but we still know relatively little about the risk and protective factors and, more generally, the applicability of the three approaches to cyber offences. One of the reasons for this lack of knowledge is that little diagnostics take place before applying interventions, so that risk factors related to the committing of crime are not sufficiently mapped out. In addition, it seems that traditional diagnostic tools need specific adjustments in order to be sufficiently capable of measuring specific cyber offender-related risks (van der Wagen et al., 2019).

Up to now, evidence on interventions that may or may not be effective in countering cybercrime is still typically scarce (Brewer et al., 2019). Also, very few interventions currently exist that are specifically designed for cyber offenders. As a result, the current body of literature on interventions for cyber offenders has two major limitations. First, it is predominantly either descriptive in nature, for example the types of punishment imposed for cybercrimes, or theoretical in nature, for example, analysing the potential effectiveness of interventions. Second, the few empirical studies that have taken place were able to use only a small sample of offenders and often include hackers only. There is little knowledge on interventions for other types of cyber offenders, such as those involved in distributed denial-of-service (ddos) attacks, phishing or the distribution of ransomware. As a result, evaluation studies that actually measure the outcomes of interventions applied to cyber offenders are scarce. Hence, we know little about their successfulness in preventing recidivism. In the following sections, we elaborate on the various approaches for interventions to analyse which interventions may be suitable and effective for cyber offenders.

9.3 The rational choice approach

9.3.1 Deterrence and situational crime prevention

A fair amount of (theoretical) studies apply the rational choice approach to offenders of cybercrime, focussing on both deterrence and situational crime prevention strategies. Central to the rational choice approach is the notion of rational, calculating human beings, *homo economicus,* whose actions are determined by a cost-benefit calculus (Cornish & Clarke, 1986). According to this 'classical' criminological perspective, interventions are effective if the calculating offender is sufficiently deterred from committing crime (Bentham, 1789). In other words, individuals will refrain from offending if the costs outweigh the benefits.

The situational opportunity theory of crime and the related situational crime prevention strategies emphasise the need for adjusting the environment in order to reduce the opportunity for committing crimes and, thereby, influencing the cost-benefit ratio of (potential) offending (see Chapter 7 for a detailed discussion). To achieve this, different strategies can be used. Clarke and Felson (1993) have developed a specific model of situational crime prevention, in which they distinguish five main strategies: (1) increase risk; (2) increase effort; (3) reduce reward; (4) reduce provocation; and (5) remove excuses. Interventions aimed at situational crime prevention are likely to work not only for the physical, but also for the digital environment (Leukfeldt & Yar, 2016; Miró-Llinares, Drew, & Townsley, 2020). A relevant question is, for example, whether increasing online supervision will also increase both risk perception and the effort to commit crime, thereby decreasing motivation.

Within deterrence theory a distinction is made between general and special deterrence. General deterrence aims at deterring persons from committing crime, including those who are not (yet) in contact with the criminal justice system (both offenders and potential offenders). Special deterrence is a criminal justice response to convicted criminals aimed at reducing re-offending due to the deterrent effect of the punishment or measure imposed (Kleck et al., 2005). To create general deterrence, the costs of committing crime should be increased by enlarging the risk of being caught, on the one hand, and by increasing the threat of punishment, on the other. These elements are, together with the timeliness of a criminal justice response, considered to be the three core elements for successful deterrence, according to rational choice theory. The greater the 'certainty', 'severity' and 'swiftness of punishment', the lower the crime rate (Gibbs, 1975; Kleck et al., 2005). These elements do not necessarily have equal weight (Clarke, 1997, in Hutchings, 2016), particularly since the perception of the offender plays an important role as well. For interventions to be sufficiently deterrent, offenders need to *perceive* that a response from the criminal justice system is certain, swift and severe. Yet, the question is whether criminal justice responses to cybercrime meet these criteria, and whether these are sufficiently deterrent to cyber offenders (Bossler, 2019; Hong & Neilson, 2020).

First of all, not only is the chance of getting caught low for cybercrime (Boekhoorn, 2020; Lee & Holt, 2020; see also Chapter 8), this chance is also *considered* to be very low by (potential) offenders (National Crime Agency, 2017; van der Wagen et al., 2019). The literature describes that the perceived chance of getting caught can be increased by, on the one hand, improving detection capabilities (van der Wagen et al., 2019) and, on the other hand, communicating more about police capabilities and online intervention strategies being carried out (Goldman & McCoy, 2016). This strategy was applied, for example at the takedown of the darknet market called the *Hansa Market*, thereby aiming to disrupt one of the key features of darknet markets: trust between buyers and sellers (van Wegberg & Verburgh, 2018, as discussed in Chapter 8). The broadcasting of certain cases in the media can therefore have a signalling effect – a strategy that is also used for white-collar crime (see Huisman & Lesmeister, 2018).

Second, in addition to a *certain* response, a *rapid* response is also often lacking. The investigation of cybercrime can be complex and time-consuming, so it often takes a relatively long time – sometimes years – before the suspect is both arrested and prosecuted (Boekhoorn, 2020). This is partly due to the use of anonymisation tools by offenders (Bossler, 2019), in combination with the right of the suspect to remain silent. In addition, submitting technical inquiries regarding digital evidence to a forensic institute can lead to severe delays in the process, which can ultimately lead to dismissal of the case or lowering of the sentence due to reasonable time constraints (van der Wagen et al., 2019). Moreover, if a suspect remains abroad, jurisdictional issues make it quite difficult and sometimes impossible to proceed with investigation and trial at all (see Chapter 8).

Third, the question of what constitutes an appropriately *severe* response to cybercrime remains largely unanswered. Several difficulties arise when ordering punishment for cybercrime. First of all, it is not always possible to determine the exact number of victims or damage caused by the offence (Marcum, Higgins, & Tewksbury, 2012; van der Wagen et al., 2019). As discussed in Chapter 2, cybercrimes may deal with a *de minimis* problem: involving a large number of victims while each victim suffers relatively little damage, also known as *small-impact bulk victimisations* (Wall, 2007b). Also, a balance must be found between proportional punishment with a sufficiently general and special deterrent effect where large-scale damage has been caused, and re-integrative punishment for young persons and first offenders. For example, in a large-scale Dutch ransomware case (CoinVault, as discussed in Section 3.2.2.1) the two young offenders were sentenced to 'merely' 240 hours of community service and a conditional prison sentence. Judges in cybercrime cases are challenged to properly weigh the nature and severity of the offence with the suspect's personal and mitigating circumstances (Smith, Grabosky, & Urbas, 2004). As a result, a clear general deterrent effect seems to be somewhat lacking. Not primarily because the threat of punishment, that is, the maximum penalty that can be imposed is too low, but because the penalty that will finally be imposed is oftentimes much lower than the penalty required (van der Wagen et al., 2019). The following section discusses specific interventions that can influence the rational choice and thus be potentially effective in deterring cyber offenders.

