National Crime Agency

National Strategic Assessment of Serious and Organised Crime 2016

9th September 2016

Contents

Foreword from the Director General of the National Crime Agency

The threat from serious and organised crime continues to evolve and has done so over the last year in ways that have attracted considerable and understandable public attention, particularly in relation to organised immigration crime, child sexual exploitation and abuse (CSEA), firearms, cyber crime and money laundering.

Against this backdrop, there have been major operational successes spanning multiple areas of crime including one of the UK's biggest-ever firearms seizures, the arrest of over 280 individuals and 150 children safeguarded in one of the country's largest ever investigations into online CSEA and the biggest class A drug seizure on record in the UK.

All these successes have been built on collaboration – collaboration which continues to grow nationally, internationally and across the public and private sectors and is exemplified by developments such as:

- the NCA-led multi-agency intelligence cell developed to establish and maintain a fully joined-up intelligence picture on organised immigration crime;
- wide-ranging collaboration across the UK and international public and private sectors to tackle the pervasive threat of cyber crime; and
- the ground-breaking NCA/GCHQ Joint Operational Cell to tackle CSEA and criminal activity on the hidden internet.

Collaboration such as this is fundamental both to our understanding of the threat and to our delivery of the most effective response; in the year ahead we will continue to take it forward. We will continue to work with our partners – collectively – to develop a more comprehensive intelligence picture as the threats from serious and organised crime continue to evolve. Informed by this picture, we will then make flexible use of our collective resources to lock up more serious and organised criminals or, where this is not possible, to disrupt them in other ways.

The National Strategic Assessment is a reflection of this collaborative approach, and I would like to express my appreciation to all who have contributed. I am confident that it provides us with a very solid understanding of the threat from serious and organised crime for the year ahead as we work together to have maximum impact on the serious and organised criminals damaging the UK and its interests overseas.

Lynne Owens CBE QPM MA
Director General, National Crime Agency

Introduction

1. The National Strategic Assessment (NSA) provides a comprehensive picture of the risk posed to the UK and its interests by serious and organised crime. It informs both the national response – what the priorities are and what action will be taken – and the expected results – how success will be measured.

2. The NCA's National Intelligence Hub (NIH) has produced this document on behalf of UK law enforcement. Its preparation has involved wide consultation across the law enforcement community and its partners including police forces in England and Wales, PSNI, Police Scotland, Regional Organised Crime Units (ROCU), Border Force, the National Offender Management Service (NOMS), Her Majesty's Revenue and Customs (HMRC), the Serious Fraud Office, the Crown Prosecution Service, Immigration Enforcement, Cabinet Office, Home Office, the Foreign and Commonwealth Office, and the security agencies.

Methodology

3. Throughout the document an assessment tool[1] has been used to ensure consistency across the different threats and themes when assessing probability. The following table provides definitions.

Qualitative Statement	Associated Probability Range
Remote or Highly Unlikely	‹10%
Improbable or Unlikely	15-20%
Realistic Possibility	25-50%
Probable or Likely	55-70%
Highly/Very Probable/Likely	75-85%
Almost Certain	›90%

4. The period of the assessment covers the year from the beginning of March 2015 to end of February 2016. The United Kingdom's recent decision to leave the European Union in June 2016 has not been taken into consideration during the drafting and review process of this document.

1 Professional Head of Intelligence Analysis (PHIA) 'Uncertainty Yardstick'

Overview

5. The national-level impact of serious and organised crime has been reinforced over the last year by the evolution of a number of threats which have attracted significant and understandable political, public and media attention.

6. The unprecedented scale of irregular migration, with domestic and European ramifications, has highlighted the damaging impact of organised crime involvement. The serious and organised crime threat from firearms, which potentially links to terrorism, was highlighted again by the November 2015 Paris attacks. Child sexual exploitation and abuse (CSEA) continues to pose exceptional challenges to law enforcement.

7. Cyber crime has risen in the public consciousness owing to high-profile attacks which threaten UK business and public confidence in the security of their information online. And the daily impact of high-end money laundering persists, threatening the UK's financial system and international reputation.

