Marleen Weulen Kranenbarg

Cyber-offenders versus traditional offenders

An empirical comparison

English summary

Cyber-offenders versus traditional offenders: An empirical comparison

The main goal of this dissertation was to empirically compare cyber-offenders with traditional offenders on four domains in criminology: offending over the life-course, personal and situational risk factors for offending and victimisation, similarity in deviance in the social network, and motivations related to different offence clusters. The focus was on new forms of crime that target IT and in which IT is key in the commission of the crime, so-called cyber-dependent crimes, like malicious hacking, web defacement, illegal control over IT-systems, malware use, and so on. These crimes provide a unique test case for traditional criminological explanations for offending, as these did not exist prior to the rise in the use of IT-systems. The anonymous digital context in which these crimes take place may have changed, for example, the situations in which opportunities for committing crime occur, the skills and personality characteristics that are needed to commit these crimes, the perceptions of the consequences of offending, and the interpersonal dynamics between offenders and victims.

Results

Offending over the life-course

In Chapter 2, a longitudinal dataset of registration data for the period 2000-2012 was used to study cyber-offending and traditional offending over the life-course. The results seem to indicate that social control of others can reduce the likelihood of cyber-offending. Nevertheless, some traditionally protective life circumstances can increase opportunities for cyber-offending and apparently the control of others in these situations cannot prevent a person from using those opportunities to commit cybercrime.

For personal life circumstances it was found that living with a partner or with a partner and a child reduces the likelihood of cyber-offending, and living as a single parent increases the likelihood of offending, in comparison to living alone. These estimates were in the same direction and even stronger for cybercrime compared to traditional crime. With respect to professional life circumstances, there was no statistically significant effect of employment or enrolment in education on cyber-offending, while these life circumstances did reduce traditional offending statistically significantly. Within the complete offender population of this study, general employment reduced the likelihood of cyber-offending, but employment

in the IT-sector and being enrolled in education increased the likelihood of cyber-offending (not statistically significant).

Risk factors for offending, victimisation, and victimisation-offending

Based on the cross-sectional dataset collected for this dissertation, Chapter 3 compared patterns in personal and situational risk factors for separate groups of offenders-only, victims-only and victim-offenders, between cybercrime and traditional crime. The results indicated the existence of a victim-offender overlap for cybercrime. For both cybercrime and traditional crime, victim-offenders had more risk factors. Differences between the two types of crime were mostly found in situational risk factors that seem to be the result of the different context in which these crimes take place. Online activities are more important for cybercrime, while offline activities are more important for traditional crime.

For cybercrime, offenders-only committed the relatively more technically sophisticated crimes compared to victim-offenders. This was also reflected in the risk factors for offenders-only, as the likelihood of offending-only was higher if a person had more IT-skills, did not have a statistically significantly low self-control, and had online activities in which they could increase their criminal IT-skills. For victim-offenders, on the other hand, IT-skills also increased the likelihood of victimisation-offending, but less so compared to offenders-only. In addition, low self-control increased the likelihood of victimisation-offending. Lastly, more general online routine activities, in which both opportunities for offending and risks for victimisation could emerge, were related to victimisation-offending.

Similarity in deviance of social network members

Based on ego-centred network data from the cross-sectional survey dataset collected for this dissertation, Chapter 4 compared the relation between deviance of an individual and deviance of a social network member between cybercrime and traditional crime. A statistically significant similarity in deviance was found for cybercrime, but the comparison with traditional crime indicated that this similarity was much weaker for cybercrime.

Subsequently, this chapter indicated that both for cybercrime and traditional crime the relation is stronger for daily-contacted network members of the same gender. However, for cybercrime the relation is strongest for older social network members, while for traditional crime the relation is strongest for same-aged contacts. This indicates that older role models may be relatively more important for cybercrime compared to traditional crime.

Clusters of offences and related motivations

Chapter 5 used the self-reported offending questions from the cross-sectional dataset to examine which clusters of crime could be identified and to what extent cyber-offenders could be distinguished from traditional offenders. The analyses indicated that cyber-dependent crime is seldom committed by offenders who also commit traditional crimes. The cybercrimes that were often committed by the same offender appeared to be part of the same modus operandi or to be related because they require the same skill set and context.

In addition, self-reported motivations were used to examine which motivations offenders provide for the different clusters of offending and to what extent the clusters can be distinguished from the others by these motivations. The cyber-offenders in this sample almost never indicated a financial motivation. Intrinsic motivations, like curiosity and learning from committing crimes, were most important for all cybercrime clusters. Extrinsic motivations were less important for cybercrime compared to traditional crime. However, some differences between the cybercrimes could be observed for extrinsic motivations, as hacking and internet related crimes were more often committed to put things straight or deliver a message, and internet related crimes were also more often committed out of revenge, anger or to bully someone. Impressing others or trying to gain power was rarely indicated as a motivation for cyber-offending.