9.3.2 Reactive interventions in line with the rational choice approach

9.3.2.1 Incarceration

Little is known about the application of incarceration to cybercrime offenders. Some authors argue that cybercrime offenders receive a prison sentence less often than traditional offenders and that the prison times are relatively short. Moreover, cyber offenders with a criminal history of violent or public order offences are much more likely to receive a prison sentence than those without previous violent offences (Marcum et al., 2012). The prison sentences imposed are also generally shorter for cyber-dependent crimes than for cyber-enabled crimes, such as large-scale phishing, online drug trafficking or distribution of child pornography cases (Smith et al., 2004; van der Wagen et al., 2019).

When it comes to the (potential) effectiveness of incarceration also little is known. It is suggested that in various cyber cases in the United States, being detained does not have a sufficiently specific deterrent effect, since offenders continued their criminal behaviour after serving their time in prison (Smith et al., 2004). In the Dutch context it was found that the experience of being arrested and taken in custody already has a serious impact on young first offenders and therefore a sufficiently deterrent effect (van der Wagen et al., 2019). At the same time, it is expected that regular punishments such as imprisonment do not sufficiently meet the criminogenic needs and responsivity of juvenile cyber offenders. Moreover, imprisonment creates the risk that cyber offenders will establish new criminal connections in prison or may be recruited by (members of) criminal organisations (van der Wagen et al., 2019). For these reasons, alternative interventions are needed, such as an educational programme as part of community service or a special intervention such as Hack_Right (see Section 9.4.2).

9.3.2.2 Financial penalties

Other interventions that could have a deterrent effect include financial sanctions and measures such as confiscation, fines, restitution and the forfeiture of assets. In cases involving ransomware, banking malware or bitcoin money laundering, the criminal proceeds are usually forfeited. Yet, the effectiveness of financial penalties and measures for cyber offenders has not been evaluated so far. In theory, these can convey the message that crime does not pay and, moreover, create more awareness among first offenders of the financial consequences of cybercrime. For offenders driven by curiosity and thrill, the confiscation of their hardware and tools are already experienced as ‘punishing’, not only because of the value of their equipment (e.g. an expensive laptop), but also because of the tools and data that is stored on their device. This may involve large databases with data or self-written programmes (see also van der Wagen et al., 2019).

Complicating factors for imposing financial sanctions and measures are the determination of the exact extent of the damage caused and – as is generally the case – the question of whether the offender is able to repay the damages (Smith et al., 2004). If he or she is not able to do so, it can result in serious financial burdens and debts, which, in turn, can impede the process of desistance. Restitution is, moreover, partly dependent on victims' filing requests for compensation of the damages they suffered. Yet, in cybercrime cases such claims are not always made, partly because not all victims are aware of the fact that they have suffered losses as a result of the crime. And partly because some victims, for example, commercial businesses, fear that being involved in the trial will cause negative publicity and reputational damage (van der Wagen et al., 2019; see also Chapter 6).

9.3.3 Preventive interventions in line with the rational choice approach

9.3.3.1 Cease-and-desist-visits

In addition to the reactive interventions discussed above, there are also preventive interventions aimed at special deterrence. The first example is cease-and-desist visits (also called *knock-and-talks*). The police pay a visit to the homes of (potential) suspects to have a conversation about the criminal nature of their online behaviour. Such conversations are increasingly taking place in cybercrime cases in the Netherlands (Vermaas, 2018) and the United Kingdom (National Crime Agency, 2017), among others. In the Netherlands, for example, this was done in the Webstresser case, after this website facilitating ddos attacks was taken offline in 2016 (as discussed in Chapter 3, Section 3.2.4). Several 'buyers' of ddos attacks have been visited by the police. Europol coordinated this intervention in several countries in Europe as well as in the United States and Australia. As a result, at least one hundred persons using booter services had been informed and warned about the illegal nature, the damages and the possible consequences of using these services (Brewer et al., 2019).

These knock-and-talks are clearly aimed at deterrence, since they convey the message that the police are watching the suspects' online movements, so they are not as invisible and anonymous as they think they are. Knock-and-talks can also involve the parents of young suspects, so that later they can keep a closer eye on their child and thus enhance social control. In Chapter 7, it has already been described that, in line with the opportunity theory, the likelihood of committing cybercrimes is related to the extent to which potential offenders believe that formal and informal social control is exercised over their online behaviour (Berenblum et al., 2019). A cease-and-desist conversation not only makes it clear that online (criminal) behaviour is being observed by the police, but also raises awareness of the risks and consequences of this behaviour. This can lead to a different cost-benefit ratio and can eliminate possible excuses (van der Wagen et al., 2019). In addition, cease-and-desist conversations may lead to seizure of equipment or software, which increases both costs and efforts to commit cybercrime. This intervention thus aligns with both rational choice theory and situational crime prevention. Another positive aspect is that these conversations enable intervening at an early stage, so to prevent potential offenders from entering the criminal justice system. In so doing, stigmatisation and collateral consequences which are detrimental to the desistance process, such as having a criminal record, can be averted.

Still, we may expect that for some offenders the cease-and-desist visits are not sufficiently deterrent but only encourage them to take extra measures to conceal their identity and activities. In addition, a visit by the police may be seen as a reward (a 'badge of honour'), as the cease-and-desist conversations can have a status-enhancing effect, or increase feelings of challenge, excitement and sneaky thrill (Brewer et al., 2019; van der Wagen et al., 2019; see also Chapter 4). More empirical research is needed to determine the effectiveness of this intervention for different types of offenders.

9.3.3.2 Online policing

In addition to cease-and-desist visits by the police in the offline world, the online presence of the police can be potentially effective in reducing cybercrime. Online policing is of great importance not only for investigative purposes, but also for awareness, prevention and cybersecurity (Aiken et al., 2016). Particularly since individuals can easily believe that their online behaviour has no real-world consequences, due to negligible detection, apprehension and clearance rates (Holt, Brewer, & Goldsmith, 2019). When police officers are present on, for example, online forums and games, they can alert participants to the criminal or deviant nature of their behaviour and inform them about the possibilities of challenging their IT-skills in a legal way (Aiken et al., 2016). Especially during the COVID-19 crisis, Dutch police officers started to spend more time online, by participating in popular games played by juveniles. Their aim was to start a dialogue and possibly prevent them from transgressive or criminal online behaviour.

