Youthful offenders of cybercrime in the Netherlands: An empirical exploration

Summary

Sven Zebel[1]
Peter de Vries[1]
Ellen Giebels[1]
Margôt Kuttschreuter[1]
Wouter Stol[2]

[1] University of Twente, Psychology of Conflict, Risk and Safety (PCRS)
[2] Northern Graduate School Leeuwarden, Lectorship Cybersafety / Dutch police academy / Open Universiteit

Research carried out for the WODC, Commissioning Research Division, Ministry of Security and Justice.

UNIVERSITY OF TWENTE.

NHL Hogeschool / Politieacademie / Open Universiteit

The use of Information-and Communication Technology (ICT) among young people has increased enormously. This widespread usage of ICT also implies however that ICT applications may become increasingly important in the illegal and punishable activities in which young people are involved, either as targets (victims) or as offenders of crime.

For the Management of Judicial Youth Policy of the Ministry of Security and Justice in the Netherlands, it is important to have as much insight as possible into the involvement of young people in cybercrime in a broad sense (where ICT is used as a means to commit crime) and cybercrime in a narrow sense (when the ICT structure itself is the target of criminal conduct), as well as their interrelation. When cybercrime appears to be best characterized as traditional juvenile delinquency with new means, different policy choices are required than when cybercrime in a narrow sense turns out to be on the rise with juvenile offenders who diverge from traditional juvenile delinquents in terms of their characteristics , motives and modus operandi (see also Yar, 2012).

The purpose of this investigation is therefore to map the nature and extent of cybercrime in the Netherlands in which young people under 18 are involved as perpetrators, and offer insight into the characteristics of this crime.

Several authors note that (very) few scientific empirical studies have been conducted that focus on perpetrators of cybercrime (e.g. Holt, Bossler & May, 2012; Van der Hulst & Neve, 2008; Leukfeldt, Veenstra & Stol, 2013). For that reason, the focus of the present study will be on the formulation of evidence-based answers to the research questions. The following research questions are central:

1. To what extent are young people under 18 years involved as perpetrators of (different forms of) cybercrime in the narrow and broad sense in the Netherlands?
2. To what extent and which kind of combinations of cybercrime in the narrow and broad sense appear in the Netherlands among juvenile offenders under 18?
3. What kind of profile do young people have who commit cybercrime in the narrow and broad sense?
4. Which modus operandi are used in the different forms of cybercrime in which young people are involved as perpetrators?
5. How do young people become involved in cybercrime in the narrow and broad sense?
6. How do young people think about cybercrime in the narrow and broad sense?
7. Are there specific risks that flow from the digital behavior of young people and from their potential involvement as perpetrators of cybercrime?

To answer these research questions a mix of quantitative and qualitative methods was deployed on different information sources: the Monitor of Self-Reported Juvenile Delinquency of the WODC and the study "Youth and Cyber Safety" of Kerstens and Stol (2012) - both self-report studies, - the Research and Policy Database Judicial Documentation (‘OBJD’) of the WODC, the statements found on Rechtspraak.nl, and a series of interviews with experts and stakeholders on this topic. A limited amount of overlap exists between these sources. Few sources answer all research questions, and the degree to which specific forms of cybercrime can be found in each source differs.

The results of this examination led us to formulate a number of propositions. These are listed and elaborated below. We conclude with a discussion of the risks involved in the digital behavior of

young people. The recommendations that flow from this research for policy, and the direction and methodology of future research can be found in the final chapter of this report.

"Young people are involved to a small extent in cybercrime"

The present study was unable to confirm the idea of a large and growing problem of cybercrime among young people that is present in the media. The self-report studies and cybercrime registered in judicial data show that the majority of cybercrimes under investigation in the period 2006-2011 are reported to a (very) low degree (less than 5.5 % of all young people surveyed in the samples) or registered among juvenile offenders (0.3% of all registered youth crime in the Netherlands consists of cybercrime). These numbers apply to the following forms of cybercrime: online auction fraud, the distribution of a virus, hacking, creating or distributing sexual materials, forgery of debit or value card and threatening others online.

The qualification 'to a small extent' that we attach to these percentages perhaps needs some explanation. When we focus on the percentage of 5.4% of young people that indicates that they threatened someone online, this implies that on an average high school of 800 students 43 students will indicate that they committed this offense in the last year. Forty-three students almost entail two classes of 25 students each. However, this number also implies that an overwhelming majority of 757 students at this school will indicate that they did not commit this offense. In other words, almost 95% of the students will indicate that they did not threaten someone online in the past year. This latter consideration is the reason that we interpret these findings as an involvement of young people 'to a small extent' in cybercrime. That said, the other forms of cybercrime mentioned above were self-reported by 3.1% or less of the young people surveyed, or accounted for less than 0.3% of the registered youth crime in the Netherlands.

