Appendix 3
Deterrence as a security concept against organised crime

Sander Huisman[1]

Current situation

The nature of so-called organised crime in the Netherlands is inextricably linked to the nature of Dutch society and the Dutch economy, as well as to the country's geographic location and its physical and digital infrastructure. Europol notes for instance that the Netherlands functions as a major transit point for various forms of international crime, such as drug trafficking and smuggling, the illegal cigarette trade and cybercrime.[2] The Netherlands has played a dominant role in various criminal markets for decades, particularly in relation to drugs, fraud, money laundering and cybercrime.[3] The (1) international orientation of the open Dutch economy and (2) the country's highly developed financial system with its specialist service providers foster an environment that is conducive to trade. Moreover (3), the risk, from a criminal's viewpoint, of illegal goods being intercepted is limited because of the volume and sheer diversity of the legal trade. The opportunities are further increased by the open borders with other European countries. The Netherlands also has an (4) excellent road, water, rail and air transport infrastructure. In addition, the country (5) is favourably located relative to several markets and is a European distribution point and logistics hub, as manifested by Schiphol and other airports, the port of Rotterdam and other centres of transhipment. The (6) presence of various migrant communities means that there are many bridgeheads that contain an active or passive network of helpers. Amsterdam (7) is an attractive international meeting place. This applies particularly with regard to foreign criminals, who, according to a number of experienced investigating officers, usually remain under the radar of the police and intelligence services. Lastly, the Netherlands (8) is seen as being soft on crime, as a result of which criminal entrepreneurs like to do their business in the country.

The Dutch Advisory Council on International Affairs[4] (2013) identifies VAT fraud in the EU and cybercrime as the most extensive and rapidly growing forms of international crime in relation to the Netherlands. The National Threat Assessment[5] prepared by police investigators observes that criminal activity is currently influenced most by developments in digital technology and the use of the internet. This applies to different forms of organised crime, in

1 The author wrote this contribution in a personal capacity.
2 Europol, 'EU Serious and Organised Crime Threat Assessment (SOCTA) 2013'. The Hague: Europol 2013.
3 Netherlands Police Agency (KLPD), *Overall-beeld aandachtsgebieden Dienst Nationale Recherche 2010*. Driebergen: KLPD, 2010.
4 Advisory Council on International Affairs (AIV), *Criminaliteit, corruptie en instabiliteit: een verkennend advies* 85, The Hague, 2013.
5 F. Boerman and M. Grapendaal, *Nationaal Dreigingsbeeld Georganiseerde Criminaliteit 2012*. Driebergen: KLPD, 2012.

the context of which several people cooperate primarily for the purpose of making money. In terms of characterising the core of criminal organisations,[6] a division into three categories can be made. First, there are the career criminals who hold dominant positions in the global and European drug markets. Second, there are individuals who, with the help of legal entities, enrich themselves through environmental crime, fraud, swindle and money laundering methods (such as the Palm Invest and Easy Life or construction fraud and property fraud cases). Third, there are cyber saboteurs who used advanced digital technology to con private citizens and companies and who often pose a threat to vital infrastructures (such as in the 2012 Bredolab case).

In view of the key position held by the Netherlands in the international drugs market in geographic and logistics terms, the country is a logical base for criminal entrepreneurs from a variety of source and destination countries. The ability of foreign criminals to reside anonymously in the Netherlands is facilitated by, among other things, willing estate agents, the anonymous prepaid telephones that are, for now, still available and the lack of compulsory identification checks in some internet cafés. In recent years, there has been growing awareness of the existence of various foreign individuals and criminal groups. Various groups or subcultures, such as Brits, Colombians, Italians, individuals from the former Yugoslavia and Hong Kong Chinese, have been present in the Netherlands for decades. Numerous investigations have shown that criminal enterprises in the top segment of the drugs market are typically active in many countries. In addition to the geographic scope, the most dominant networks are also firmly embedded in legal sectors and have contacts with government agencies in the Middle East, West Africa and South America.

Career criminals who occupy a dominant position in certain criminal markets usually also have an extensive network of international contacts. This is certainly the case in the international drugs market, which is dominated by the Netherlands and Dutch career criminals. Virtually every major criminal investigation concerning this underworld has revealed international branches. Criminals typically regard Belgium as more of a hinterland rather than as a different country. Countries and regions that tend to feature most heavily in Dutch criminal investigations are Spain, Morocco, Turkey, various countries in South America, Eastern Europe, East Asia and West Africa and the city state of Dubai.[7] This sometimes has to do with the origin of the suspects and sometimes with the role of the country in the smuggling process, as a source country of goods or as a link in financial processes. Various investigations have shown that new relationships are usually forged during periods of detention in the Netherlands or abroad, since it is during such periods that new business opportunities are discovered.

