INTERVENTIONS FOR YOUNG CYBERCRIME OFFENDERS

K. Oosterwijk Msc
T.F.C Fischer, PhD
Section Criminology
Erasmus School of Law
Erasmus University Rotterdam
Date: June 5th 2017

Summary

Introduction and research questions

Together with a strong increase in the use of the internet in the past decades, levels of cybercrime also increased strongly. Young people are strongly represented on the internet and research shows they are relatively often offenders of cybercrime. There is, however, limited systematic knowledge available on possible interventions reducing offending risks. This study aims to increase this knowledge in order to facilitate the development of preventive measures against cybercrime offending among young people. Therefore, we study the design, (intended) mechanisms, and effects of cybercrime interventions for young people.

The research questions are:

1. Which interventions can be found in the international literature, aimed at reducing cybercrime offending among young people?
2. In what categories can we organise those interventions with respect to:
   a. The type of cybercrime it treats.
   b. The population it selects.
   c. The underlying theory that explains why it is expected to be effective.
   d. The methods used.
   e. The stakeholders who are involved.
3. What do we know about the program integrity of the interventions?
4. What do we know about the effectivity of the interventions in reducing digitalised crime and cybercrime among youngsters and what study designs were used?
5. How do effective and promising interventions differ from not effective interventions, with respect to characteristics summed up in the second research question?

Research methods

The research was done in two phases. In *phase 1* we analysed evaluation research of programs for (potential) young offenders of cybercrime as described in the scientific literature. In *phase 2* an in-depth study was held for two types of cybercrime, i.e. cyber aggression and hacking. In this phase we looked beyond the evaluated interventions and searched for insights, experiences, and suggestions in literature and from experts in the field that might be relevant in the development and selection of future interventions.

To find evaluated interventions for (potential) young offenders of cybercrime an extended systematic literature search has been done. This search focused both on sources that specifically concern evaluated interventions for young cybercrime offenders (reduction of re-offending) and evaluated interventions that aim to prevent cybercrime offending in general populations (prevention of cybercrime in general). For the in-depth study on cyber aggression and hacking interventions (phase 2) we used sources from the systematic literature search that did not qualify for phase 1, but that gave background information on offender groups or offending behaviour. Several additional reviews and sources about cyber offender populations

have been included too. Next to the literature we also consulted experts (from the field and in research) during expert meetings, interviews and in e-mail conversations. With this consultation of experts we aimed to collect *up to date* information on recent and innovative interventions as well as reflection on the results from our literature study.

Results

Systematic literature review of evaluated programs

Our quest for program evaluations produced studies for 39 different programs. This appeared to be almost exclusively programs designed for general populations. These programs focus on offending prevention for possible offenders instead of re-offending reduction among proven offenders. Moreover, the large majority of preventive programs focussed on the whole system, so these programs also try to change behaviour of (possible) victims and bystanders and not just behaviour of (possible) offenders. Two studies focus on interventions specifically designed for actual offenders, namely the use of *reintegrative shaming* for hackers and of *restorative justice* for *stalking*. Both interventions however were rather approximations than actual and detailed programs. The program evaluations therefore, were content evaluations and could not draw any definite conclusions on actual effects. Below, we discuss the characteristics of the programs found to answer research questions 2 until 4. This section will end in the conclusions that an in-depth study is necessary for the answer on research question 5.

Type of cybercrime

The programs from the systematic search focus on the following types of cybercrime:

- cyberagression (10)
- sexting (13)
- hacking (4)

Moreover, eight programs on online safety in general were found in which the offender role was treated explicitly (i.e. creating consciousness about what illegal behaviour is and what consequences this behaviour might have). Finally, we selected evaluations on four technical interventions that are specifically focussed on (potential) offenders. The cyber aggression programs focus mainly on cyberbullying and in one case on stalking. This means that for many types of cyber aggression no programs were found. Moreover, no programs were found for the prevention of financially economical offending in cyberspace.

Populations selected

The programs for online safety and cyber aggression, focus in most cases on children and youngsters from primary school and the first stages of secondary school. Sexting programs are aimed at youngsters at secondary schools. The hacking and technical interventions do not mention specific age groups. Most programs select the entire population and not only offenders.

