Summary

Nature and magnitude of cybercrime victimization and offending in the Netherlands'

Cybercrime is a serious issue in the Netherlands—estimations suggest that hundreds of thousands become victims of cybercriminals on a yearly basis. Hence, cybercrime is a hot topic for law enforcement and in politics. Two forms of cybercrime are distinguished. Firstly, cyber-dependent crime, in which both modus operandi and target concern information and communication technology (ICT). Examples for this first type of cybercrime are hacking and ransomware. Secondly, cyber-enabled crime, in which the modus operandi concerns ICT, but the target does not. Examples for this second type of crime are death threats via social media and online purchase and sales fraud (e.g., via Amazon).

Information on cybercrime victimization and offending in the Netherlands is available through self-report measures of victimization and offending, and registrations of law enforcement and private parties. In the current report this information is collected, clustered and presented in a coherent manner, thus providing an overview of the nature and magnitude of cybercrime victimization and offending in the Netherlands. The report concerns cybercrime from 2008 and forward.

This report contains answers to three research questions:

1 How is the nature of cybercrime victimization and offending conceptualized?
2 How are cybercrime victimization and offending operationalized?
3 What is the magnitude of cybercrime victimization and offending?

Conceptualization addresses what (experienced) behaviours and offenses are cybercrime, whereas operationalization concerns how these concepts are measured. Furthermore, the current report focusses on victimization of and offending by natural persons. Cybercrime exclusively between legal and/or state entities are beyond the primary scope. Victimization includes victimhood as experienced by individuals, and police reports of victimhood. Offending includes law enforcement registrations of suspects, offenders and crimes, as well as self-reported offending. Cybercrime is relevant when the offender and/or victim are Dutch. Moreover, cybercrime combated by Dutch law enforcement is relevant, even when there is not necessarily a Dutch offender or victim. The nature of cybercrime victimization and offending covers type, seriousness and impact, whereas magnitude concerns measures, such as percentage prevalence of victimhood or number of offenders and crimes.

This report is the result of a multi-method and multi-source approach using a systematic literature search, traditional empirical exploration of (registration) sources, and innovative methods applied to online platforms (i.e., social media and dark web forums).

Victimization

Cybercrime victimization in the Netherlands is mostly measured via self-report and police reports. The magnitude of victimization differs per type of offense, consulted source and population of interest.

8-15% of Dutch citizens victim of cybercrime, trends differ per source—relatively stable or decline

According to the Netherlands' Safety Monitor, the percentage of Dutch aged 15 years and older victimized by cybercrime declines from 12% to 11% in 2012-2017. In 2019, this percentage grows to 13%. In another study, the LISS-panel, the percentage of victimhood is initially 15% in 2010, which declines to 8% by 2018. Although both sources concern the same population, differences can occur through different methods and item questions. For instance, the Safety Monitor uses a new representative sample for each measurement, while the LISS-panel uses panel data (supplied with new respondents in case of attrition). In addition, the LISS-panel addresses computer virus infections, a steeply declining form of cybercrime victimization, whereas the Safety Monitor does not.

Cybercrime constitutes minority of police reports, though not negligible in absolute terms

Due to the limited amount of cybercrime victims reporting to the police (7-8%), only a fraction of all cybercrime victimization exists in police records. Textmining research on police reports from 2016 suggest that out 3.9 million registrations 4.000-25.000 of those concern cyber-dependent crimes, and 132.000-293.000 concern cyber-enabled crimes. Even though these numbers constitute a minority of all registrations, in absolute terms they are not negligible.

Malware most common form of cybercrime victimization

The prevalence of victimization differs per type of cybercrime and consulted source. Computer virus infections (i.e., malware) affect 2-62% of Dutch citizens, based on self-report measures. The large range is (likely) due to the inclusion or exclusion of explicit harm. When harm or damage is not included in the item description, prevalence rates are higher. Furthermore, 1-16% of Dutch citizens report hacking victimization, and 0-16% report some form of online fraud victimization. Moreover, 0-9% experience cyber harassment victimization, such as threats, bullying and distribution of private sexual images without consent. In police reports from 2016 online threats are the most common form of cybercrime, whereas hacking, ransomware and DDoS-attacks are much less prevalent. Lastly, reporting victimization to the police differs per type of cybercrime—online fraud shows higher report rates (12-22%) than hacking (2-3%).

Online threats against Dutch mayors largely hidden on social media

With social media and other online platforms, the distance between citizen and government has shrunk considerably, allowing for direct communication between the two—including harassment.
On basis of an empirical study on traditional and social media, there is little found on why and how often Dutch mayors receive threats via Twitter and other online platforms. Exploratory research does suggest three recurring themes of threats:

organized crime and motorcycle gangs, dissatisfaction from individual citizens regarding governance, and other threats.

Offending

Cybercrime offending in the Netherlands is largely studied through law enforcement registrations and self-report measures. As with victimization, prevalence of offending differs per type of cybercrime and consulted source.

Limited information on cybercrime in law enforcement registrations

Only a few sources provide information on cybercrime offending in the Netherlands, often concerning estimates of number of offenders, criminal cases, registered crimes or investigations. Moreover, information on specific types of cybercrime is scarce, as law enforcement registration is mostly limited to computer trespassing. In addition, cyber-enabled crime can be registered under its traditional counterpart (e.g., online threats as "regular" threats), making them hard(er) to recognize.