6 The term ‘criminal organisations’ is controversial in the academic world because it places an emphasis on the existence of ‘organisations’, whereas in the opaque world of fighting crime, such entities usually cannot be observed. Moreover, ‘organisation’ suggests a certain duration, whereas practical experience shows that most partnerships in criminal circles are rather transient (Kleemans et al., 2002). In terms of criminal law, a criminal organisation exists in the case of ”participation in an organisation that intends to commit crimes”. A conviction virtually always concerns an individual, however, rarely a legal entity. For this reason, the decision was made to approach the subject in terms of an individual who, with or without others, engages in organising profitable crime, in other words, in terms of criminal entrepreneurs (Van Duyne, 1995) who are referred to in popular parlance as ‘career criminals’ or ‘professional criminals’ who are active in ‘organised crime’.

7 Netherlands Police Agency (KLPD), *Overall-beeld aandachtsgebieden Dienst Nationale Recherche 2010*.

The use of legal entities plays a crucial role in environmental crime, various forms of large-scale fraud and money laundering operations. These entities offer a veneer of legitimacy and protect the individuals who organise the illegal processes. Accounting items such as assessment reports and false claims create a false reality on paper to create the impression of compliance and adherence to proper procedures. As the analysis of the Netherlands Police Agency states regarding money laundering, the capital must pass the review of regulators in such a way that it receives a stamp of approval and can therefore be used in the legal economy.[8]

With respect to cybercrime, the range of suspects is extremely diverse and ranges from a 16-year-old school whiz kid to a 38-year-old computer science ace from a former Soviet republic. Motives also vary, from hacking for ideological purposes to sabotaging for fun to monetary gain, for example by extorting money from victims. Attacks on vital infrastructure constitute the main threat. Although government agencies appear to be the most capable of carrying out such attacks (think of the destructive power of the Stuxnet computer worm or Regin malware, for example), individuals can also do a great deal of damage. Police investigations reveal that the attacks, which are usually aimed at the financial system, are becoming more technically advanced. Use is often made of botnets, networks that commonly consist of millions of infected computers. The network hides the identity of the perpetrator and makes it possible to carry out powerful attacks. Against this backdrop, it is safe to say that international crime poses a threat primarily to the following national security interests: political and social stability (confidence of citizens in the state and vital infrastructure), economic security (financial damage to the government and private individuals and the functioning of the business sector) and environmental security (environmental damage).

Expectation for the coming five to ten years

The threats emanating from organised crime will probably remain acute in the coming five to ten years. As described in the Clingendael Monitor 2014, among elsewhere, two trends are set to dominate future developments. First, international crime will be characterised by increasing flexibility (in terms of form, composition and sphere of activity) and mobility (people, money and goods). In addition, there will be a further shift towards the virtual world.[9]

As a result of increasing digitisation and the increasing ease with which borders can be crossed, it will become more difficult in the future to combat criminal organisations, especially if they operate internationally. It is not just the case that cybercrime will substantially increase. Even in traditional organised crime cases there is an increase in the use of digital anonymisation and encryption techniques.[10] Furthermore, 'old school' members of the underworld occasionally hire cyber criminals to gain control of increasingly digitised logistics processes, for instance by hacking computer systems in seaports. With regard to financial processes, it is conceivable that greater use will be made of what are commonly referred to as new payment methods, which include prepaid debit cards onto which vast amounts can be loaded without being linked to traceable account holders. In addition, police investigators consider it likely that Trade-Based Money Laundering (TBML) will become more

8 Netherlands Police Agency (KLPD), *Criminaliteitsbeeldanalyse Witwassen 2012(b)*. Driebergen: KLPD, 2012.
9 Jan Rood, Frans-Paul van der Putten and Minke Meijnders, *Een wereld zonder orde? Clingendael Monitor 2015*. The Hague: Clingendael, Netherlands Institute of International Relations, February 2015.
10 Netherlands Police Agency (KLPD), *Criminaliteitsbeeldanalyse Hightech Crime 2012*. Driebergen: KLPD, 2012.

commonplace. In TBML, the proceeds of crime are used to purchase legal goods, after which the goods are traded on the international market. This enables criminals to transfer large amounts of money and illegal profit can be reported as legal profit.[11]

Successful criminal enterprises are also engaged in legitimate business practices that provide them with access to information. This enables them to influence the business community and political representatives in the non-criminal world. Positions can be secured in local communities, for instance in the hotel and catering industry, real estate or retail. These positions make such enterprises a counterpart (discussion partner and legal actor) of the local authorities. The ongoing economic recession may make individuals who are in debt more willing to provide assistance. Such assistance can be provided in many ways. Examples include the services of money mules and the selling of information within public service providers, banks or logistics companies (such as in ports). Logistics and financial links may be corrupted as a result. The protection of identities remains an integral part of the modus operandi of career criminals, financial legal entities and cyber saboteurs. Digital concealment techniques are expected to be used more often and will also become more readily available. In recent years, anonymity networks (The Onion Router, or Tor) and anonymous payments have become more popular in the physical crime world. In addition, career criminals will continue to rely on the loyalty and alertness of their supportive and robust communities (streets in certain neighbourhoods, trailer parks and clubhouses of outlaw motorcycle gangs (OMGs), for example).