8. Our understanding of the threat from serious and organised crime has continued to improve. Based on that understanding, and the effectiveness of the response, the top five threats to the UK (not in any order of priority) for the year ahead are:

- **Child sexual exploitation and abuse**
- **Organised immigration crime**
- **Cyber crime**
- **Firearms**
- **High-end money laundering**

Key judgements

Child sexual exploitation and abuse

- The large increase in the volume of reported crime, intelligence generated from industry, and forensics continues to have very significant resourcing implications for law enforcement.
- The advancement of technology poses challenges for law enforcement. Live streaming and cloud storage of CSEA content which can be hosted on infrastructure outside UK jurisdiction, together with challenges in identifying online offenders, mean that current law enforcement approaches may need to be refined.
- The practice of live streaming is one example of how offenders can simultaneously create indecent images of children (IIOC) online, view IIOC, and commit contact abuse by proxy overseas. This convergence across all CSEA threat areas is an indicator of the threat evolving with new technologies.

Organised immigration crime

- The highest priority Organised Immigration Crime (OIC) threat is clandestine activity using Roll-on Roll-off (Ro-Ro[2]) and containers. This poses a threat to the lives of those concealed within. Organised Crime Groups (OCGs) often use seaports away from the migrant camps.
- OCGs often move migrants from their own ethnic backgrounds and have networks with a presence in the originating countries, intermediate countries and the UK.
- As security around borders increases, the growth in organised people smuggling and trafficking targeting the UK will grow through clandestine activity and use of false documents.
- Attempts to reach the UK from the near continent are made by a mixture of individual effort, loosely organised attempts by the migrants themselves, and organised criminals.
- Fewer irregular migrants seek to enter the UK using false documents than clandestinely. However, the availability of false documents will allow more irregular migrants to use air travel into the UK.

Cyber crime

- Financially motivated, international OCGs responsible for sophisticated malware campaigns remain a substantial threat to the UK.
- Cyber crime is becoming more aggressive and confrontational, with a rise in easy-to-execute criminal tools, many designed to extort money from victims. Both international and UK domestic criminals are engaged in these attacks.
- Cyber criminals based in the UK and overseas make use of an enabling marketplace providing products and services which continue to lower the barrier of entry to cyber crime.

2 Ro-Ro includes accompanied road goods vehicles, unaccompanied trailers, goods loaded using port-to-port trailers and import/export motor vehicles via ferry and Channel Tunnel. It also includes passenger ferries.

Firearms

- Whilst the threat from firearms in the UK is relatively low due to comparatively low availability, there is evidence of an escalating threat in Europe.
- Firearms currently entering the UK are commonly sourced from Eastern Europe and the Balkans. Transit countries include the Netherlands, Belgium and France.

Money laundering

- Our picture of high-end money laundering is limited but improving. Estimates of the global scale of money laundering based solely on international averages of between 2% and 5% of GDP are likely to underestimate the threat, given the UK's position as a key global financial centre. The critical importance of the financial sector to the UK's economy means that money laundering, particularly high-end money laundering, has the potential to threaten the UK's national security, national prosperity and international reputation.
- Virtually all high-end money laundering schemes, and several cash-based ones, rely on professional enablers to facilitate this activity. The skills, knowledge and abilities of professionals in the financial and legal sectors allow highly complex structures to be created that move and store large amounts of criminal money and conceal ownership effectively.
- Cash-based money laundering continues to play a major part in many crime groups' modus operandi (MO). A high proportion of cash movements are managed by a small number of international controllers.
- Private sector engagement is critical to identifying and disrupting high-end money laundering schemes, whether targeting individuals, disrupting techniques or target-hardening the UK's financial system.

Bribery, corruption and sanctions evasion

- The proceeds of grand corruption committed overseas are laundered through the global financial centres of the world. The UK is one of the most attractive destinations for these funds to pass through and be invested in. Politically exposed persons (PEP) continue to pose a reputational and financial risk to the UK when they abuse their position for personal gain and choose to launder the proceeds of their corruption into the UK.
- Bribery committed internationally by UK entities has reputational, financial, political and social consequences. It disadvantages people overseas while undermining the UK's ability to promote sustainable growth and raise international standards.
- UK entities involved in breaching financial sanctions damage the UK's international reputation and undermine foreign policy goals, as well as those of international partners.
- Professional enablers and intermediaries are used to launder the proceeds of corruption, evade sanctions and facilitate bribery payments involving UK entities. They create complex and sophisticated structures that distance the individuals from the money whilst retaining control of the illicit funds.

