# Summary


## Cybercrime in numbers
### Exploring the possibilities to include cybercrime in the National Security Indices

This study examines whether and how cybercrime can be included in the National Security Indices. Cybercrime is generally used as an overarching term to describe offences where ICTs play a prominent role. In line with previous studies, we make a distinction between offences where ICTs are used as a mean to commit crimes (referred to as 'digitized crime') and offences where ICTs are the target of the criminal activity (referred to as 'cybercrime').

In our explorative study, we show that it is currently impossible to distinguish digitized crime from other crimes in the National Security Indices. Although digitized offences are already included in the crime index, they are not recorded as a separate category. The crime index is predominantly based on police crime records. Through use of ICT-related terms, text mining methods might be useful to further analyze police crime records and to make a distinction between offences with a digital component and offences without a digital component. However, more research is needed on this issue. We suggest that a pilot study be undertaken to explore whether and which ICT-related terms allow a reliable measurement of digitized crime. A drawback of applying text mining is that it causes some major changes in the methods of the National Security Indices. By applying it we cannot rely on open access data anymore, but need to use police data that are not openly available to the public. Moreover, it may drastically change the crime trends of the security indices.

Furthermore, we show that the inclusion of cybercrime in the security indices is not feasible in the short term. Because police statistics give a limited view of cybercrime, these figures seem less suited to examine cybercrime. It is possible to examine changes in cybercrime by focusing on its forms, such as hacking, botnets, Denial-of-service attacks, malware and defacing. These forms can be measured by using (and combining) data from law enforcement officials, crime victimization surveys, victim reporting initiatives (e.g. a website or hotline), and developers of cyber security software (e.g. anti-virus software and firewalls). First, however, a list should be made of data sources that provide a reliable picture of the forms of cybercrime. Still much is unknown about this matter. It is recommended to cooperate with other Dutch organizations that have an interest in drawing up such a list. These organizations include the National Cyber Security Centre, Team High Tech Crime of the police, and Statistics Netherlands. Moreover, when examining different forms of cybercrime, one needs to take into account the level of overlap between the forms of cybercrime, and between these forms and traditional crimes. Neglecting this overlap would lead to double counting of offenses and therefore to an overestimation of the crime problem.

This study shows that there are opportunities to include digitized crime and cybercrime in the National Security Indices. These opportunities however lead to major changes in the methods used, and require data that are not openly accessible. Because there is a general shift from offline to online crime, we believe that trends in cybercrime should be analyzed alongside trends in more traditional crimes. Yet, as

shown in this study, there are still questions about the reliability of measuring cybercrime left unanswered.

Within the WODC, there are now taken several initiatives to provide insight into how to measure cybercrime. Currently, we are drawing up a research program to better understand cybercrime among young people. There is also a project planned to describe (developments in) the various forms of cybercrime on the basis of all available data sources. The aim in this project is not only to use traditional data sources such as police records and victim surveys, but also to use 'new' data from, for example, (Internet) reporting centers and security companies. On the basis of the results of these projects can be examined how the NVI can be expanded with the development of 'the' cybercrime.