In the years ahead, particular attention will need to be paid to the growing ease with which international relations are established in criminal circles. Career criminals who have a dominant position in certain criminal markets usually also have an extensive network of international contacts. The international phenomenon of expanding outlaw motorcycle gangs is relatively new. Until 2009, the Hells Angels were the only international outlaw motorcycle gang in the Netherlands. The next five years saw the emergence of Satudarah, No Surrender and the Bandidos. The number of members and chapters also grew tremendously in the five-year period referred to.[12] Many career criminals are members of an outlaw motorcycle gang. Plausible reasons for joining include the additional contacts and trading opportunities provided by an international outlaw motorcycle gang and the protection that comes with membership. If these gangs continue to grow, tensions between them are likely to increase as they compete for territory and seek to protect their interests. This competition will probably include violent incidents in the Netherlands and in other countries where there are chapters.

In the coming years, the use of the latest technological innovations is likely to be a key element in criminal activity. An increasing number of goods and services will be traded in hidden online markets (through Tor networks). Examples of such markets are the Silkroad 2.0 and Black Market Reloaded sites that were dismantled by the Team Hightech Crime of the Dutch police. Innovations such as the 3D printer and drones are also used in criminal circles, mainly to hide from and to monitor competitors and authorities more effectively. The hardware deployed is becoming smaller (easier to conceal), smarter (remote control, for example) and more powerful. Nanotechnology and robots, for example, will undoubtedly also be used in criminal circles in the future. A ‘traditional’ crime such as identity fraud

11 Netherlands Police Agency (KLPD), *Criminaliteitsbeeldanalyse Witwassen 2012*.
12 Police, *Outlaw Bikers in Nederland*. Woerden: Police Central Unit, 2014.

(the cornerstone of many criminal acts) may also acquire new dimensions as a result of technological innovations. This race is likely to continue.

The relevance of deterrence as a security concept

Deterrence based on retaliation is an important instrument in countering threats emanating from national and international criminal activity. Research has shown that preventive measures have the greatest effect in a broad-based approach aimed at undermining logistic elements of criminal markets.[13] When the authorities have identified suspects, administrative or tax-related interventions can also be highly effective in fighting crime. To be successful, such actions must be based on a multidisciplinary approach in which several parties feel that they own the problem and therefore consult on an approach in which to use all of the capabilities available to them. The Netherlands is a European and international leader in this context.

Apart from the development of a more broad-based approach initiated in recent years, however, it is not clear which approach has a deterrent effect on criminal organisations or individual career criminals. An approach based on criminal law usually results in detention or confiscation, an approach based on administrative law results in an administrative measure (the withdrawal of a licence or closing of a home, for example), and a tax-related approach results in a financial penalty (a tax assessment or an additional tax assessment, for example). A combined, or better, integrated approach is probably the one that is experienced as being the most effective and is therefore the one that probably has the greatest deterrent effect.

Criminal enterprises respond rapidly to changes in their environment. When government interventions occur, activities are temporarily suspended or relocated. When the authorities implement legislative changes, operations are adapted where possible to keep up the appearance of legality. When certain branches change logistics processes, logistic activities are adapted. The fragmentation that characterised criminal investigations in the Netherlands for many years made the country an ideal place for those who wished to advance to the position of 'king of the hill'. Such individuals can thwart, overcome or endure the existing measures (checks, investigations, prosecution, detention and rehabilitation) with relative ease. The climb up the criminal career ladder can be countered more effectively if opportunities to intervene are recognised and acted on at an earlier stage. This means, however, that the threat of an intervention, such as a rapid seizure or a rapid conviction, must also be credible, which is only possible if the authorities have built up a track record in terms of these measures.

The most successful career criminals derive their power from their reputation and status in criminal circles. They cannot sustain this power, however, without a reliable social environment (neighbourhood, family, criminal 'crew'). It is clear that temporary detentions have no effect on heavyweight career criminals. To them, such detentions come with the territory. They are business risks that they have taken into account. Moreover, such periods offer new opportunities, mainly in terms of forging new business relationships. The strategic ties with the social environment are strong and are not undermined by temporary detentions. The robustness of criminal groups is therefore virtually inextricably linked to the presence

13 See for example H.G. van de Bunt and C.R.A. van der Schroot, *Prevention of Organised Crime: A Situational Approach*. The Hague: Boom, 2003.

of thick crime habitats and community support.[14] A good reputation in the relevant circles is essential to the development of a criminal career. The status of career criminals is partly based on historical success, trust, discipline, useful contacts and business acumen. It also relies on their ability to intimidate, and to ensure that those closest to them remain silent with respect to the authorities.[15] Visible public servants (counter staff of a municipality and community police officers, for example) have the most to fear in this respect. This situation has an added dimension in cases where friends or family members are employed at a government agency and have access to specific information. Criminal networks can thereby gain in robustness and, as a result, benefit from an enhanced capacity to absorb government interventions. Reducing the resilience of criminal circles is by no means easy.