Drugs

- UK wholesale prices provide significant profit margins for all imported drugs.
- An increase in competing OCGs, coupled with changing demographics, continues to put pressure upon existing UK-based crime groups This increase in competition is assessed to be influencing the criminal demand for and use of firearms.

Economic crime

- The overall scale of complex fraud against the UK private sector is unknown but is likely to involve losses of hundreds of millions of pounds. This has the potential to cause financial and reputational damage to the UK economy and individuals' wealth.
- There may be many more UK victims of fraud than previously thought. Estimates of fraud based on the Crime Survey of England and Wales and released in October 2015 suggested there could have been over five million cases of fraud in the last year.
- The public sector continues to be a target for organised criminals. Whilst there are estimates of the losses to criminal attack in some areas (such as the HMRC estimated GBP 5.1 billion per annum losses to the UK tax system), the full extent of serious and organised fraud against the public sector is not known.
- Fraud and wider economic crime is increasingly cyber-enabled and often involves international networks operating across numerous jurisdictions.

Modern slavery and human trafficking

- Greater engagement, activity and awareness of the modern slavery and human trafficking (MSHT) threat and the available reporting pathways has contributed to increased reporting, with labour and sexual exploitation and the exploitation of minors all exhibiting increased National Referral Mechanism (NRM) referrals.
- Whilst cases of inter-nationality exploitation have been recorded, the majority of MSHT criminals share a national or ethnic background with their victims.
- Modern slavery is a financially motivated crime. Whilst in a substantial number of cases criminal assets and proceeds are thought to be held overseas we judge that the seizure of cash and assets of traffickers under the powers expanded by the Modern Slavery Act 2015 could significantly disrupt the threat.

Organised acquisitive crime

- OCGs involved in OAC are commonly active across regions, challenging law enforcement coordination.
- Vehicle theft is an enabler for broader OAC and other criminal activity.
- Violent, destructive and weapon-enabled MOs are common in commercial robbery and commodity crime.

Border vulnerabilities

- Corrupt workers within both the private and public sector facilitate the movement of illicit goods into the UK and the avoidance of border controls by irregular migrants.
- Criminals seek to use yachts, tug boats and other small vessels, as well as light aircraft, to help with the smuggling of illicit commodities into the UK.
- Border controls at UK ports have been improved in response to increasing levels of attempted clandestine entry. However, criminal groups continue to develop new methods for concealing the movement of illicit commodities and people in order to avoid detection.

Criminal use of identity

- Physical document abuse remains the primary way in which criminals use identities. The production of false documents can take place on a mass scale.
- The production and supply of false documents are key enablers for migrants looking to illegally enter or remain in the UK.
- The scale of cyber-enabled identity crime is likely to be increasing due to the volume of personal data now online.

Criminal use of internet technology

- Intelligence indicates an increase in the use of encrypted communications by criminals across all threat areas and across all levels within crime groups.
- The number of marketplaces found on the dark web and their scope have increased since 2013. Drugs remain the main commodity sold.
- Trusted, anonymous payment systems are an enabler for dark web trade. Bitcoin remains the virtual currency of choice.

Foreign national offenders

- FNOs are involved in most threat areas and are occasionally involved in the development of new areas of criminality, often responding flexibly to market demands.

Prisons and lifetime management

- The concentration of offenders in prison helps maintain existing groups, the formation of new networks, and the identification of experienced offenders to enable future crimes.
- Intelligence strongly indicates that access to illicit mobile phones is aiding the continuation of serious and organised crime from prison.

