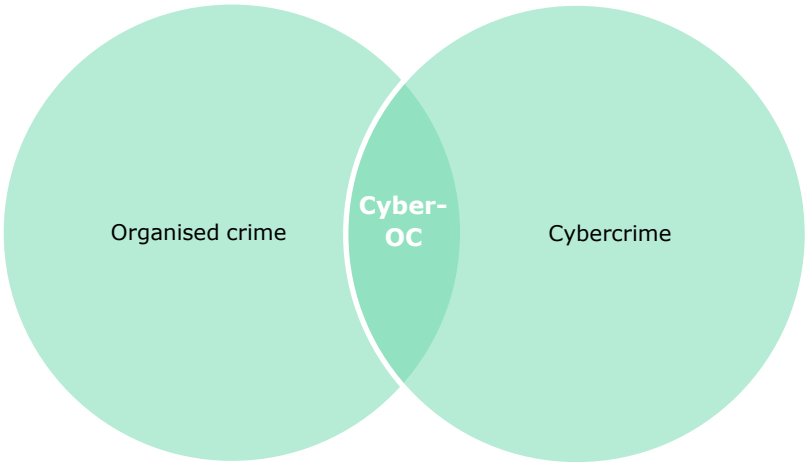
Summary

Aims of the study

The growth of cybercrime and increased vulnerability to become the victim of a cyber offence concern the public, law enforcement and policy makers. However, not much information is available yet about the nature and organization of those crimes. Our research explored how criminal groups involved in criminal activities on, via and against the Internet operate by focusing on their modus operandi, the organisational structures of the crime groups, and the profiles of the offenders involved in these groups. We also addressed the ways in which law enforcement agencies investigate these forms of cybercrime and the challenges and obstacles they encounter. By 'cyber organised crime', or 'Cyber-OC' (see also Bulanova-Hristova et al., 2016) we mean the overlap between organised crime and cybercrime, in other words the links and convergence between cybercrime and organised crime.



Other aims of the study are to explore: if the Internet provides new windows of opportunity for illegal business ideas and for the identification and approaching of new targets?; and if the Internet lead to structural changes in organised crime?

Methods: police files and interviews

To find answers to our research questions, different research methods were used. An analysis is made of the police files of criminal investigations into cyber organised crime. We selected eleven cases in which the police inquiries have been completed. The suspects in our selected cases were active in a number of different forms of cybercrime: distributing malware, hacking, running botnets, phishing, abusing the banking system, (digital) money laundering and illegal online trading. Most of the cases have already been tried and judged (ten), and one is still before the courts. The cases were initiated between 2009 and 2014. The eleven files examined, describe a total of 107 suspects.
Next to the police files, we interviewed twelve law enforcement officials to gather information. These officials are working as public prosecutors, police officers of investigating teams, and representatives of the Electronic Crimes Task Force and

Europol. The data for this study was originally gathered in the context of an international research project funded by the European Commission (see also Bulanova-Hristova et al., 2016).[1]

Results: traditional groups and new alliances

Among the case files analysed, we saw on the one hand, traditional crime groups engaging in cybercrime to perform their (traditional) criminal activities more efficiently or in a more sophisticated way. For example, selling drugs online, or using the Internet and encryption in their 'internal' communication. On the other hand, there are new groups developing specific cyber-related criminal activities, new crimes in fact (DDos attacks, distributing malware and ransomware). The new emerging issues and challenges related to cyber-OC we encountered in this study mainly originate from these new online activities.

New opportunities: new ideas, new targets

Next to anonymity, crime as a service and the option to use fora, this study has shown that the Internet provides for new business ideas and new targets. In this way ICT functions as a tool to increase the efficiency and economic gain of crimes. Considering the new marketing channels, this has lead to new opportunities to get in touch with targets. In the end, one could also argue that through new opportunities caused by globalisation these 'new' crimes are rather an evolution of traditional crimes.
This development makes crimes that require coordinated activities seem less complex and more accessible to larger groups of people. This leads, apart from changes in the modus operandi and changes in the target groups, to (1) new players in the field, (2) new forms of collaboration and (3) new economic structures.

1 New Facilitators

Most notable are new facilitators, consisting on the one hand of people who are technically skilled, and on the other hand of (legitimate) companies (private parties), such as hosting providers, online advertising firms, web shops, courier firms (postal companies) and telecommunication companies. We also encountered new kinds of front businesses, bitcoins exchangers and money mules who facilitate illegal activities. These facilitators in the digital world are not the same parties as we know from offline organized crime cases and offer new possibilities for law enforcement and prevention in the field of cybercrime. It could be worth to invest in prevention, detection and involvement of these parties, for example in public-private co-operations.

2 Collaboration and organisation

The ways suspects cooperate are partly comparable to other forms of organised crime. Similarities are:

- *Dynamic networks*: criminal alliances are changeable; people get involved and people drop out.
- *Based on social relationships*: in our cases family ties, friendships and exclusively online relationships all appear within collaborations.