There are examples of government interventions in which a criminal network was dismantled in such a way that those in the more immediate social environment who were also benefiting from the criminal activity were also 'reprimanded'. This kind of dismantling occurred in 2010 in the case of an extremely wealthy drug dealer who had operated under the radar for many years and had built up an excellent reputation in criminal circles. A thorough national and international criminal and financial investigation resulted in long jail terms for those who had been directly involved in the criminal activity as well as the seizure of a range of movable and immovable property that had been registered as belonging to confidants and family members. This intervention therefore sent out a signal that went beyond those who were convicted. For capacity reasons, however, large-scale and comprehensive interventions of this kind will always be the exception rather than the rule. Smart and well-considered choices will therefore need to be made. Ideally, the actual effect of an intervention should also be gauged on the basis of current information. Various studies show that the most effective measures against criminal entrepreneurs and criminal organisations are those that affect the financial situations of such individuals and organisations. Use should be made first and foremost of rapid prejudgment attachment to ensure that the suspect and those in his or her social environment experience the effects immediately.[16] This measure would have a deterrent effect.

A special form of deterrence is the provision of information by former partners in crime to the police and judicial authorities for the purpose of incriminating other criminal entrepreneurs. It should come as no surprise to learn that criminal lawyers who mainly represent individuals who are often a focus of investigations into organised crime are highly critical about the more frequent use of criminal civilian infiltrators. From an investigative perspective, however, obtaining human intelligence from the underworld itself is becoming more important. This is because it is becoming more difficult to obtain information of real evidentiary value through more traditional investigation methods such as surveillance and the interception of communications. Cases often concern close-knit groups, the members of which consistently seek to conceal their activity. For this purpose, they use technical means and front men, and intimidate and threaten potential witnesses or officials. Sources in criminal circles are therefore becoming increasingly important in terms of both the informants and the (threatened) witnesses and, in certain cases, criminal civilian infiltrators.

14 J. Ayling, 'Criminal Organizations and Resilience'. In: *International Journal of Law, Crime and Justice*, 37 (2009), p. 182-196.

15 Netherlands Police Agency (KLPD), *Overall beeld aandachtsgebieden Dienst Nationale Recherche 2010*.

16 E.W. Kruisbergen, H.G. van de Bunt and E.R. Kleemans, *Vierde monitor georganiseerde criminaliteit*. The Hague/Rotterdam: Research and Documentation Centre (WODC)/Erasmus University Rotterdam (EUR), 2012.

Deterrence can only be effective if the threat of retaliation is credible.[17] Strikingly, this rule also applies in criminal circles as a condition for obtaining a respected and credible status. The risk of discovery, prosecution and detention must be high. This requires a robust government that intervenes swiftly, flexibly and firmly. It requires high-quality and therefore current information and proper cooperation between the partners involved (both public and private). It requires a solid contingent of capable guardians who are able to deal with willing offenders on the basis of current insight. The importance of international cooperation is self-evident in a world in which national borders are becoming less significant as a result of globalisation and the internet. This means that requests for assistance from other countries must be dealt with without delay. Interventions must take place in quick succession in order to secure and execute a judgment so that a clear message is also sent to those close to the criminal in question. This requires close cooperation between authorities as well as rapid action by professionals in their respective spheres of work. Finally, how to communicate with the general public must be properly considered. Media strategy is therefore extremely important, since substantial gains can be made with the correct 'framing'. Experience to date has shown that such communications are meaningful only if a new and unique understanding has been gained through investigation methods. In the right circumstances, deterrence based on retaliation can therefore be an effective instrument against crime, also with respect to criminal activity from abroad. However, other forms of deterrence that are part of the analysis framework of this report, i.e. indirectly increasing the costs that the perpetrator must incur or reducing the gains that the perpetrator can achieve, appear to be less relevant in countering this threat, except in the case of defensive measures in the field of cyber security that substantially increase the costs of engaging in cybercrime against targets in the Netherlands.

17 K.H. Hicks, 'The Case for Deterrence'. In: C. Cohen and J. Gabel (eds.), *2015 Global Forecast: Crisis and Opportunity*. Washington, DC: Center for Strategic and International Studies, 2014.