National Control Strategy

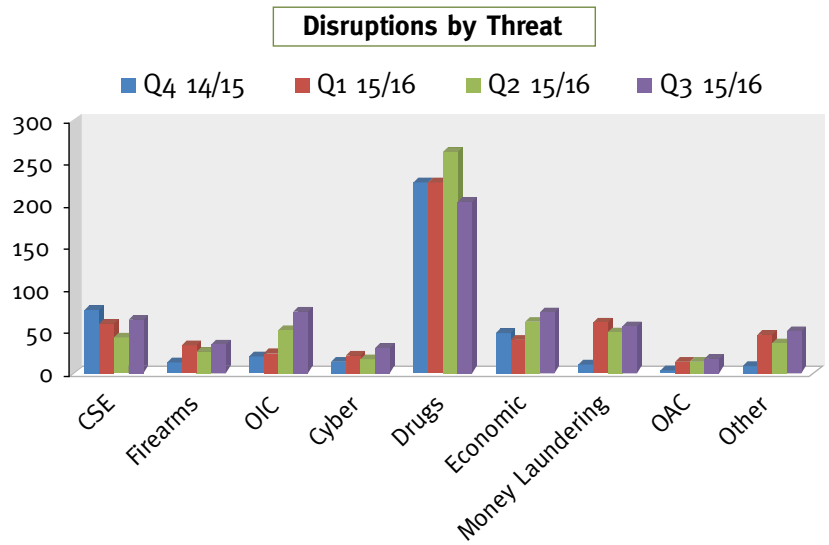
The NSA provides a comprehensive picture of the threat to the UK from serious and organised crime and informs the National Control Strategy (NCS), which prioritises the response to the threats and cross-cutting issues identified in the NSA. The NCS outlines mitigating actions for UK law enforcement and its partners to counter serious and organised crime and provides a framework for flexibly deploying the UK's collective resources to catch or disrupt more serious and organised criminals. The NCS has identified the following **five national priorities** for response: **child sexual exploitation and abuse, organised immigration crime, cyber crime, firearms, and high-end money laundering**.

The following table indicates the relative priority of sub-threats by threat area with criminality in Band 1 representing the highest level of threat to the UK and that in Band 3 the lowest in relation to the rest.

	Child sexual exploitation and abuse	Organised immigration crime	Cyber crime	Firearms	Money laundering	Bribery, corruption and sanctions evasion	Drugs	Economic crime	Modern slavery and human trafficking	Organised acquisitive crime
Threats	Contact sexual abuse of children	Facilitation of illegal immigration	The cyber crime marketplace	Firearms – international supply	High-end money laundering	International bribery and corruption	Heroin	Fraud against the public sector	Trafficking children and young adults	Organised vehicle crime
			Multinational cyber OCGs				Cocaine	Fraud against the private sector		
	Transnational child sexual offenders	Clandestine people smuggling				Sanctions evasion			Trafficking of adults for labour exploitation	Commercial robbery
			UK-based cyber criminals and infrastructure	Firearms domestic and legitimate supply			Cannabis	Insider dealing/ market abuse		
		False documents				Politically exposed persons			Trafficking of adults for sexual exploitation	Commodity crime
			High volume, low impact attacks on UK victims		Cash-based money laundering		Synthetics	Fraud against the individual		
	Online child sexual exploitation	Abuse of legitimate means to enter or remain in the UK		Firearms advance technology and emerging trends		Domestic bribery and corruption			New and emerging exploitation threats	Wildlife crime
			Emerging new crimeware				New psychoactive drugs	Counterfeit currency		
Cross Cutting Enablers	Borders vulnerabilities									
	Criminal use of identity									
	Criminal use of internet technology									
	Foreign national offenders									
	Prisons and lifetime management									

Priority Band 1
Priority Band 2
Priority Band 3

National Results against Serious and Organised Crime in 2015



What is a disruption?

A disruption is a measurement of impact against serious organised crime. It may be achieved by any activity covered in the Serious and Organised Crime Strategy and will have involved some form of resources intervention (input) by an agency, resulting in an output impacting upon the threat.

Major disruption – Significant disruptive impact on an OCG, individual or vulnerability with significant or long-term impact upon the threat.

Moderate disruption – As above but with noticeable and/or medium/term disruptive impact.

Minor disruption – As above but with limited and/or short-term disruptive impact.