Three other forms of cyber criminal behavior that young people reported more often in the current research were virtual theft, illegal downloading and / or sharing of software and music, and cyberbullying. However, some clear explanations exist for these higher self-report rates. Not all actions involved in these behaviors are criminal offenses under Dutch law (for example, illegally downloading music and gossip as part of cyberbullying); young people therefore do not consider these behaviors as criminal acts (see Kerstens & Stol, 2012; Moon et al, 2012). In addition, the fact that virtual theft is a criminal act (and thus punishable) is virtually unknown among young people (Jansen, 2012).

Can we interpret these findings as a reliable representation of the low degree of involvement of young people in cybercrime in the Netherlands? This is an important and at the same time difficult question to answer. It should be noted that the registered cybercrime among juvenile offenders in this report is almost certainly incomplete. That is, Leukfeldt, Veenstra, Domenie and Stol (2013) recently identified several major obstacles in the handling of cybercrime cases in the criminal justice domain in the Netherlands.

However, the self-report studies in this report are not affected by these obstacles in the criminal justice domain, because young people are asked directly to indicate what criminal acts they have committed. In doing so, their anonymity is guaranteed. Obviously, these studies have others limitations (see chapter research methods in this report). The main limitation of the study of Kerstens and Stol (2012) is that their sample of young people is not representative of the population of Dutch

youth. However, the findings of the self-report study of Van der Broek and colleagues (2013) can be considered as representative of Dutch youth, and in their study the self-reported degree of involvement in cybercrime was low as well. In short, taking into consideration the limitations of the self-report studies, we can be more confident in the picture that these studies paint on the degree of involvement of young people in cybercrime in the Netherlands. And, this degree of involvement is, as explained above, low.

"When young people do commit cybercrime, it often involves one specific type of cyber offense"

The findings of this investigation suggest that combinations of different forms of cybercrime (in the narrow and broad sense) are rare among young people. For example, the self-report studies indicated that threatening others online and the distribution of viruses are committed largely by different juvenile offenders; the registered cybercrime showed that in a large majority of all cybercrime cases with juvenile suspects only one form of cybercrime was found (i.e. one section of the law). The statements on Rechtspraak.nl as well as the interviews also did not give rise to concrete conclusions about the occurrence of combinations of cybercrime in the narrow and broad sense among young people.

"Youthful cyber offenders have largely mundane characteristics"

The (small number of) juveniles who committed cybercrime showed to a large extent features that do not differ from everyday juvenile offenders. The demographics sex and age played their usual role: boys commit more online threats, auction fraud, and virtual theft, and produce and distribute more sexual images that display young people than girls, and the degree of cybercrime committed increases between the age of 12 and 17. The only cyber offense under investigation that formed an exception to this pattern was cyberbullying: girls reported this to the same extent as boys (see Kerstens & Stol, 2012, p 95.). Victimization also predicted committing cybercrime: young people who had been the target of cyberbullying, auction fraud, virtual theft and unpleasant sexual questions and /or requests online, also reported more frequently being the offender of these cybercriminal behaviors. In offline juvenile crime, this relationship is also observed (see Wittebrood & Wilsem, 2000). Young people also indicate well-known motives to commit cybercrime: virtual theft and cyber bullying are done for fun, to reciprocate being bullied (in the case of cyber bullying), to take revenge, or for financial reasons (in the case of virtual theft) (Kerstens & Stol, 2012).

Isn't there anything then that distinguishes youthful cyber criminals? Yes, there is. In the introduction, the psychological "disinhibition" that can occur when young people engage in cyberspace is discussed (Suler, 2004). This online disinhibition has significant meaning for committing cybercrime: young people who indicated that they feel less restrained online and find it easy to disclose personal information online also report more frequently that they were perpetrators of auction fraud, virtual theft, cyber bullying and the production and distribution of sexual material. The influence of this disinhibition remains strong even when the influence of all other traditional factors is controlled for (see Kerstens & Stol, 2012).