Law enforcement shows limited, though increasing, numbers of cyber-dependent crime offending

Registrations by law enforcement suggest only a limited amount of cyber-dependent crime offending, though these numbers do increase over time. For instance, the number of suspects of cyber-dependent crime is approximately 70 in 2008, and increases to approximately 430 in 2019. Cyber-enabled crime, however, exhibits a decreasing trend. For example, the number of criminal cases handled by the Public Prosecution Services (PPS) goes from approximately 540 in 2008 to approximately 360 in 2018. Overall, cybercrime is less than 1% of all crime handled by law enforcement in terms of offenders and cases.

Cybercrime in criminal justice chain more serious through the years

Indicators of criminal severity suggest that cybercrime in the criminal justice chain is becoming more serious through the years—over time, judges punish cybercrime more severely and the maximum applicable punishment increases as well. For instance, in 2008-2014 the amount of cyber-dependent crime cases resulting in a mandatory prison sentence is at most approximately 30%, whereas in 2015-2018 these percentages range 34-47%. For cyber-enabled crime, these percentages go from 47% in 2008 to 83% in 2018.

Gap between self-reported cybercrime offending among youths and official registrations

Information on self-reported cybercrime offending is limited to the Dutch youth population. The prevalence of cyber-dependent offending among 10 through 22 years olds is, depending on age category, 7-22% in 2015. For cyber-enabled crime, the prevalence ranges 4-13%. Hence, a gap between tens of thousands self-reported juvenile cyber offenders and tens to hundreds of yearly officially registered offenders exists.

Cybercrime-as-a-service on the rise

Cybercrime-as-a-service (CAAS) concerns goods and services provided by cybercriminals to other criminals, who do not have the means to commit cybercrime by themselves. A textmining study on the supply of CAAS on dark web forums (e.g., AlphaBay) suggests that this phenomenon increases over time—during 2011-2017 both the number of advertisements and consumer responses regarding CAAS is up. However, due to methodological limitations, it is hard to interpret what the magnitude of CAAS on dark web forums really is.

Answering the research questions

1 How is the nature of cybercrime victimization and offending conceptualized?
2 How are cybercrime victimization and offending operationalized?

The consulted sources conceptualize and operationalize the nature of cybercrime victimization and offending in the Netherlands in two ways. Firstly, short descriptions of criminal behaviour in questionnaire items, and secondly, derivations from law enforcement registrations, such criminal codes or offence labels (i.e., computer trespassing). Operationalization of cybercrime victimization and offending usually concerns population percentages, though other measures exist, such as absolute numbers of offenders and criminal cases.

3 What is the magnitude of cybercrime victimization and offending?

There is no single answer to this question, as the ranges and units of measurement differ largely per type of offense, consulted source, and target population. For instance, in 2015, respectively, 7-22% and 4-13% of Dutch youths report to have committed a cyber-dependent or cyber-enabled offense. Meanwhile, cybercrime suspects in that same year number only between approximately 120 and 200 individuals. Moreover, youths compared to full population samples report more cybercrime victimization, cyber-dependent crime goes up, whereas cyber-enabled crime goes down, and malware infections are much more prevalent than online fraud. Hence, providing a single answer to the question of what the magnitude of cybercrime victimization and offending in the Netherlands is is (currently) not possible.

Conclusion and recommendations

For now, there is no uniformity in the conceptualization and operationalization of cybercrime. That said, it might be undesirable to obtain uniformity in the short run, as cybercriminology—as well as cybercrime itself—is still developing. Locking in too early on one concept or operationalization might hinder acquisition of knowledge later on.

It is clear that cybercrime is a serious issue in the Netherlands, with a significant amount of Dutch citizens becoming a victim every year. However, the belief that cybercrime is becoming an ever bigger problem is not necessarily supported by the data, as longitudinal sources on victimization suggest relative stability or a modest decline. Some specific cybercrimes, such as online purchase and sales fraud, do

show an increase over time. Also, the number of cyber-dependent offenders in the criminal justice chain increases as well.

Furthermore, cybercrime remains a serious issue, when compared to traditional crime. Although victimization of traditional crime is more prevalent than cybercrime, traditional victimization does show a steep decline, whereas cybercrime victimization might be stabilising.

This report contains two policy recommendations. Firstly, invest in the improvement and continued development of instruments to measure and register cybercrime victimization and offending. This does not only include how to measure, but also what to measure. Adequately reacting to novel cybercriminal developments requires policy makers to collaborate with institutions and experts that are able to detect novel forms of cybercrime in its early stages. Also, do not focus too narrowly on only novel forms of cybercrime, which may only briefly stay relevant. Within registration systems of law enforcement, development should not solely focus on expanding registration possibilities (e.g., more labels for different forms of cybercrime), but also on utilizing innovative methods on existing data. After all, law enforcement registration already does contain large amounts of detailed data (e.g., written police reports).

Secondly, keep investing in cybercrime expertise in the criminal justice chain. This report shows that cybercrime victimization is much more prevalent than criminal justice statistics suggest. This gap exists in part due to circumstances that the criminal justice chain cannot control, such as victim willingness to report. However, this gap is also in part due to controllable circumstances, such as available cybercrime expertise. Lack of cybercrime expertise in law enforcement might result in inadequate handling of victims' police reports, resulting in reports not progressing through the criminal justice chain, or being unrecognizable as cybercrime when progressing through the chain. Moreover, limited expertise might result in the misappraisal of severity, which could hinder detection and prosecution of cybercrime. Investing in cybercrime expertise in law enforcement will likely contribute to effective means of combating cybercrime in the Netherlands.