A particular method of online policing involves presenting *surveillance banners* or *warning banners* on websites. By means of such warnings, website visitors are informed that the website or system is being monitored (Wilson et al.,

2015) and that computer trespassing constitutes an offence to which certain penalties can apply (Maimon et al., 2014). In line with the situational crime prevention theory, warning messages are expected to be effective because they increase risk by reducing the (perception of) anonymity of offenders and informing them of the illegality of hacking computer systems. Also, by creating awareness they remove excuses. In doing so, they can influence both the number and severity of hacking incidents (Maimon et al., 2014). In line with the rational choice theory, such an intervention can be expected to be successful only for offenders who are sufficiently deterred by it – whereas others may not take the banner seriously or feel rather challenged by it.

Several (quasi-)experimental studies have been conducted into the effectiveness of banners, with varying results. The use of digital warning messages does not lead to the immediate withdrawal or reduction in the number of computer trespassing events, but it does significantly reduce the duration of the intrusion (Maimon et al., 2014). In other research, a similar partial effect of warning messages was found, for example that they only reduce the level of activity or the time spent on the compromised computer (Testa et al., 2017; Wilson et al., 2015; Stockman, Heile, & Rein, 2015). Furthermore, varying the type of warning message (for example an altruistic message aimed at moral persuasion or a threat of official sanction) yielded ambiguous outcomes. In one study no significant effects were found (Howell et al., 2017), yet another study found that moral conviction did have an effect on trespassers' level of activity (Jones, Maimon, & Ren, 2017). Thus, no clear and conclusive support was found for the deterrent effect of warning banners. As with for example cease-and-desist conversations, the limited deterrent effect of these messages may also be due to the fact that the risk of being caught actually provides a form of excitement ('sneaky thrill') for cyber offenders and therefore actually stimulates hacking activities (Steinmetz, 2017; van der Wagen, 2018a; 2018b). Yet, the evidence shows that computer trespassers are not so much deterred from intruding the computer system altogether but do change their behaviour with regard to the time and activities they undertake during a trespassing event in order to limit the risk of detection.

Another form of online policing that may be effective is the strategy of *disrupting* criminal activities, as was already briefly discussed in Chapter 8. This strategy is especially used in the context of profit-driven cybercrime (see Chapter 5). In order to disrupt criminal activities, barriers are put in place in various phases of the execution of cybercrime. Disruption can occur, for example, by negatively affecting the reputation of buyers in illegal markets by leaving negative feedback from a large number of accounts (sybil attack), by creating distrust or by taking a server or market offline (Hutchings & Holt, 2017), as the police have done in darknet markets such as Silk Road, Alpha Bay and Hansa Market (Soska & Christin, 2015; van Wegberg & Verburgh, 2018). Disruption can increase the threshold or costs of committing cybercrime and can lead to increased online visibility of the police, thus increasing the (perceived) risk of getting caught (Goldman & McCoy, 2016; van der Wagen et al., 2019). However, Hutchings and Holt (2017) point out that disruption may lead to a waterbed effect, with offenders moving, for example, to other (better protected) forums or markets, as seemed to be the case after Silk Road was taken offline (Soska & Christin, 2015). At the same time, this requires more effort from offenders and thus limits the number of offenders that relocate (Hutchings & Holt, 2017). Empirical research has indeed shown that the coordinated intervention that first took Alpha Bay offline while infiltrating and running Hansa Market for several weeks before taking it offline too, can be considered a game-changing intervention (van Wegberg, 2020). Following this take-down, only limited displacement took place, because most vendors did not simply move along to a new market. Many vendors started under a new name and thus had to rebuild their customer relations and reputation from the start.

9.3.3.3 Education in schools

Finally, educating young people in schools about the consequences of committing cybercrime can impact their rational choice (see also Chapter 4 about the school context). Several authors argue that schools should offer lessons on correct computer and internet use, the rules of cyberspace, the illegal nature of certain online activities and its possible consequences (Aiken et al., 2016; Bae, 2017; van der Toolen et al., 2020; van der Wagen et al., 2019). Raising awareness about the illegality of certain behaviour and its consequences could lead to general deterrence among young persons and eliminate possible excuses. However, an evaluation study in the United States found that internet safety education did indeed increase knowledge of school-aged children, but did not change their behaviour (Chibnall et al., 2006). Moreover, merely providing information could also have the unintended effect of arousing curiosity and stimulating ideas in youngsters (Brewer et al., 2019). As a result, education may be less effective for (would-be) offenders who are looking for excitement or challenge (van der Wagen et al., 2019). For these youngsters, engaging in a serious dialogue among their (online and offline) peer groups about their perception of the nature of their online activities is considered to be helpful (van der Toolen et al., 2020). General deterrence could thus be created by educating young people, taking into account both the online and offline context. This should be combined with a criminal justice system responding to online criminal behaviour with swiftness, certainty and severity.

Apart from a possible general deterrent effect, a key element of educational interventions should be a focus on the online dynamics among peers and the individual skills of young people to resist online peer pressure (Brewer et al., 2019). Interventions using positive role models and focussing on the endorsement of positive online behaviour are expected to have a positive impact (van der Wagen et al., 2019; see further Section 9.5). Such interventions should draw attention to both online and offline peer group dynamics, inside and outside schools.

9.4 The What Works approach

9.4.1 What Works and effective treatment

From the What Works literature, it is clear that reducing recidivism is not achieved by imposing deterrent punishment and education only (Cullen, Johnson, & Nagin, 2011). The What Works approach formulates three principles for effective interventions: the risk principle, the need principle and the responsivity principle (risk-need-responsivity, RNR). Interventions that meet these principles are usually imposed as a condition for release from pre-trial detention, a conditional sentence or conditional release from prison. First, the risk principle prescribes that the intensity of penalties and measures must accord to the offender's recidivism risk (Lowenkamp et al., 2006). The higher the recidivism risk, the more intensive the intervention should be.

Second, the need principle implies that interventions should specifically target potentially changeable circumstances and behaviour directly related to the offending (Bonta & Andrews, 2007). Initially, the approach primarily focused on *risk factors* (or criminogenic needs) that needed to be reduced. This specifically concerns *dynamic* risk factors such as a pro-criminal attitude (which, for example, is the result of negative influence from deviant peers), low self-control and a lack of parental supervision. Dynamic factors can be changed by means of interventions, whereas *static* factors, such as age and gender, cannot. As the RNR-principles developed over time, more and more attention was paid to strengthening *protective* factors in individuals and their surroundings, such as positive parenting or employment.