It is noteworthy that the above profile only relates to young people who committed cybercrime in the broad sense. Profiling young people who commit cybercrime in the narrow sense was difficult in this study. However, the registered cybercrime in the judicial data (OBJD of the WODC), although incomplete, offered some insight into the profile of juvenile suspects of cybercrime in a narrow sense

(n = 106), as well as cybercrime in a broad sense (n = 166). Moreover, it was possible to compare these profiles with the profile of juvenile suspects in the general population in the Netherlands. This source revealed that juvenile suspects of cybercrime in a narrow (and broad) sense are born more often in the Netherlands than juvenile suspects in the general Dutch population. With respect to cybercrime in a narrow sense, there was not a single offender who was born elsewhere. In addition, juvenile cyber suspects differentiate themselves in terms of their criminal career: a larger part is first offender and a much larger portion does not relapse into crime compared to the general population of juvenile suspects in the Netherlands. We must be careful in drawing firm conclusions based on these data, but the above profile at least raises the question whether the juvenile suspects that are accused of cybercrime in the strict sense in the Netherlands constitute a more specific, homogeneous group of offenders than those involved in other forms of juvenile delinquency.

"A limited view on the modus operandi of young people who commit cybercrime in a narrow sense"

It is striking that only in some forms of cybercrime in a broad sense more insights emerge into the modus operandi; whereas the "MO" of young people who commit cybercrime in a narrow sense remains largely unknown. According to Kerstens and Stol (2012), cyberbullying is often done together with others, and in the majority of cases the victims are acquaintances of the offender. With respect to virtual theft slightly less than half of the offenders indicate that they know the victim; it often involves acquaintances, friends/girlfriends in their neighborhood or at school, and/or family members.

A common technique for virtual theft is social engineering: persuading the victim to do something that he or she normally would not do. To commit virtual theft, perpetrators use "phishing", try a scam or simply ask the password of victims to steal virtually. In addition to these forms of social engineering, offenders also try to crib passwords or attempt hacking to commit virtual theft.

The statements on Rechtspraak.nl shows how the offense threatening others online is committed: threats of violence are expressed via Twitter, Facebook, mobile phone or chat; it may constitute threats to abuse, impose death, commit sex crimes, or to disclose harmful (picture) material about the victim online.

Finally, the interviews offer support for the existence of two types of juvenile hackers as is discussed in the introduction. There are young people who have little knowledge and skills, and get information from others about how to hack, which they will then try for kicks (the "novices" or "newbies" from the scheme of Van der Hulst & Neve, 2008). Then there are the "nerds", who have considerable knowledge and as a hobby experiment on the Internet; they may share this knowledge later with other young people which also offers them status in the offline world. This latter group is similar to the "virus writers" or "encoders" that are mentioned in the introduction.

"Experimenting, anonymity and gaining respect as causes?"

We could only use the statements from the interviews to say anything about the origin of cybercrime among young people; in doing so, it needs to be taken into account that the interviewees had a limited degree of experience with young people who commit cybercrime. Their answers to the

questions concerning the origin of cybercrime were therefore based mainly on indirect information, impressions, and their perspective on perpetrators.

Several interviewees indicated that young people can become perpetrators of specific forms of cybercrime (hacking, identity theft and slander via the Internet) through a combination of experimentation and anonymity, in a safe home environment. Cybercrime can also be a way to acquire respect for young people who are less popular or socially skilled in the offline world. In doing so they can easily progress in committing forms of cybercrime, because the probability of detection is relatively small, and the police has difficulties to keep up with all new developments (something which young people are aware of).

Interviewees from the IT and investigative sector point out that technical knowledge does not necessarily play a crucial role in committing cybercrime in the narrow sense; it is more important that young people have an interest in committing these forms of crime. One interviewee from the IT sector indicates that cybercrime in the narrow sense starts among the "nerds"; similarly, an interviewee from science indicates that cybercrime in the narrow sense begins with trying out the knowledge that a young individual already possesses. This is in line with a recent Chinese study based on interviews among Chinese hackers, in which it was concluded that particularly very talented students are those that become hackers. On the one hand, the researchers attribute this finding to identification with peers in combination with limited social control in their environment, and on the other hand a limited moral development (Xu, Hu & Zhang, 2013). Furthermore, this study suggests that there may also be a positive relationship between certain forms of cybercrime and education level.

In addition, interviewees mentioned the role of the media: the fact that cybercrime is sometimes positively viewed upon in the media makes young people more inclined to participate.

