ORGANISED PROPERTY CRIME:

winning the arms race
The goal of this paper is to shed light on several aspects of the arms race in relation to organised property crime (OPC), the prevention thereof and the challenges it will face in the future.
The goal of this paper is to shed light on several aspects of the arms race in relation to organised property crime (OPC), the prevention thereof and the challenges it will face in the future. In order to achieve this objective, we take a closer look at the key challenges posed by organised property crime and modern organised crime groups. As no crime happens in a vacuum, we need to look at the current context, an era marked by the fourth industrial revolution that impacts targets, opportunities and working methods of organised crime groups (OCGs). We highlight the importance of the design and development phase of products, such as mobile phones, safes and buildings and finish with recommendations on how to win the arms race by anticipating future threats and by setting a proactive course.

Information was assembled through a literature review and by calling upon the advice of experts during the expert meeting “Innovation and technology within the prevention of OPC” on 18 April 2019 in Brussels, organised by the EUCPN Secretariat. We would like to thank the participants for their contributions: Prof Rachel Armitage, Ms Pilar De La Torre, Prof Paul Ekblom, Mr Florian Mattinson, Mr Rob Van Dijk and Mr Paul Van Soomeren.
CONTENTS

Preface 3

01 Challenges of organised property crime 5

02 Arms race in the digital era 6
  Continuously changing world 6
  Organised property crime in a digital era 6
  Design and development 7
  Arms race 7
  Design contradictions and iatrogenic effects 7

03 Winning the arms race 9
  Anticipate future threats 9
  Set a proactive course 9

Conclusions 11

Bibliography 12

Endnotes 13
Organised property crime is a crime category characterised by two elements: it concerns crime on property and crime that is organised. Firstly, since property crimes are highly visible, they have a strong impact on feelings of insecurity. Commonly discussed forms of OPC are motor vehicle crime, domestic burglaries, burglaries on commercial premises, theft, pickpocketing and physical ATM attacks.

Secondly, the organised aspect of OPC makes it complex and makes the prevention thereof even more challenging. Depending on whether the perspective is academic, policy-related or law-enforcement-driven, there are different definitions of organised crime, with some definitions emphasising the illegal organisation (‘who’) versus others emphasising the organising of crime (‘what’). In the reality of the EU, with all its diverse Member States, a unified definition is not simple. Nevertheless, the EU definition states:

“A group of three or more persons existing over a period of time acting in concert with the aim of committing crimes for financial or material benefit.”

As the definition implies, organised crime involves multiple people who have the advantage of strength in numbers. It allows for specialisation and pooling of both labour and resources. Additionally, OCGs display increasing levels of professionalism and entrepreneurship. This is, for instance, reflected in the trend of crime-as-a-service. An OCG, or an individual, has their own skills set and area of expertise. This specialisation, combined with professionalism, has led to a crime-as-a-service industry. Consequently, OCGs have more access to developing technology than before and are able to evade preventative measures.

Besides, it is important to mention that OCGs have limited constraining conditions. They are not bound by a legal system or ethical boundaries, which is an advantage in respect of crime prevention actors who have to follow certain procedures and rules before adopting new prevention measures.

Finally, the motives that criminals have to commit crime are independent of time or other changing circumstances. The most obvious motive in the context of OPC, greed, is a motive that will remain constant in the foreseeable future and it is very likely that OPC will never cease to exist. However, property crime will adapt to the changing world. Targets will shift, modus operandi will evolve and prevention has to evolve accordingly.
Continuously changing world

We live in a continuously changing world. The acronym PESTELOMI stands for Political, Economic, Social, Technological, Environmental, Legal, Organisational, Media and Infrastructural changes. Developments in these domains have impacted both society in general and our daily lives. Moreover, they have generated new criminal opportunities that lead to more diverse crimes. Even though our society has already faced major developments, especially seen over a long period of time, we are in the middle of new developments in the domains of (information) technology, bioengineering and climate change.

Thanks to PESTELOMI changes and the ability of offenders and other actors within the crime ecosystem to adapt to these changes, new crime-related issues are continuously emerging. From a crime prevention perspective, future crime-related issues and solutions need to be anticipated.

Technological development can be seen as the primary driver for social change. In fact, it is safe to say that technologically-induced changes have drastically and progressively reshaped the routine activities of society. Some say we are currently experiencing the fourth industrial revolution. The use of water and steam characterised the first industrial revolution mechanising production; the second created mass production with the help of electric power and the third encompasses the digital revolution. The fourth industrial revolution uses a convergence between technologies that is blurring the lines between the physical, digital and biological spheres. Clearly, technology is an important factor to understand trends in crime and crime prevention.