National Results Reporting in 2015

National performance reporting made significant progress in 2015, primarily due to the provision of data, including disruptions, from the National Crime Agency (NCA), Regional Organised Crime Units (ROCUs) and Home Office Immigration Enforcement (HOIE). The picture was enriched by performance metrics from HM Revenue & Customs (HMRC) and the National Ballistics Intelligence Service (NaBIS).

There were **2,137** disruptions reported between January and December 2015, inclusive. Disruption volumes have increased quarter-on-quarter since reporting commenced, reflecting our developing understanding of the impact of our combined activity.

Notably, there has been an increase in major disruptions. This is indicative of the level of impact being made across several areas of complex criminality.

Q4 2014/15	Q1 2015/16	Q2 2015/16	Q3 2015/16
429 disruptions	531 disruptions	569 disruptions	608 disruptions
1,102 arrests	1,334 arrests	1,305 arrests	984 arrests
670 charges	749 charges	720 charges	609 charges
206 convictions	362 convictions	324 convictions	419 convictions
£3.04m cash seized	£3.06m cash seized	£3.96m cash seized	£4.52m cash seized

National Results against Serious and Organised Crime in 2015

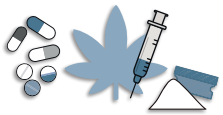
Results Metrics

4,725 arrests

2,748 charges

1,311 convictions

145 tonnes cannabis seized



382 guns seized

3.8 tonnes heroin seized

55.7 tonnes cocaine seized

£65.04m assets recovered

Developing the National Results Picture

Analytical development is furthering understanding of the impact of activity against the serious organised crime threat. This analytical approach is being developed throughout 2016.

Quantitative data from the ROCUs is now being augmented with qualitative information to better inform the understanding of impact.

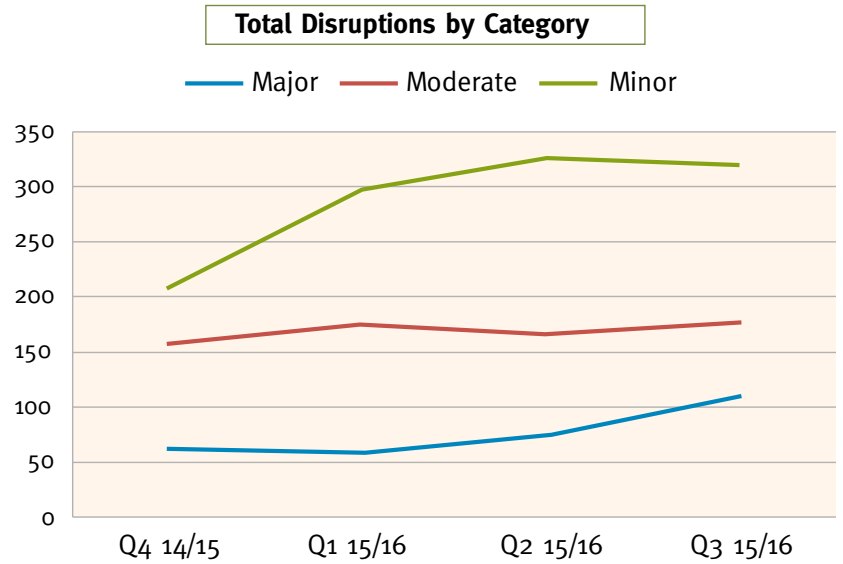
A systematic approach will be established in 2016/17 to capture the activity of all 43 police forces in England and Wales against serious organised crime.

An alignment of the National approach to capturing disruptions is underway to ensure data consistency, including the development of National disruptions guidance.

Improved data capture methodology and accuracy across all data and information sets is being developed.

Prioritised Threats

- 2015 has seen a sustained rising trend in reported major disruptions against the firearms threat.
- OIC-related disruptions are rising, driven in part by the increased reporting of activity, and the improved understanding of impact, against the people smuggling threat.
- Results against the CSE threat were characterised by a large number of arrests and convictions by the NCA and police forces, following NCA surge activity in response to the IIOC threat.
- Operational outcomes against high-end money laundering and professional enablers may take considerable time to be realised, due to the complexity within this area of threat.
- There is an upward trend in recorded disruptions against the cyber threat, particularly in relation to ROCU reporting.
- Further development of the performance framework is being undertaken Nationally to adequately reflect activity and impact against each of the 4Ps.