Theories

Just for a small part of the programs, theories were described that explain why the program is expected to work. Theories that were most often described are social learning theories, the

theory of normative social behaviour, and the theory of planned behaviour. The cyber aggression programs are based in particular on or are remakes of established anti-bullying programs. These programs especially use system focussed theories in which group norms (descriptive and injunctive) and the impact of such norms on the behaviour of individuals has a central position. For this type of cyber aggression, decreasing the social benefits for offenders, by creating disapproving norms at the group level, will decrease offending risks. The theoretical basis of the *sexting* programs is very limited, the only theoretical notion that is described is deterrence. The hacking programs describe a combination of assumptions derived from the rational choice approach, *reintegrative shaming* and deterrence.

Methods

(Psycho)-education and cognitive behavioural methods (including positive enforcement and increased moral reasoning) are methods used frequently in the programs that were evaluated. Role-playing is a tool in those programs to facilitate possible offenders to learn about the norms of others and to train reaction strategies. In several programs training is also used to increase social skills and cognitive and affective empathy. The psycho-education tries to increase knowledge about victim consequences and possible sanctions for the offender. This final strategy is also used in hacking programs however the specific methods used in hacking interventions are poorly described.

Stakeholders involved

A sound consequence of the fact that most programs aim at general populations of youngsters is that execution of the programs takes place mainly at schools. Sometimes, lessons are given by teachers themselves, sometimes by external trainers from (privat) companies who often also developed the programs. For some programs it is described that they are, also available in the correctional field but no evaluation studies were found for such use. For one possible effective hacking intervention (the *hack-in-contests*) companies are important parties in the execution of the program.

Program integrity

Limited information is available about whether programs turn out the way they should according to the program description. One clear omission in many programs, both in the program descriptions and in practice, is the lack of a central role for activating modules in which the training of skills and interactive learning should take place. As a consequence, both in the translations of known working mechanisms to program descriptions and in the program integrity itself are not sufficiently elaborated. Effects of the programs might become stronger if these elements are better integrated in the programs.

Effectivity

Effect studies were available for one third of the programs (13 of 39). These are mainly online safety and cyber aggression programs. For the rest of the programs theoretical evaluations were available that discussed the possible effectivity of the programs by analysing the

descriptions of the programs. Of the 13 effect studies only 4 (3 on cyber aggression and 1 on hacking) had a fully experimental design, another 5 studies had a quasi-experimental design[1]. The cyber aggression programs decrease cybercrime offending to some extent. No effects were found for the programs on online safety, sexting-, and hacking.

Differences between effective or promising programs and non-effective programs
Only one type of programs: anti-cyberbullying programs, were found to be effective in the reduction of offending risks. These programs include several success factors for effectivity, like a focus on dynamic criminogenic needs (i.e. group pressure, lack of supervision, and lack of empathy for victims, partly as a result of the online disinhibition-effect), and the [afstemming] of the program at the responsivity of the population at aim (in this case a system approach with clear attention for groupnorms is important). Programs, solely using education or deterrence appear to be not effective.

For many programs no effect studies are available so few firm conclusions can be drawn about the effectivity of the programs studied. Based on content analyses, we have positive expectations about hacking interventions bases on *reintegrative shaming*.

In-depth study potential interventions

The in depth study in the second phase of our research concerns cyber aggression and hacking and facilitates a somewhat more elaborate answer on research question 5 and as a result insights for effective interventions. Although the answer on this question differs between the two types of cybercrime, a great need for more knowledge and training is present among professionals in dealing with both types of crime. Besides knowledge about the behaviour and circumstances of cyber offenders, professionals should be trained in using technological interventions for supervising and treating young cyber offenders. In the development of interventions, train-the-trainer program should therefore not be forgotten.

Cyberagression
The literature shows that young offenders of cyber aggression mainly resemble offline aggression offenders. Existing behavioural programs used by correctional and forensic care institutions (i.e. Aggression regulation treatment or cognitive skills programs) might be effective in reducing the risk of reoffending in cyber aggression. An important difference, however, is that general levels of aggression for offenders of cyber aggression are lower than for offline aggressive offenders. Moreover offenders of cyber aggression are more often victims of online and offline aggression, so motives for offending might be different. Finally, differences were found in characteristics affecting responsivity for interventions like social intelligence.