Organised property crime in a digital era

The fourth industrial revolution provides new resources to criminals to reach their goals. They are quick to adopt new modi operandi and to find new lucrative activities. The rise of online trade in illicit goods and services has even created entirely new criminal markets. This new landscape consequently challenges the traditional definition of OCGs as mentioned above. The definition does not encompass the complexity and flexibility of modern OCGs in the digital era. This is achieved by their ability to increasingly communicate and operate anonymously and by the emergence of the crime-as-a-service model.

Furthermore, it is a challenge to separate cybercrime from traditional OPC, or other crime phenomena, such as drug trafficking or trafficking in human beings for that matter. This is because both means and targets have become more digital. Another reason for this is that cyberspace facilitates many crimes. For example, in the case of domestic burglary, online services aid OCGs by offering a social media platform that might expose residents being away from home. Additionally, the freely accessible online navigation tools are helpful to scout targeted neighbourhoods. Besides, online market places offer a relatively comfortable platform to fence stolen goods in relative anonymity. For these reasons, it makes strategical sense to include cyber-enabled crime into the efforts of anticipating future OPC threats and the development of crime prevention initiatives.
Design and development

Products, such as mobile phones, safes, buildings for commercial activities or ATMs, are often designed and developed in a way that is naive – or vulnerable to crime – to a certain extent. However, when designers consider the ways in which the product might be susceptible to crime, they can prevent crime or at least reduce the opportunities for offending. Designing out crime must be done at the start of the designing project, not added on at the end. Design and development are crucial phases in the lifetime of a product. Even though one cannot foresee all dangers, the goal of crime prevention should be high on the agenda when designing a product. Crime prevention actors and law enforcement must maximise their cooperation with the private sector as it is the driver for technological innovation and plays a pivotal role.

Overall, the concept of designing out crime is not new. In this regard, the UK makes for an interesting case with the introduction of the Crime and Disorder Act in 1998 and the Foresight Crime Panel in 1999. Unfortunately, the potential of this momentum was never fully harvested. Nevertheless, it might be useful to zoom in on the goals and recommendations out of this era, as this case might inspire others in their crime-proofing endeavours. Section 17 of the Crime and Disorder Act is an example of crime proofing through regulation. It imposes the obligation upon local authorities, police, fire services and their partnerships to consider the crime implications of every decision that they make. The Foresight Crime Panel, one of three cross-cutting panels of the Department of Trade and Industry, made some recommendations with regard to designing out crime. The recommendations were to provide funding to direct the attention of science and technology to crime reduction, to establish a national strategy for all crime related to theft and illegal use of electronic services, to extend the obligation of Section 17 of the Crime and Disorder Act to central government and businesses and finally to develop a programme that addresses crime at all stages of a product’s lifespan. This last programme should then encompass the following elements: encouraging a climate of demand or secure products amongst consumers, identifying the roles for manufacturers, retailers and consumers in developing secure products and the creation of a voluntary standards system within manufacturing which shows the criminogenic capacity of a given product.

Arms race

In the longer term, adaptations and counter adaptations eventually led to an arms race between criminals and preventers. Even after having found an effective security measure to make a product less vulnerable to crime, preventers cannot afford to rest on their laurels. An example can be found in the drop of car thefts experienced two decades ago. Apparently, professional car thieves could be stopped by designing-out-crime efforts, such as immobilisers. Recently, car thieves are catching up by managing to circumvent the security of keyless luxury cars. The problem is of such an extent that insurers insist that owners of certain keyless luxury cars revert back to more ‘old fashioned’, yet effective, security measures.

Design contradictions and iatrogenic effects

Unfortunately, there are some factors that can restrain the full use of new technologies at the prevention side, which do not affect criminals or do so to a lesser extent. These are design contradictions or trade-offs. When someone designs a product with crime prevention in mind, this person must consider how the need for security relates to sustainability, convenience, market freedom, health and safety, privacy, trust and collective efficacy, freedom of movement, aesthetics and social inclusivity. In other words, a balance must be struck. For example,
the need for a highly aesthetic product does not trump the need for security. Besides, privacy is often at the centre of heated discussions in relation to security. When security measures, such as CCTV or digital fingerprints on electronic ID cards, are on the table, privacy concerns always prevail.

