Summaries

Justitiële verkenningen (Judicial explorations) is published six times a year by the Research and Documentation Centre of the Dutch Ministry of Security and Justice in cooperation with Boom juridisch. Each issue focuses on a central theme related to judicial policy. The section Summaries contains abstracts of the internationally most relevant articles of each issue. The central theme of this issue (no. 5, 2018) is *The digitalization of organized crime.*

The effect of the internet on the structure of organized cybercrime. Findings from an international empirical study

Geralda Odinot, Christianne de Poot and Maite Verhoeven

Worldwide, the digitalization of society is proceeding rapidly and this brings new forms of crime. The threats arising from different types of cybercrime are real and constantly evolving, as the internet with its anonymity and borderless reach, provides new opportunities for criminal activities. This article describes some results from an international empirical study aimed to gather more insight on the link between cybercrime and organized crime as well as on the question whether cybercrime is organized. It shows how cybercriminals cooperate with each other and what this organization structure looks like.

Criminal money flows and IT. On innovative modi operandi, old certainties, and new bottlenecks

Edwin Kruisbergen, Rutger Leukfeldt, Edward Kleemans and Robby Roks

In this article we analyze how organized crime offenders use IT to handle their money flows. How and to what extent do offenders use IT-facilitated possibilities, such as bitcoin, to launder their money? The empirical data consist of thirty large-scale police investigations. These thirty cases are part of the Organized Crime Monitor, an ongoing research project into the nature of organized crime in the Netherlands. One of the most striking findings is the fact that cash is still king – even for online drug dealers who get paid in digital currencies.

Organized child pornography networks on the Dark Web

Madeleine van der Bruggen

The emergence of Dark Web child pornography forums and their availability to large offender communities has enabled a professional form of child pornography distribution as well as an increased exchange of criminal and social capital. Offenders have access to a new platform in which strong ties and long-lasting relationships with co-offenders are formed. Moreover they could be classified as organized crime, because child pornography Dark Web forums are characterized by a hierarchical order, a clear role division and illegal power structures that regulate the illegal activities. The implications from a law enforcement as well as from scientific perspective are discussed.

The non-human (f)actor in cybercrime. Cybercriminal networks seen from a cyborg crime perspective

Wytske van der Wagen and Frank Bernaards

Botnets, banking malware and other high-tech crimes are increasingly analyzed by criminological scholars. Their distributed and automated nature poses however various theoretical challenges. This article presents an alternative approach, denoted as the 'cyborg crime' perspective, which adopts a more hybrid view of networks and also assigns an active role to technology. The value of this approach is demonstrated by reflecting on findings from earlier empirical work that analyzes conversations between cybercriminals involved in botnets and related activities. The research shows that technological nodes can take an important position in the organizational structure of cybercriminal networks and do not merely have a functional role. Viewing technology as an actor within a criminal network might offer new criminological insights in both the composition of these networks and how to disrupt them.

Out of the shadow. Opportunities for researchers in studying dark markets

Thijmen Verburgh, Eefje Smits and Rolf van Wegberg

In this article the authors present the lessons learned from previous research efforts into dark markets. First the important features of dark markets are discussed, i.e. anonymity and trust, as well as the question how data on dark markets can be collected. Next, the authors illustrate

how this data can be used to study the phenomenon of dark markets itself as well as the impact of police interventions on dark markets.

Befriending a criminal suspect on Facebook. Undercover powers on the Internet

Jan-Jaap Oerlemans

This article investigates which online undercover investigative methods are applied in practice and how they fit in the Dutch legal framework. In particular, the three special investigative powers of a pseudo purchase, systematic information gathering and infiltration are examined. Investigative powers cannot be applied unilaterally (across state borders). When law enforcement officials cannot reasonably determine the location of the suspect, the online unilateral application of undercover investigative powers is allowed. However, there is still a risk that diplomatic tensions arise with the involved state. States should agree in treaties under which circumstances cross-border online undercover operations are allowed.

New investigative powers and the right to privacy. An analysis of the Dutch Cybercrime III Act

Bart Custers

In 2018 the Dutch parliament accepted new cybercrime legislation (the Cybercrime III Act) that creates several new online criminal offences and gives law enforcement agencies new investigative powers on the Internet. This article describes the background of Dutch cybercrime legislation and the contents of the Cybercrime III Act. The newly introduced cybercrimes are discussed as well as the new investigative competences. Particularly the legitimacy and the necessity of the investigative power of the police to hack computer systems of suspects may significantly interfere with the right to privacy.