Summaries

The dynamics of cybercrime law in Europe and the Netherlands

B.J. Koops

Because of the special characteristics of the Internet, cybercrime inherently crosses national borders and has fewer natural barriers than classic cross-border crime. This triggers the question whether criminal law with its traditional national focus is able to combat cybercrime. Can legislatures respond to technological change with sufficient speed in an internationally aligned approach? This article tries to answer this question by mapping the dynamics of cybercrime law, focusing particularly on the interplay between European and Dutch legislative initiatives. It shows that the dynamics consist of a European framework of minimum standards on major issues, with much room for national legislatures to interpret the standards and to add initiatives of their own where the European framework remains silent. Although this has worked well so far, if cybercrime continues to transform into large-scale organised crime, a step-change in the dynamics towards more steering European approaches may be necessary.

Cybercrime and police; state of affairs in the Netherlands in 2012

W.Ph. Stol, E.R. Leukfeldt and H. Klap

In 2004 the main problem of the Dutch police concerning cybercrime was a lack of knowledge, for example about how to act in a digital world, about the character of cybercrime and about the effectiveness of measures. The main question in this article is if this situation has changed, and if so, how. Although the legislator has given the police special powers to fight crime in a digital world, the police still struggle with questions about what exactly are the powers they have. Although the police have invested in pilot projects and in the recruitment of digital experts, knowledge about 'policing a digital society' is not yet common in the police organisation – which is a shortcoming since 'digital is normal' in the lives of the common people. Although the police established digital aspects in police training, digital is not yet a common feature in police education. In sum, although the police in various ways pay attention

to digital aspects of policing, digital is not yet a regular part of the police organisation, police training and/or everyday police practice.

A safe cyberspace requires new thinking

R. Prins

This article describes the main security threats in cyberspace as well as the various types of actors behind these threats. The author discusses the reaction of existing and new state security agencies towards the new cyber threats. After analyzing the main obstacles in tracing cybercriminals he gives some recommendations for a more effective strategy against cybercrime.

Cyberwar? What war? More specific: what law?

A.R. Lodder and L.J.M. Boer

This article presents an overview of cyberwar from an international law perspective, in particular from the framework of the laws of war. It discusses some of the difficulties in applying these laws to cyberattacks, further complicated by the characteristics of the Internet. A distinction is made between cyberwar, -crime, -espionage and -terrorism, and the different fields of law that apply to these distinct 'cyberevents'. Next to discussing several historic cyberattacks, the question is raised whether cyberwar is merely a hype or whether we should be taking this threat seriously. Rather than answering this question, the authors feel that the actual threat posed by 'cyber' is less important than the political and military prominence gained by this phenomenon in these past few years. The authors conclude by stating that a lot of work has yet to be done to address the issues raised by the occurrence of cyberwar.

The leaking of secrets in cyberspace

J.H. Maat

When it comes to cybersecurity usually little attention is payed to internal threats, i.e. from within organizations themselves which may – intentional or not – breach the confidentiality of digitally stored information. When a secret reaches the media, it often generates a lot of public attention. Not only because of the content or the curiosity-value of the secret itself, but also because of the – sometimes shockingly simple – way the secret has been leaked. This kind of security breach in particular gives rise to negative publicity, which not only impacts the organization which it concerns, but also

reflects badly on other peers in the sector, especially in the case of breaches that are government-related. In this article, the author explores the issues of the leaking of secrets in 'cyberspace' by using several examples – such as the WikiLeaks affair – to illustrate the effects of ICT developments in the last two to three decades on vulnerabilities in information security. The article then focuses on new developments in 'Alternative Workplace Strategies' and the related use of new technologies in relation to the vulnerabilities in information security. Organizations can reduce the threats by facilitating their employees with smart solutions which are also results of new technologies.

Sense and nonsense of a download-ban; actual developments and insights in digital piracy

H.B.M. Leeuw

In this contribution, the author explores some of the issues that are currently dominant in the debate revolving illegal downloading (also known as digital piracy). Four specific issues are addressed. Firstly, the legal status of downloading is discussed, followed by a brief analysis of a debate currently being held within the Dutch parliament dealing with this issue. Of particular interest is the proposed 'download-ban' which is intended to decrease digital piracy and increase legitimate sales. However, as will be demonstrated, this proposed ban is not without criticisms. Following this analysis, the question is raised what is actually empirically known about the impact of illegal downloading on the involved industries, and whether proposed measures such as a 'download-ban' can have the desired impact. Finally, the role of copyrights in the digital environment is explored.

Identity fraud and victimhood; a literature research into nature, size, risk factors and aftermath

J. van Wilsem

Identity fraud involves the theft of another person's identity information (e.g. bank account number and password), mostly for purposes of financial gain to the offender. The literature review summarizes main results from international and Dutch research with respect to the nature, size, risk factors and aftermath of identity fraud as well as the consequences for its victims. Though scientific research on these phenomena is taking place more and more, much work yet remains to be done. This review ends with suggestions for future research on identity fraud.

Internet and fraud; a comparison between internet swindlers and classic swindlers

E.R. Leukfeldt and W.Ph. Stol

Based on different criminological theories in combination with the unique characteristics of the Internet, it is assumed that there are significant differences between cyber criminals and traditional criminals. This article compares the characteristics of fraudsters who use the Internet to execute their scams (e-fraudsters) and fraudsters who do not use the Internet (classic fraudsters). The personal characteristics, social economical background and criminal careers are compared. The main conclusion is that e-fraudsters are not ‘new’ criminals that only commit crimes because of the perceived benefits of the Internet. But the use of the Internet does make the perceived consequences of committing a fraud offense less severe, so offenders who use the Internet will commit fraud offenses earlier in life. Internet provides the opportunity for fraudsters to commit frauds at a younger age.