Next to design contradictions, preventers might also be faced with iatrogenic effects of implemented crime prevention measures, which must be taken into account. These effects are wider than side effects and might include error and negligence resulting from poor decisions or actions on account of the preventers. More specifically, iatrogenic effects kick in when measures meant to prevent crime actually become crime facilitators. Offender-based research (OBR) is helpful to understand this problem, as offenders can explain where the wrong measure was implemented or why the measure did not work properly in certain cases. An example of a lesson learnt from OBR is how a label attached to products stating “only sold in (store name)” does not make the goods less attractive for thieves, because one would assume that the label underlines the stolen character, which makes it harder to sell and helps to return the recovered stolen goods back to the owner. As it turned out, however, the labels did not hold thieves back. Either because they stole for self-use or because their buyers would not care that it concerned stolen goods. What’s more, the label served as proof for the goods not being counterfeit.
WINNING THE ARMS RACE

Anticipate future threats

Preventive action is crucial in the fight against crime. Europol confirms that especially in the context of rapid evolutions in technology and criminality, it is no longer enough to be reactive.\(^{20}\) In order to overcome a merely reactive strategy, law enforcement will need to adopt a proactive strategy that meets certain requirements (see further). For the purpose of developing this proactive strategy, Europol explored future threats so as to recognize them early on and to understand their implications.\(^{21}\) Even tough Europol explored these threats with law enforcement in mind, the results are relevant for the wider crime prevention domain.

Even though the threat of Artificial Intelligence (AI) is largely applicable to cybercrime, it does have some implications for OPC. Social bots based on machine-learning technology can be used to interact with customers. This facilitates the fencing of stolen goods.\(^{28}\) 5G - or the fifth generation of telecommunication systems - poses another threat for criminal investigations in general. The problem is situated in the fact that 5G technology will complicate the use of unique mobile-phone-card identifiers that allow for the identification and localisation of devices by law enforcement. This is challenging as it is perceived as one of the most important investigation tools. Unfortunately, this challenge does not appear to be a priority for developers. Therefore, it is important that law enforcement continues to engage with the private sector in order to defend its interests.\(^{29}\) Furthermore, dark web networks and cryptocurrencies have been identified as key enablers of crime in general in the 21st century. Largely due to the rising popularity of block-chain technology, decentralised systems have become more prominent. It is noteworthy that privacy (trade-off) drives innovation in this field. The difficulty with this development, according to Europol, is that within a decentralised web, no single entity is responsible for operating, or storing, data and thus is held accountable for the criminal abuse of its networks.\(^{30}\) Finally, 3D printing poses a threat as it is already being used to manufacture ATM skimming devices.\(^{31}\)

Besides threats, the digital era also brings opportunities for crime prevention. A wide range of products and services are becoming digitised and interconnected. This opens the pathway to new methods of detecting criminals’ digital traces. Predictive policing enables a shift from a traditionally reactionary approach to one that is more proactive and preventative. Progress in the domain of multimedia analytics has led to improved possibilities for facial and object recognition. This includes software that analyses images and communication patterns on a criminal’s electronic device and cross-matches databases and other devices. The advantages of such applications are less human bias, increased accuracy, a better use of resources and an efficient solution for an ever increasing amount of data.\(^{32}\)

Set a proactive course

OCGs are complex opponents in the arms race. The fact remains that while prevention actors need to adhere to a set of rules, be they legal, ethical or even administrative, OCGs often do not. Nevertheless, this does not mean that the arms race should benefit the criminals. Ekblom formulated several recommendations on how to keep up, or ideally stay ahead, in the arms race.\(^{33}\)

He suggests to study offender resources, such as knowledge, information sources and networks, skills and adaptability. Results might help designers to keep crime reduction in the back of their minds.
Also to slow offender adaptation. Knowledge on methods of offending, vulnerabilities of targets and methods of prevention is readily accessible to offenders via the internet. A third suggestion is to encourage variety in security. Even though the standardisation of security techniques seems attractive, it is likely to be counterproductive. Offenders faced with uncertainty about what preventative systems they may find are at a disadvantage. Furthermore, he stresses the importance of specifying security requirements using performance standards (e.g. lock must resist expert picking for 20 minutes) instead of construction standards. This will maximise design freedom. Besides, one should avoid rigidity. The possibility for remedy should, if anything, be built to avoid rigidity, to anticipate design failure and be future proof when needed. Another recommendation is to be ready to roll out the next solution when existing security is cracked. Even the best preventive method will have a limited life span.34

In order for crime prevention actors to follow this proactive strategy, several requirements need to be fulfilled on an organisational level. Although these requirements are listed with law enforcement in mind, these are true for the wider crime prevention domain.