Third, the responsivity principle assumes that interventions must take into account the offender's skills, abilities and learning style. Important factors of responsivity are cognitive and emotional aspects and motivation for behavioural change (Andrews et al., 1990). The What Works approach makes a distinction between *general* responsivity and *specific* responsivity. When it comes to behavioural change, offenders are considered to be generally responsive to methods applying cognitive behavioural therapy and social learning (Andrews et al., 2006). In addition, it should be taken into account that offenders differ in learning styles and abilities. Moreover, they may have different motivations for their criminal behaviour, which has implications for the necessary composition of interventions (McMurran & Ward, 2010).

It follows that the identification of risk, criminogenic and protective factors, and responsivity, are important prerequisites for composing a tailored intervention. To this end, various diagnostic instruments have been developed in which actuarial risk taxation is commonly used, such as the 'Oxford Risk of Recidivism Tool' (OxRec). However, these instruments have been developed for traditional offenders and have not yet been validated for cyber offenders. Moreover, they do not include risk factors associated with the online context in which these offenders operate (van der Wagen et al., 2019). In the following section, we discuss the literature on interventions based on the What Works principles – some of which are especially developed for cyber offenders – in order to analyse which may be potentially successful in reducing recidivism among cyber offenders.

9.4.2 Interventions in line with the What Works approach

9.4.2.1 Strengthening cognitive and social skills

It is only partially clear to what extent personality traits that play an important role in traditional crime such as impulsiveness, antisociality, sensation-seeking, lack of empathy, lack of moral awareness, aggressiveness and restlessness also contribute to online deviant and criminal behaviour. Existing research is not very clear on this point (see Chapter 4). It is generally assumed that cyber offenders, like traditional offenders, will benefit from traditional interventions aimed at strengthening cognitive and both offline and online social skills (Brewer et al., 2019; van der Wagen et al., 2019). Just as traditional offenders, cybercrime offenders may have specific problems that contribute to their offending behaviour, such as psychological, relational or financial problems, as well as problems at home, at school or at work (van der Wagen et al., 2019; Wieland, 2020; see also Chapter 4). These problems do not necessarily have to count as risk factors that are directly related to criminal activity, yet improving them can strengthen their pro-social skills. Treatment focussed thereon could include, for instance, learning to deal with characteristics of autism, social shyness or loneliness, guidance in securing a suitable job or qualification and involving parents to talk about and supervise their child's online behaviour. If problems in these domains exist, then regular interventions and treatments, as applied to traditional offenders, may suffice (van der Wagen et al., 2019).

Still, it is largely unclear whether the arsenal of available treatment possibilities will suffice to deal with the problems of various types of cyber offenders. Notwithstanding this lack of evidence, research has found that generally there is sufficient confidence in the probation service's capacities to offer tailored support to cyber offenders under their supervision (van der Wagen et al., 2019). Nevertheless, it has also been noted that due to a lack of use of diagnostic instruments in cybercrime cases, risk factors and criminogenic needs remain undetected. Some criminogenic needs, which are considered uncommon among traditional offenders, such as loneliness, seem to be important with regard to cyber offenders (van der Wagen et al., 2019).

Apart from the question which traditional risk factors of cyber offenders have to be targeted by interventions, we should ask to what extent interventions should take into account the online context in which cybercrimes take place. Aspects such as the anonymity of both the offender and the victim and a lack of awareness of the consequences of online criminal behaviour are important risk factors in cyberspace (see Chapter 4). In particular, due to the nature of online activities, offenders may have a disturbed day-night rhythm, which can make it more difficult for them to engage in offline pro-social relationships. An existing Dutch intervention for juveniles aims to disconnect them for 24 hours from the online world, in order to enable them to better regulate their time spent online and to create possibilities for them to start offline social activities (van der Wagen et al., 2019). Interventions aimed at cognitive and behavioural change need to address risk factors and criminogenic needs that are particularly relevant to the online context.

To conclude, new interventions do not seem to be necessary per se. Rather, more adequate diagnosis of criminogenic needs and responsivity is needed whereby more attention should be paid to the ways in which the online environment contributes to deviant or criminal behaviour.

9.4.2.2 Reducing pro-criminal attitudes and increasing awareness of criminality and harm

An important criminogenic factor that interventions should focus on is a pro-criminal attitude, according to the What Works approach (Bonta & Andrews, 2007). First of all, the root cause of this pro-criminal attitude must be established. As already seen in Chapter 4, some of the cyber offenders (mainly the young ones) are rarely aware of the criminal nature of their behaviour. For these offenders, interventions should focus on raising awareness, by providing information and training combined with dialogue in which offenders are actively challenged to compare and contrast their own views with these newly provided insights (van der Wagen et al., 2019). There is also a group of offenders, however, that is aware of the fact that their behaviour is illegal, yet do not realise that it actually causes serious harm to victims. Interventions for these offenders should aim at raising awareness on the possible consequences of their criminal activities for both the victims and their own future, in order to reduce the rationalisation that neutralises the damage (Zebel et al., 2013). Taken together, raising awareness of criminal conduct and resulting harm, based on the principles of cognitive and behavioural therapy, could help to curb the neutralisation of their behaviour.

When it comes to the limited awareness of consequences of the behaviour in terms of victims and harm, interventions that focus on empathising with the victim could be successful, and is also referred to as *mentalisation* (van der Wagen et al., 2019). Restorative justice-based approaches, such as victim-offender mediation, specifically focus on this. Mediation can take place by way of writing a letter of apology to the victim or a victim-offender conversation. In addition to removing distance, anonymity and invisibility, facing the victim can contribute to both awareness and responsibility, and remorse regarding the damage caused. This could, moreover, strengthen the empathy and moral awareness of the offender and thus play a role in changing a pro-criminal attitude. Although mediation is a potentially effective intervention, it is not often applied in cybercrime cases, let alone evaluated (Brewer et al., 2019; van der Wagen et al., 2019). It has been suggested to be potentially effective for young, first offenders, as well as for offenders of online fraud such as scammers (Button et al., 2015; Levi et al., 2015). Furthermore, it could be effective in cases in which the victim is located in another country, as mediation can take place by means of videoconferencing (Brewer et al., 2019). Naturally, the victim's interests should always be kept in mind.