Another important effect that should be concerned is that of online disinhibition. Because of the anonymity of both offender and victim, the experience of the consequences of the behaviour for offenders might be fundamentally different compared to offline aggression. Possibly, recent developments in *virtual reality* and *serious gaming* can contribute to interventions in which youngster better become aware of the consequences of their behaviour.

[1] Those quasi-experimental design studies have a pre- and post- intervention measurement and compare intervention and control groups. However those groups are not formed by chance as in a real experiment.

Those techniques should however first be tested more elaborately and next be adjusted for different types of offenders, crimes and situations.

Hacking

According to both the literature and experts, hacking interventions should not focus on the suppression of hacking behaviour in general, but on preventing that youngsters turn from the more 'bening' types of hakcing to more detrimental types in which financial gains or power are important motives. Hacking interventions aimed at creating consciousness among hackers about the damage they create and the consequences there actions may have for their own future are expected to be the most effective. Offering legal alternatives (hack in contests) in which youngster can find the challenges and sensations might help in preventing illegal and harmful hacking. Among young hackers it is important that reactions on illegal actions are prompt and that controlling actors stay in contact with the offender. Both expert and the literature point at the *peergroup* as an important factor of influence and suggest to give the peergroup an important role in the interventions. There is however, very limited information available about the possibilities and risks of such a role for the peergroup. Automized reactions on hacking behaviour as used in interventions like 'digigeren', may become useful in the future to improve possibilities for prompt reactions on young hackers. Format and content of the message brought with such an intervention appears to be crucial for effectivity. Until now, no effect studies were found supporting effectivity of such automatic warnings.

Finally, various technological interventions are being developed at the moment that might be helpful in supervising offender behaviour after sentencing (i.e. biofeedback, or wifi-blocking in a bracelet). Again, no evaluations of the effectivity of the interventions could be found. Comparable with such interventions for offline crime (like electronic monitoring) we can expect that they will only be effective on the long term if combined with interventions treating the criminogenic needs of offender.

Conclusions

The most important conclusion of this study is that in scientific literature no descriptions were found of effective interventions being a correctional reaction on actual offending behaviour of young cybercrime offenders. A couple of studies describe methods that can be used in reaction on actual offending (*reintegrative shaming* and *restorative justice*), but most programs are aimed at the prevention of offending in general populations of youngsters. Of all preventive programs, just the anti-cyberbullying programs showed to be effective in the prevention of offending. These programs mainly use system-focussed methods in which building disapproving group norms against cyber aggression and the training of bystanders and victims play an important rol. Besides, the programs focus on improving (potential) offenders' consciousness of the consequences of their behaviour.

Recent studies improved our knowledge on backgrounds and dynamics of cybercrime (see chapter 5). These insights suggest that offline aggressive offender programs can probably be used for cyberaggression offenders too. However, adaptations wil be necessary for considering cybercrime specific factors in the behavior (i.e. different offender characteristics compared to offline aggression and online disinhibition). Interventions that respond to hacking should be capable to give prompt reactions. The specific content that effective reactions should

have, is however still unclear. In the preventive sphere, offering legal alternatives that challenge hackers may be a possible effectieve strategy, but again little is known about effectivity and scope of such interventions.

An important comment is that both in the population of cyberagression offenders and of hackers a wide variation in offender characteristics exists. Moreover, both populations appear to have subgroups we know only little about. For aggression we know that offline and online aggression often comes together in the same persons. However there is a group online aggressive offenders who only offend online. It is still unclear which criminogenic needs this group has. The same is the case for hackers who have financial gains or power as the core motivation for offending from the start of their hacking career on. Those offenders are not hacking with the samen motivations as the often described *eager* and *sensation seeking* secundary school student who attains step by step into a criminal hacker.

The final conclusion of the study therefore is that for the development of (correctional) reactions toward offenders of cybercrime, it is important to further improve the knowledge about the group. As a part of this job it would be relevant to study how well cybercrime offenders are recognized and registrated in the correctional system at the moment. Next, we should describe in more detail how the correctional system reacts on these cybercrime offenders and to what extent this reaction answers to the criminogenic needs and responsivity of the offender. As a result of this exercise, it can be decided which specific interventions can be used or should be developed, how to deal with the cyberelement in signaling an diagnosing by police and (youth)probation services, and (forensic) care, and how professionals should be trained.