The crime prevention field should engage in a dialogue with the private sector in order to defend its interests in a process where security is not perceived as a number one priority. Europol puts itself forward as the ideal platform for this with regard to law enforcement.

There has been increasing regulatory activity tailored to new technological realities. Data privacy concerns are a priority for legislators. The voice of law enforcement agencies must be heard in order to protect needs with regard to accessibility of data and lawful interception. With regard to crime prevention, crime-proofing regulation, such as the UK case, offers ample scope.

Traditional command and control organisations often have difficulties adapting to changes in the threat environment rapidly. What we need is a culture that welcomes new ideas and embraces cooperation with external partners with a view to benefiting from the expertise from the private sector and the academic world.35

Another recommendation is to be ready to roll out the next solution when existing security is cracked. Even the best preventive method will have a limited life span.

In order for crime prevention actors to follow this proactive strategy, several requirements need to be fulfilled on an organisational level.
CONCLUSIONS

Property crimes are highly visible and have a major impact on people’s sense of insecurity. The organised aspect turns it into a complex crime phenomenon and makes the prevention thereof an even more challenging mission. Additionally, living in a continuously changing world in terms of politics, economy, technology, etc. impacts society in general and our daily lives. The technological development can be seen as the primary driver for social change and has progressively reshaped the routine activities of society. Technology is an important factor to understand trends in society, crime and crime prevention. Furthermore, design and development are crucial phases in the lifetime of a product. Even though one cannot foresee all dangers, the goal of crime prevention should be high on the agenda when designing a product. The private sector is the driver for technological innovation and plays a pivotal role. Unfortunately, there are some factors that can restrain the use of new technologies at the prevention side, which do not affect criminals or do so to a lesser extent. These are design contradictions or trade-offs, such as aesthetics and privacy. Finally, preventers cannot rest on their laurels once they have found an effective security measure to make a product less vulnerable to crime because adaptations and counter adaptations are part of a larger arms race between criminals and preventers.

In order to stay ahead in the arms race, the crime prevention field needs to anticipate future threats and set a proactive course. Europol explored future threats so as to recognise them early on and to understand their implications. Artificial Intelligence, 5G, dark web networks, cryptocurrencies and 3D printing pose a threat. In the context of rapid developments in technology and criminality, it is no longer enough to be reactive. In order for crime prevention actors to adopt a proactive strategy, certain suggestions should be followed. Ekblom suggests for the crime prevention field and their partners to study offender resources, slow offender adaptation, encourage variety in security, use performance standards, avoid rigidity and to be ready to roll out the next solution. Besides these recommendations, there are several requirements to be fulfilled at a more organisational level. Firstly, crime prevention actors and law enforcement should engage in a dialogue with the private sector in order to defend its interests in a process where security is not always perceived as a number one priority. Secondly, the crime prevention field needs to enhance their access to technical infrastructure and specialist expertise. Thirdly, the culture that should dominate the crime prevention sector, should be one that welcomes new ideas and embraces cooperation with external partners in order to benefit from the expertise from the private sector and the academic world.

DE LA TORRE, Pilar, Efus, group discussion at EUPCN's expert meeting “Innovation and technology within the prevention of OPC”, Brussels, 18 April 2019.


EKBLOM, Paul, UCL, Future crime problems & solutions – How to anticipate them and what to do about them, presentation at EUPCN's expert meeting “Innovation and technology within the prevention of OPC”, Brussels, 18 April 2019.


EUROPOL, Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement., 2019, 9.


3. EUROPOL, op.cit.
4. Paul EKBLOM, UCL, Future crime problems & solutions – How to anticipate them and what to do about them, presentation at EUPCN’s expert meeting “Innovation and technology within the prevention of OPC”, Brussels, 18 April 2019.
6. Paul EKBLOM, op. cit.
7. Ibid.
15. EUROPOL, op. cit.
22. An immobiliser is an electronic device that protects your vehicle from being hot-wired and thus stolen.
23. EUROPOL, op.cit., 5.
25. Ibid., 38.
27. Ibid., 8.
28. Ibid., 11.
29. Ibid., 12.
30. Ibid., 13.
31. Ibid., 15.
32. Ibid., 18.
33. Paul EKBLOM, UCL, Future crime problems & solutions – How to anticipate them and what to do about them, presentation at EUPCN’s expert meeting “Innovation and technology within the prevention of OPC”, Brussels, 18 April 2019.
CONTACT DETAILS

EUCPN Secretariat
Phone: +32 2 557 33 30
Email: eucpn@ibz.eu
Website: www.eucpn.org