Finally, 'gamification' can be used as an intervention strategy to reverse or prevent pro-criminal attitudes (Aiken et al., 2016). Gamification, in this context, refers to learning appropriate (online) behaviour through 'game mechanisms', or gaming (Power & Kirwan, 2014). These types of games could teach (potential) offenders the distinction between ethical and malicious hacking in a playful and competitive manner. Moreover, with the help of these games they can learn valuable cyber security skills (e.g. Švábenský et al., 2018), which they learn to apply in a pro-social way (Matthijsse et al., 2021). A recent example of an initiative based on gamification is 'Gamechangers', which was launched during the COVID-19 crisis by the Dutch police.[1] This online platform stimulates and challenges young people to use and improve their hacking skills in a pro-social way. It offers young people, who had to spend a lot of time at home and online, and who might have become bored, an online alternative for being exposed to pro-criminal environments and attitudes. As with many of the interventions, empirical research into their effectiveness for cyber offenders is, to date, lacking.

9.4.2.3 Manipulating criminogenic opportunity factors

Another category of interventions in targeting criminogenic factors are interventions that restrict or control computer and internet use. Prohibiting the use of computers or the internet can be imposed as a condition for suspending pre-trial detention or as part of a conditional sentence (Smith et al., 2004). Such a ban can give impetus for change in both time spent behind a computer and the nature of online activities, especially if it is combined with treatment or supervision by a probation officer or counsellor. An important contribution of such restrictive measures is that they can serve as a cooling down period in which offenders can start to undertake more offline activities, enter into new offline (intimate) relationships and realise that there is more than a 'life behind the screen' (Matthijsse et al., 2021). Worth noting is that many social workers and probation officers still have very limited knowledge and technical skills regarding computers and the internet. This creates problems when monitoring behaviour and offering guidance in online activities (van der Wagen et al., 2019).

[1] The police are carrying this out in cooperation with Deloitte (the Hacklab challenges | Hackazone), WeFitter (the WeFitter challenge), ESL (the Gamechangers FIFA Cup) and Stichting Hack in the Class (Hack in the Class), see 'Gamechangers: keep youngsters away from cybercrime', Politie.nl, 21 April 2020.

Another way of manipulating criminogenic opportunity factors is by way of seizure of equipment, as previously discussed. Seizure can be used to reduce or temporarily remove the availability of tools for offending (van der Wagen et al., 2019). Although an offender can, of course, acquire new equipment and develop new tools, the costs for committing crime are nevertheless increased. Moreover, the seizure can create momentum for the offender to change his perspectives, attitudes and behaviour online. This change can lead to different choices and create space for new possibilities and experiences, as a result of which criminal behaviour may decrease in the long term. Finally, parents have an important role in controlling opportunities to offend by supervising their child's online behaviour and preventing it from slipping into transgressive or criminal behaviour. It has been found that there is a negative relation between parental management of computer use and online deviant behaviour (Baek, 2018). However, parental supervision in cyberspace appears to be difficult, because parents do not have the skills to monitor online behaviour, while juveniles know how to keep their deviant behaviour well hidden. Moreover, youngsters have to be online a lot nowadays, for many pro-social activities such as school, whereas parents have limited ability to supervise all their online activities, especially when having full-time jobs (Matthijsse et al., 2021; Zebel et al., 2013). For these reasons, the National Crime Agency in the UK launched the #CyberChoices campaign in which parents were educated about the potential cybercriminal behaviour of their children.[2] Whether such campaigns are effective is not clear yet.

9.4.2.4 Diversion

Diversion strategies are aimed both at addressing criminogenic needs and supporting the process of desistance from crime. The strategies may help to avoid or cope with the negative consequences of labelling that often goes hand in hand with being processed through the criminal justice system. Moreover, diversion is aimed at strengthening pro-social bonds, activities and identities and avoiding the criminogenic effects of exposure to pro-criminal peers within the criminal justice system (Brewer et al., 2019).

An example of such an intervention associated with diversion is the Dutch 'Hack_Right intervention' which is developed and supported by a collaboration of actors within the criminal justice system, for example, the police, public prosecutor's office and the probation service, private cyber security companies and the hacker community. The Hack_Right programme can be imposed as an alternative for punishment or as part of a supervision

[2] See www.youtube.com/watch?v=DjYrxzSe3DU&t=1s.

programme. It addresses a number of the aforementioned criminogenic needs and specifically takes into account the online context and responsivity of the offender (de Bruijne, 2018; Schiks, van 't Hoff-de Goede, & Leukfeldt, 2021; Wieland, 2020). It is aimed at juvenile and young adult first-time cyber offenders who want to take responsibility for their actions and are motivated to participate in the programme, and who, in addition, possess a certain level of IT-skills.

The intervention consists of four modules of which the first two, 'recovery' and 'training', focus on reducing criminogenic factors (de Bruijne, 2018; Wieland, 2020). The recovery module focusses on mediation and the 'training' module focusses on cognitive and social skills that are insufficiently developed. By this training, the young (adult) offenders should gain better understanding of the consequences of their criminal actions and feel more confident about their abilities to refrain from committing cybercrime and develop pro-social behaviour. Moreover, in contrast to most of the current cognitive-behavioural interventions for offenders, this training module offers a great deal of information, for example, on what is and is not permitted under Dutch law and where the boundaries between ethical and malicious hacking lie (Schiks et al., 2021). Such knowledge can also contribute to a better cost-and-benefit analysis, as well as reduce the use of excuses or neutralisations (Xu et al., 2013). The third and fourth modules fit mainly into the desistance approach and are discussed in the next section.

The Hack_Right intervention is quite unique in the world. As far as we know, no other country has developed such intervention. However, in the United Kingdom we can find interventions (e.g. 'Rehab For Hackers' weekend) that share some similarity by focussing on talent development (see further Section 9.5.2)

9.5 The desistance approach

9.5.1 Why people stop offending

According to the desistance approach, it takes more to desist from committing crimes than just 'to quit'. It must be accompanied by a positive change in identity, as a result of which someone is committed to law abiding behaviour in the long term (McNeill et al., 2012). A distinction can be made between *primary desistance* (a period without recidivism) and *secondary* *desistance* (an identity transformation after which the ex-offender views him- or herself differently) (Maruna & Farrall, 2004; Maruna & Toch, 2005). Also, *tertiary desistance* can be important in the process of desistance, referring to the degree to which society re-accepts the offender, giving the offender a strong *sense of belonging* (McNeill, 2016; Nugent & Schinkel, 2016).