[1] EU Project: Bulanova-Hristova et al. (Eds.) (2016). Cyber-OC - Scope and manifestations in selected EU member states (HOME/2012/ISEC/AG/4000004382).

There are also aspects of organised cybercrime that differ somewhat from other forms of organised crime:

- *Anonymity in cyberspace*: online activities can be conducted anonymously, and offline contact between 'partners in crime' is not necessary to commit online (criminal) activities. This makes cooperation less risky and changes the role of trust within criminal cooperation.
- *Crime as a service*: certain tasks can be bought online as services, which gives the organisation of cybercrime a new or different dimension. ICT-skilled people can sell their services to other online or offline active suspects. Within this 'cooperation', different individuals undertake specific activities and there is no real need for them to make contact before the task is complete.
- *Role of forums*: online cybercrime forums seem to provide a meeting place for criminals and function as communication channels. They facilitate the collaboration between suspects and lead to the formation of new collaborations between suspects active on these forums. Through this way suspects are able to build online relationships and collaborate and communicate without meeting each other offline. The channels are used for selling and sharing knowledge, software, scripts, goods, products and raw materials. The fact that online communication services mostly use encryption appears to be an important motivation to use these forums instead of more traditional communication channels.

Chain-structures and divided responsibilities

As a result of these opportunities, in contrast to more traditional organized crime groups, the newer groups emerging in the cyber field, sometimes seem to differ in their approach to a *long-term perspective* on their co-operation. Although individuals seem to have a long-term perspective regarding their own activities, the alliances involved in a particular crime are often less stable and do not always share a long-term perspective on conducting ongoing criminal activities within the same alliances. It seems to be less necessary to form a stable group, since the quality of one's contribution seems to be more important than trust between co-operating people. Due to the anonymity of online collaborations, this collaboration is less risky, and building trust is less important in these cyber-OC groups. Within these more loose networks or alliances the cooperation between suspects can take the form of a chain, linking people involved in different activities, which together constitute a criminal act. In these chain-like collaborations, suspects work together, but are responsible for only a single part of a crime. As a consequence, suspects can get involved in organised crime without knowing exactly what they are involved in. Within these chain-like structures, in a way, every suspect has power, and every suspect has a certain role, but either everyone or no one seems to be responsible for the crime as a whole. There might not even be an intended goal. This appears to be quite a new characteristic of organised crime, manifesting itself in cyber-OC cases that we did not see before and that definitely changes our concept of what organised crime entails. In such a chain structure, the different players can all act for themselves and achieve private goals. Together they accomplish an organised form of crime, using the bottom-up approach rather than being organised top-down. This way, crimes as well as crime groups seem to more or less co-incidentally arise and take on a certain form.

Because of these developments, cyber-OC can be committed either under mutual arrangements between offenders (suspects knowing each other and working together on a criminal project, relying on the division of tasks) or without any coordination in a chain environment. As a result, there is huge diversity and uncertainty, and it

may become difficult to allocate crimes to specific crime groups or criminal organisations and to predict how crimes will take shape.

3 New economic structures
New economic structures relate to the use of cryptocurrencies to transfer and launder money via the Internet. This has created new underground economic structures that are difficult to control. It would be interesting to examine to what extent rules, reporting systems and inspection bodies in the field of unusual transactions could also apply and be used for cryptocurrencies.

Criminal investigation of organised cybercrime

Anonymity online and the identification of suspects
The special cybercrime team of the Dutch Police – the National High Tech Crime Unit – has grown rapidly during the last years. This means capacity and expertise is reserved for the criminal investigation of cybercrime cases. However, the amount of possible cybercrime cases rises and the police is forced to fix priorities in detecting and investigating cases.

Special investigative powers
The wide array of sophisticated technical methods to act anonymously on the Internet, require the use of special investigative powers to reveal people's identity. These investigative powers can be applied both online and offline. The upcoming new Computer Crime Bill offers the police new investigative tools, and creates possibilities to get access to information before it is encrypted.

Information position on the Internet
To get grip on traditional organized crime groups, the Dutch police has a special unit, the Criminal Intelligence Unit (CIU). People from the CIU can work undercover with some people in a criminal group and provide information about criminal activities. This information is often used as a starting point for a criminal investigation. However, according to our interviewees, the information position within the Internet community needs attention. Several of our interviewees think that developing this in the future, would be valuable in the fight against cybercrime.

International cooperation
Since a suspect on the Internet can physically be anywhere; identifying, localising, arresting and finally convicting suspects often requires thorough international collaboration. Our interviewees are positive about the facilitating role of Europol within international cooperation. However, the success of Joint Investigation Teams appear to be heavily dependent on capacity and priorities in the collaborating countries. In police investigations that do not have the formal status of a JIT, formal requests to other jurisdictions are required for assistance or information. Due to different priorities, complicated paperwork or political difficulties, these requests are often dealt with a pace that is incompatible with the speed of the Internet. Overcoming these kinds of problems would be a real gain in investigating (organised) cybercrime.