"Young people neutralize, downplay, or exhibit signs of disinhibition when they talk about committing cybercrime"

Based on two of the five sources (interviews and the self-report study of Kerstens & Stol, 2012), information was gathered about the views young people have on committing cybercrime in a broad and narrow sense. We observed three recurring aspects. Firstly, young people make use of neutralization techniques when they talk about cybercrime: e.g. "everybody does it" or "it's normal to do so" in relation to virtual theft, or "to bring malpractices to the forefront" as a reason for hacking. Secondly, young people downplay the criminal aspects of cybercrime: they think or do not know that something is punishable, or think that there is no police investigation taking place into this form of crime (low probability of detection). Finally, we found evidence for the role of disinhibition among young people as they go online: reactions of others on the Internet are often delayed and asynchronous, which makes young people think that their criminal actions online do not have any harmful effects. In addition, the interviews revealed that young people often take on another name online, which sets the stage for experiencing dissociation: they do not ascribe the criminal actions to themselves anymore, they perceive it as a game (see also Suler, 2004).

"Risks associated with the digital behavior of young people: disinhibition, sexual behavior and the emergence of criminal services on the Internet"

With the advent of the Internet it seems to have become easier to commit crime. In the introduction a number of aspects are mentioned which enable offenders to ignore or put a gloss on their behavior and its consequences: neutralization, playing down, disinhibition, and dissociation (see also Suler, 2004). In line with this, the self-report studies found that statements like "everybody does it" or "it is part of the game" are often recorded when young offenders are asked about their motives, and the experts in the interviews indicated that young offenders are often surprised when they are arrested for cybercrime and claim to have had no bad intentions. As explained before, the degree to which one feels disinhibited and easy to disclose personal information online is robust predictor of multiple forms of cybercrime. This strongly suggests that young people experience antisocial and criminal actions online quite differently than similar actions offline. Noteworthy in this respect is the fact that young people are not aware that virtual theft is punishable (Jansen, 2012). Taking all this in consideration, it seems that the line between legal and illegal behavior online is more fuzzy and unclear than between legal and illegal behavior offline. In this sense, the behavior of young people online has a clear risk, despite the fact that the involvement of young people in cybercrime to date can be called small.

A second risk concerns the way in which sexual activities of young people online are labeled. Leukfeldt and colleagues (2010) found that nearly one-tenth of the suspects of child pornography in their study were younger than 18 years; they suggested that on the one hand this could be due to technical resources that facilitate criminal conduct, which increases the prevalence of this cybercrime among the youth. On the other hand, it could also be a new expression of an old phenomenon, namely that young people tend to (as they always do) experiment with their sexuality. The question this raises is how the police and judicial authorities should deal with this. If it actually is a new expression of normal behavior, should these authorities then ignore many such cases? Or should they continue to consider this as a criminal offense and prosecute the offenders?

One of the interviewees in the OM pointed out that there is a change in policy at this point. Offenders who were spreading sexual images of juvenile victims to others were initially prosecuted and labeled as "creating and distributing of child pornography." That proved to have very serious consequences for the juvenile offenders involved, as they were regarded as a perpetrator of a sexual offense after conviction. Therefore, they proceeded to distinguish between severe cases, in which for example coercion has taken place, and milder cases in which all actions were voluntary. This latter category is now treated as slander, a different offense with far less serious consequences for the young people involved.

The findings with regard to the production and dissemination of sexual imagery in this study differ slightly from those of Leukfeldt and colleagues. As far as concrete data were available, it seemed to point in the direction of a much smaller number of young offenders involved in this type of cybercrime. This appears to nuance somewhat the possibility that Leukfeldt and colleagues suggested that this cyber offense might be a form of experimentation among the youth. One the other hand, it must be considered that socially desirable responding may have played a role in the self-reported answers (perhaps in an enhanced degree with this topic), leading possibly to underreporting of this particular behavior.

Finally, as a third risk, one of the interviewees working at the Prosecution Office expects to see a rise in cybercrime in the narrow sense among young people. The "criminal services industry" and the ICT knowledge among young people will continue to increase and it will be possible to make a lot of money with committing cybercrime. Eventually, this will lead to the growth of "economically driven" crime in the narrow sense. He also indicated that criminal syndicates in the offline world continue to develop themselves online, as can be seen in the online trade in drugs and arms. For their online activities, there is a need for people with ICT skills, and therefore cybercriminals may also approach young people. The acquisition of status and respect is an important motive for many young people to start (and continue) hacking for example, and they will very much like to share their achievements with others on web fora. This makes it relatively easy for cybercriminals to get into contact with young people.