Above all, desistance approach is characterised by a natural, dynamic process that, like other behavioural changes, proceeds through both ambivalence and hesitation, trial and error, hope and despair (Laub & Sampson, 2003; McNeill et al., 2012). In order to be effective, interventions must connect to that process, rather than putting (too) much emphasis on risk factors and isolated treatment programmes – as is the criticism of the desistance approach on the What Works approach.

The desistance approach thus focuses not so much on outward behaviour and whether or not offenders commit crimes, but on events in the life course of offenders that involve changes in identity, social roles and hope for the future. Interventions should contribute to and create opportunities for important life course events and life goals. This is why they are referred to as *strength-based* interventions (Hampson, 2018; McNeill et al., 2012). The (outward) reduction of delinquent behaviour should thus go hand in hand with the (inward) development of a pro-social identity, as well as with external possibilities and opportunities to put this changed identity into practice and to realise a positive future ('hooks for change'). In that regard, it is stated that it is important for offenders to have the opportunity to *desist into something* (McNeill et al., 2012), thus emphasising the importance of non-criminal social capital, for instance, gainful employment.

The empirical evidence for the effectiveness of interventions based on the desistance approach is still limited, as the approach is still relatively young and its incorporation into specific interventions is not yet widespread. Another limitation in evaluation research is that it is complex to isolate the effects of this specific approach due to the nature of strength-based interventions, which are multidimensional, aimed at the long-term instead of at immediately and directly lowering recidivism rates.

Although no evaluation research into interventions for cyber offenders based on the desistance approach is available, it can be cautiously deduced from the literature that a great deal is expected from it (Brewer et al., 2019). Both the characteristics and motives of cyber offenders (see Chapter 4) may offer possibilities for various ‘hooks for change’ that bring about desistance from crime (Giordano, Cernkovich, & Rudolph, 2002). As far as background characteristics are concerned, it is generally assumed that cyber offenders have stronger social capital than traditional offenders, for example, because they come from families with a good socio-economic position, are generally well educated, have particular (technical) talents and possibly a career in the field of IT (see also Nycyk, 2016).

As far as motivations are concerned, a relatively large proportion of cyber offenders seem to have motivations or needs that are in principle not criminogenic, such as the need for challenge, thrill, status and peer respect in combination with an interest in IT, a curious, investigative attitude and an urge for developing IT-skills. Although some of these drives are equally important in traditional crime, in the case of cyber offenders there is usually a stronger emphasis on hackers’ abilities and skills, which require not only technical know-how but also discipline (Steinmetz, 2015a; van der Wagen et al., 2019). These characteristics and motivations provide particular starting points for the desistance process with regard to positive reinforcement (creating a pro-social identity) and providing opportunities to strengthen social roles and future plans (creating pro-social capital). Also, for offenders with an explicitly financial motive, creating social capital can be important, so the benefits of desisting from their criminal lifestyle will outweigh the benefits of continuing their criminal careers. Strength-based interventions could contribute to this process by creating clear hooks for change.

9.5.2 Interventions in line with the desistance approach

In the following pages, four (elements of) interventions are discussed that correspond with insights from the desistance approach and could be successful for cyber offenders according to the literature. Three elements can contribute directly to creating hooks for change in the life course of cyber offenders, such as education on ethical hacking, skill and talent development and strengthening their future prospects through qualifications or employment. A fourth element, involving the guidance of role models, can provide support during this entire process.

9.5.2.1 Ethical hacking

Ethical hacking means that hacking is permitted to expose vulnerabilities in systems according to certain guidelines (as formulated in the Coordinated Vulnerability Disclosure (CVD) policy) and when meeting certain conditions

(NCSC, 2013; 2018; Weulen Kranenbarg, Holt, & van der Ham, 2018; see also Chapter 3). To abide by these guidelines, it should be sufficiently clear to (potential) offenders as to what exactly is and what is not allowed by the system owner, with as little 'grey area' as possible. In practice, however, there is a lot of ambiguity and confusion (Harms, 2017), which may for instance result in offenders not reporting vulnerabilities and not engaging in CVD. The literature points out several difficulties with regard to CVD policy: hackers can perceive the rules as either unclear or unjust, they still risk legal consequences, since no guarantee is given beforehand that they will not be prosecuted, and disclosure processes are often very time-consuming or demanding (compared to the severity of the vulnerability). From the side of the companies there can be a lack of communication, denial of the existence of the vulnerability, a delayed response about the investigation and patching process or unwillingness to disclose the vulnerability to the public (NTIA, 2016; Spronk & Weulen Kranenbarg, 2020; Weulen Kranenbarg et al., 2018). Given their need for status in the hacker community and motivations such as curiosity (about the data) or money, these uncertainties can lead hackers to exploiting, selling or publicly exposing vulnerabilities instead of reporting them in a coordinated manner (Weulen Kranenbarg et al., 2018).

In order to contribute to the process of desistance, ethical hacking or CVD policy should thus be based on concise rules and good communication and should be rewarding. The Dutch Institute for Vulnerability Disclosure (DIVD.nl) has raised a (global) platform for security researchers to report vulnerabilities in line with the code of conduct.[3] Also, initiatives such as vulnerability reward programmes (VRP's) or bug bounty programmes may be very suitable (Chatfield & Reddick, 2018). Such rewards do not necessarily have to be monetary *quid pro quo* bug bounties. Important rewards can also consist of involvement in patching of the vulnerability, status and recognition and personal coaching and information sharing by experienced hackers – which can contribute to skill development (NTIA, 2016; Spronk & Weulen Kranenbarg, 2020; van der Wagen et al., 2019; Weulen Kranenbarg et al., 2018). For example, the online platform 'HackerOne' meets both needs, because ethical hacking can lead to earning money ('bug bounties') and enhancing skills is accompanied by recognition for achievements through a leaderboard.

[3] See e.g. Lawrence Abrams, 'Researchers warn of unpatched Kaseya Unitrends backup vulnerabilities', *Bleeping Computer,* 26 juli 2021.

Although evaluation research on CVD policy is hardly available, the literature does describe a number of potentially positive effects. First of all, ethical hacking can contribute to improved internet security by reporting vulnerabilities (Chatfield & Reddick, 2018; Weulen Kranenbarg et al., 2018). In addition, ethical hacking stimulates the development of creativity and technical skill (Wible, 2003). Also, with the help of ethical hacking policies, online norms and boundaries (both legal and ethical) are more clearly stipulated, facilitating the need for challenge and thrill to be used in a pro-social way (Siponen, Vance, & Willison, 2012; Spronk & Weulen Kranenbarg, 2020; van der Wagen et al., 2019; Weulen Kranenbarg et al., 2018). Finally, it can be expected that cooperation and mutual trust between hackers and actors within the criminal justice system, such as the police, will increase, as will self-regulation among hacker communities. Research has shown that moral convictions and feelings of shame are strong predictors of the propensity to commit cybercrime among young people (in this case illegal downloading) (Siponen et al., 2012). Moreover, the younger the age at which hacker ethics are learned, the better hackers will be able to resist (peer) pressure of online deviance during their teenage years (Kao et al., 2009).