Limitations

The samples in this dissertation were drawn from police and prosecutor's data. For Chapter 2, this means that it is unknown if a person was actually guilty of committing a crime and it is unknown to what extent this person also committed crimes in the years he or she was not caught by the police. For Chapter 3 to 5, this means that the analyses indicated which present-day risk factors, social contacts and motivations were related to present-day self-reported offending of people who had been caught by the police for committing a crime in the past, prior to the twelve-month period of the self-report questions. In addition, because of the dark number in police or prosecutor's data, these are selective samples. The results only reflect the people who have been caught for committing a crime.

For Chapter 2 the nature of the data limited the depth of the variables under study. For example, registration data cannot inform us about the strength of social bonds and people's actual daily activities. The data used in Chapter 3 to 5 provided more

in-depth measures, but the cross-sectional nature of the data limited the ability to draw strong causal conclusions from the analyses. Lastly, the data used are based on Dutch adults. It is unknown to what extent the results also apply to juveniles and adolescents or offenders from other countries.

Future research

Replication in future research in different and larger samples, preferably with in-depth longitudinal data, is necessary. In-depth longitudinal research is necessary to (1) find the exact causal processes and life circumstances that lead to committing cybercrime or desistence from committing cybercrime, (2) identify processes of selection and influence in online and offline social networks for cybercrime, and (3) to examine a possibly causal relationship between offending and victimisation. In order to be able to use interventions that are based on explanations for traditional crime, it is necessary to keep studying the differences between cyber-offenders and traditional offenders.

Future research could examine to what extent selection and influence processes can be found in, for example, online forums and gaming communities. That research could also shed light on the extent to which these online social contacts and online interactions are comparable to traditional social contacts and offline interactions. In addition, longitudinal research on social networks and cybercrime should use a method in which all network members report on their own deviant behaviour. This will enhance our knowledge on (1) selection and influence processes, (2) the discrepancy between perceived and actual cyber-deviance of social contacts, (3) the extent to which actual and perceived deviance of social contacts differently influences cyber-offending, and (4) to what extent the invisibility of cyber-deviance results in a larger discrepancy for cybercrime compared to traditional crime.

In-depth qualitative interviews could provide us with more detailed information on, for example, the role of older social network members or the strategy that offenders use if they commit a cybercrime and if they actively seek opportunities for cyber-offending or if they simply come across these opportunities by chance during their daily activities. Future research could also focus on the role of IT-skills. For example, differences in the level of IT-skills needed to commit different types of cyber-dependent crime and in longitudinal research how people acquire IT-skills and knowledge on how to use those skills in an illegal manner over time.

Practical implications

It should be noted, that none of the prevention and intervention strategies discussed below have been evaluated empirically for cybercrime and recommendations are based on a limited number of empirical studies. Therefore, authorities that are responsible for designing and executing prevention and intervention programs, are advised to carefully design and implement evaluation studies of the programs they design for cybercrime. When using interventions designed for traditional offenders, empirically identified differences and similarities between cyber-offenders and traditional offenders should be kept in mind. It is not advisable to base the application of traditional interventions to cybercrime purely on hypothetical similarities.

Based on the comparisons in this dissertation it is to be expected that interventions for cybercrime may benefit from stimulating offenders to satisfy their IT-related curiosity in legitimate ways. One way of doing that may be to help them find employment in which they could use their skills. It is, however, important that cyber-offenders are offered ethical guidance in their path to a legitimate profession and both strong formal and informal social control should be established in their professional life. Another promising way of helping offenders to move to responsible use of IT is by assigning them to a mentor.

In interventions it could be useful that offenders who commit the more technical types of crime may behave more rational than other offenders and they may be able to assess the different ways in which they could act responsibly after they discover a vulnerability. Additionally, interventions that increase the perceived consequences for the offender and his or her victim may be helpful, for example with so-called 'cease and desist visits' or situational crime prevention.

Conclusion

The empirical research conducted on the four domains in this dissertation, indicated that correlates of cyber-offending are to some extent similar to correlates of traditional offending. Nevertheless, important differences occur in each domain, which seems to be the result of the different context in which cybercrime takes place. These differences should be kept in mind when applying explanations for traditional offending to cyber-offending. Predictions and measures based on those explanations should be adjusted to the digital domain and the strength of these predictors should be empirically compared between cybercrime and traditional crime.