9.5.2.2 Role models

Obtaining recognition, respect and personal coaching from more experienced hackers fits well within the desistance approach, which emphasises the importance of role models in undergoing identity change. Although little research has been carried out on the effects of role models in general, let alone in relation to cybercrime, interventions by the police in the Netherlands and the UK, for example, clearly take into account the contribution that role models, coaches or mentors can make in supporting young hackers to stay on the right path (National Crime Agency, 2017). In the Dutch Hack_Right intervention, as discussed earlier, training and coaching is provided by experienced hackers working as IT professionals or cybersecurity specialists. Through a working/learning trajectory, which is supervised by these professionals, young cyber offenders with IT-skills can experience what a future workplace could be like (Schiks et al., 2021).

Even in a less formal setting, the hacker community (e.g. ‘old guard’ hackers; Rogers, 2006) can generally be expected to provide good examples and to coach young hackers as to what is and what is not in accordance with the ethical hacking guidelines (Steinmetz, 2015a; van der Wagen et al., 2019). Role models or coaches can thus be important in the desistance process in several ways: by offering a good example to cyber offenders, by challenging them to develop their talents in a pro-social manner and by giving them respect and recognition, which re-affirms their self-esteem and (pro-social) identity. In addition, role models are important to hold onto in the ambivalent process of desistance, as this process does not happen overnight and has its ups and downs. Although support and coaching could also be offered by 'regular' supervisors, such as probation officers, an extra motivational effect can be expected from the involvement of 'technical' coaches, to whom cyber offenders can look up to and with whom they can speak their own (technical) language.

9.5.2.3 Talent development

In order to develop technical talents and recognise achievements, hacking competitions can play an important role. Although they are not developed as such, hacking competitions can be regarded as a preventive intervention because they can contribute to the development of pro-social attitudes and relationships as well as a pro-social identity. The literature often refers to 'hack-in-contest' or 'hackathons' (Wible, 2003), or, in a broader sense, to gamification, as discussed earlier (Aiken et al., 2016). Such hacking games are organised and sponsored by both public agencies and private parties (Oosterwijk & Fischer, 2017). For example, each year the European Cyber Security Challenge takes place that connects young talents from across Europe in a cybersecurity competition. In the Netherlands, the police have set up the website 'crimediggers.nl' to challenge young hackers to test their skills and to see if they might be qualified to join the digital unit of the police. Similarly, the UK's National Crime Agency is organising a 'Rehab for Hackers' weekend,[4] focusing on education and preventative advice, to which the parents or supervisors of the young people are also invited (Keizer, 2019; Stanton, 2019).[5]

To cyber offenders for whom challenge, skills, recognition and status are important motivators, these hack-in-contests could offer an alternative to malicious hacking. Another benefit of these competitions is that they can effectively contribute to (improved) relationships between young hackers and professionals in the field of enforcement and cybersecurity (Oosterwijk & Fischer, 2017). In addition to hacking competitions, initiatives such as hackerspaces or cyber working/meeting places could make an important

[4] See M. Ward, 'Rehab camp aims to put young cyber-crooks on right track', *BBC.com*, 24 juli 2017.

[5] See K. Collins, 'Inside the boot camp reforming teenage hackers', *CNET.com*, 6 August 2018.

contribution not only in developing skills, but also in building pro-social relationships and CV building (pro-social roles and future plans) (van der Wagen et al., 2019, Brewer et al., 2019). Young people can visit these locations on a voluntary basis to be educated by experts on IT-skills and hacking ethics at the same time. Such initiatives offer the possibility for hackers to meet like-minded peers and to build pro-social offline relationships, which can be helpful for offenders who operate mainly solo or for whom establishing (offline) social contacts is difficult and who are struggling with loneliness. It could also provide a positive daytime occupation for young people who are unoccupied or dropped out of school. An important question is, however, whether such interventions are able to reach out to cyber offenders who suffer from social isolation (van der Wagen et al., 2019).

Finally, in stimulating technical talent, schools can also play an important role. This can, first of all, be done by offering customised education that matches the technical interests of young people. After all, potential cyber offenders generally appear to be less interested in the regular curriculum but have a specific interest in ICT (see also Chapter 4), while ICT-related subjects are hardly ever offered or are of poor quality (Árpád, 2013; Chiesa et al., 2009; Xu et al., 2013). In addition, schools could offer young people a second chance if they cross the line, for example if they hacked the school system. Their technical talent can be put to good use by the school by employing these young offenders to offer education on online safety, to contribute to lessons on an IT-related topic, or to expose more vulnerabilities in the online school system based on the CVD policy (Spronk & Weulen Kranenbarg, 2020).

Similar to learning hacker ethics, the aforementioned initiatives offer challenge, competition and talent development, which is rewarded in the form of recognition, status and self-esteem (positive reinforcement). Also, rewards can be gained, either financial rewards or boosting of CVs by skills and achievements obtained, which prepares them for a career in IT (Aiken et al., 2016; van der Wagen et al., 2019). At the same time, it can also be expected that such talent development initiatives will not pull offenders away from also undertaking illegal activities for the excitement and thrill they offer. After all, legal and illegal hacking need not be mutually exclusive, especially because the internet is always ‘open’ (Brewer et al., 2019). However, it is expected that a certain proportion of cyber offenders will be motivated to leave the wrong path by learning alternative ways for using their technical skills (Oosterwijk & Fischer, 2017; van der Wagen et al., 2019; Wible, 2003).

9.5.2.4 Career perspectives

Interventions focussing on the increase of labour market skills and capital are in line with the desistance approach. Also the What Works approach recognises that the enhancement of protective factors can actively reduce the effects of criminogenic factors or the criminogenic factors themselves. For example, having a job is often considered a protective factor that can prevent delinquent behaviour (e.g. Verbruggen, Blokland, & van der Geest, 2011). Both approaches, therefore, endorse interventions that focus on helping offenders to enter the labour market. This could create hooks for change, as the desistance approach recommends especially since hackers often possess (strong) skills, talents, ambitions and creativity, which the current job market urgently requires. It thus serves society in both ways if young deviant hackers are convinced of the fact that they can use their skills in a pro-social way, in the context of a good job, with which they are able to earn a good living. In addition, having a good job can provide them with the recognition, status and challenge they are looking for. Interventions focussing on creating career perspectives can thus fulfil an important condition in the desistance process, namely creating the opportunity 'to desist into something' (McNeill et al., 2012).

Professionals in the criminal justice system consider the provision of job opportunities an important element in the desistance process of cyber offenders (van der Wagen et al., 2019). Within the fourth module 'positive alternative' of the Hack_Right intervention, young hackers are required to complete a work- and learning trajectory at a cybersecurity company or IT department at, for example, a bank or accountancy firm. There, they teach these cyber offenders how to use their talents in a positive manner (Schiks et al., 2021). Interviews with both offenders and professionals involved in the intervention showed that offenders stay in touch with the workplace afterwards, have often found an internship or job at another company and are more aware of the consequences of their actions (Schiks et al., 2021). However, more critical evaluations are also available, stating that the exercises were too easy for the more technically skilled participants or that the intervention is perceived as a 'soft punishment' or even a 'reward' (Schiks et al., 2021).

An important point to be noted here is that research among experts working with cyber offenders has shown that within certain social domains, such as education and work, problems may exist that do not immediately emerge as criminogenic factors in a risk assessment (i.e. factors related to criminal behaviour). Still, interventions addressing these problems can contribute to creating experiences of 'success' and to the strengthening of pro-social identity and pro-social relationships, which is closely in line with the strength-based approach (van der Wagen et al., 2019).

On the basis of the opportunity theory, however, the opportunity that such jobs create for committing cybercrime should also be taken into account. Longitudinal research among Dutch cyber offenders showed that employment in general does not have the same protective effect as it has for traditional offenders. Moreover, employment in the IT sector increases the likelihood of committing cybercrime, although these effects were not significant (Weulen Kranenbarg et al., 2018). This risk was also addressed by Schiks et al. (2021), while in their interviews, respondents mentioned the risk that participants may gain knowledge from the workplaces they were introduced to, which they can use for criminal purposes.

Finally, it is important that criminal justice interventions take into account the harmful consequences that contact with the criminal justice system can have for the job opportunities of cyber offenders. For example, they can be confronted with the 'mark' of a criminal record, because criminal background screening increasingly takes place, especially for positions in public service, such as police officer or cybersecurity specialist at large companies that work for public institutions (van 't Zand-Kurtovic, 2017). Diversionary interventions, such as Hack_Right, account for these collateral consequences and aim to avoid hampering of future prospects by a criminal record.

9.6 To conclude

This chapter focused on the question what interventions and elements of interventions can be considered suitable for offenders of cyber-dependent crime. Based on three different approaches to interventions, various types of interventions, both reactive and preventive, have been discussed in light of their (potential) effectiveness to reduce cyber offending.

In line with the rational choice approach, interventions are considered to be successful if they create a sufficiently deterrent effect. The problem, however, is that currently none of the three basic conditions for deterrence – a sanction being certain, swift and severe – seem to be sufficiently met: detection and apprehension rates are low, investigation and prosecution processes often take a long time, and punishments seems to be relatively mild. For this reason, better outcomes may be expected from the potential success of situational crime prevention, including online policing, digital warning messages, the disruption of online markets, and education in schools.

The What Works approach assumes that interventions are effective if they target criminogenic needs, while taking into account the offender's responsivity. Currently, however, there is a lack of adequate diagnoses of risk factors and the way they manifest in online criminal behaviour. Both existing diagnostic tools and interventions could, for example, take an increased account of the unique motivations for cybercrime and of the fact that offenders are not always sufficiently aware of the illegal nature and harm caused by their behaviour. Therefore, interventions could aim at increasing the visibility and proximity of damage and victims. Interventions that focus on creating awareness and mentalisation (empathising with others), such as victim-offender mediation, are expected to have positive outcomes.

The desistance approach favours a strength-based approach especially because social capital and social bonds – which cyber offenders seems to possess to a greater extent than traditional offenders – can be damaged by severe punishment. Cyber offenders also have particular talents and skills (strengths) that are of clear value to society, provided that they are used in a pro-social way. It is expected that these strengths can be developed by interventions such as hacking competitions and cyber working/meeting places. These interventions focus on learning the rules of ethical hacking, stimulate the development of technical skills, and by doing so enlarge career prospects. Role models are of added value by providing support throughout the entire desistance process.

Based on the above insights, it is recommended that interventions should combine elements that are in line with the principle of risks, criminogenic needs and strengths as much as possible. The Dutch Hack_Right intervention is an example of an intervention that combines a risk- and strength-based approach. Both are important, since increasing only IT skills and career opportunities without working on moral awareness and a pro-social attitude can lead to advanced ways of committing cybercrime.

To conclude, it can be noted that there is a lack of research on interventions for cyber offenders and their possible success. Besides validating existing diagnostic instruments and supplementing them with risk factors related to the online world, it is necessary to map out for which groups or types of cyber offenders traditional interventions are effective. Finally, it is crucial to take into account the varying capacities, learning styles and motivations (responsivity) of cyber offenders. Because cyber dependent crime is considerably different from traditional crime with regard to the online context and the technical nature of the crime, a tailored approach is key.

9.7 Discussion questions

1. What are the current limitations of the body of research dealing with the effectiveness of interventions for cyber offenders?
2. What unintended effects could be expected from interventions that aim to target the rational choice process, given the different motivations of cyber offenders?
3. What reasons can be provided for the limited success of warning banners?
4. In what ways can the strategy of disruption be successful, taking into account the displacement effect?
5. Why do both general and special deterrence seem insufficient with regard to cybercrime, given the three basic conditions for deterrence?
6. Why is there (still) limited knowledge of risk factors and criminogenic needs that play a role in cybercrime?
7. In what way could existing interventions be adjusted to the online environment in which cybercrime takes place?
8. What starting points do the characteristics and motivations of cyber offenders offer for a strength-based approach?
9. What advantages and disadvantages could be associated with strength-based interventions, such as the Hack_Right intervention?

9.8 Core terms

- Cease and desist
- Desistance approach
- Detention
- Disruption
- Diversion
- Dynamic and static risk factors
- Ethical hacking

- Financial penalties
- Gamification
- General and special deterrence
- Hack_Right
- Hooks for change
- Interventions
- Online policing
- Rational choice approach
- Recidivism
- Risk-Need-Responsivity model
- Role models
- Situational crime prevention
- Strength-based interventions
- Talent development
- Warning banners
- What Works approach