National Strategic Assessment

Introduction

9. This section of the report covers the 2016 National Strategic Assessment. This comprises:

    - an overview of serious and organised criminals and their pathways into serious and organised crime;
    - an overview of the international aspects of serious and organised crime;
    - a forward look over the next five years: the trends and drivers that could affect the serious and organised crime threat and law enforcement's response to it; and
    - individual chapters on each of the identified threats and cross-cutting enablers, consisting of

        a. an assessment of the current threat including reference to some response activities; and

        b. a forward look over the next 6 to 12 months assessing how the threat will evolve including reference to major developments in the response.

Serious and organised criminals

10. According to Organised Crime Group Mapping, there were over 6,000 active OCGs consisting of nearly 50,000 individuals towards the end of 2015. The majority (91%) were male. Ages ranged from 16-90, with an average (excluding outliers)[3] of 34. The most common age range was 26-35 (39%). Where nationality was mapped, 82% were British. Of the mapped foreign nationals, the most common nationalities were Pakistani (8.4%), Romanian (8.2%), Albanian (5.3%), Nigerian (5.3%), Polish (5.3%) and Lithuanian (4.8%).

11. Serious and organised criminals typically operate in loose networks based on trust, reputation and experience. Structured and hierarchical groups are usually based on family ties. Both loose and structured groups can cross ethnic boundaries, and often have international links to facilitate criminality. Some that impact the UK, however, are located entirely abroad.

12. Pathways into criminality are diverse, and differ between crime types. Individuals and businesses that commit or enable serious and organised crime often have particular characteristics and their risk of involvement increases when they belong to certain networks. There are some intelligence gaps surrounding pathways but the infographic below represents our current understanding[4].

13. The availability of criminal products and services on the internet, particularly on the hidden internet, has created an international marketplace where offenders can network and operate with a high degree of anonymity.

14. Financial gain is not always the principal motivation for involvement in serious and organised crime. For example, cyber criminals can be driven by ideology and CSEA offenders by a sexual interest. Individuals can also be coerced, corrupted, debt-bound, groomed and exploited, or even offend unwittingly[5].

3 A small number of outliers below and above the 18-60 age range were removed for the purpose of this calculation.
4 0217-HO: Pathways into Serious and Organised Crime, February 2016.
5 Ibid.

Pathways into Serious and Organised Crime

Individuals

- Specialist skills/knowledge
- Addiction
- Greed
- Financial hardship
- Mental health issues
- Transitional periods
- Troubled family life

COMPLICIT
COERCED
CORRUPTED
GROOMED
EXPLOITED
UNWITTING

Businesses

- Storage or transportation functions
- Money laundering opportunities
- Night time economy (contacts & clientele)
- Small /struggling companies
- Insider access

CHARACTERISTICS

Family

OCG families mentor and normalise criminality. Criminal favours for relatives can escalate.

Associates

Offenders in friendship, social, and employment networks can offer criminal opportunity.

Ethnicity and Culture

Can foster trust, and may give some groups global criminal contacts.

Prison

Offenders can maintain or create criminal networks. Vulnerable prison staff can be corrupted.

Online

Illicit opportunities for those who might not offend offline, and perceived anonymity on the Dark Web.

NETWORKS

Drugs

Orchestrators are driven by **profit**, whilst lower level offenders can be **exploited** or **debt-bound**.

Organised Acquisitive Crime

Offenders usually have a **history** of **prolific offending**, and may have a **limited education**.

Economic Crime

Offenders often have **knowledge** and **experience** of the targeted **sector**, usually through previous **employment**, and can **identify** and **exploit loopholes.**

Organised Immigration Crime, Modern Slavery and Human Trafficking

Sometimes **struggling ex-migrants**, offenders can be drawn in for **money**. **Traveller OCGs** are often involved in **modern slavery**.

Cyber Crime

Offenders can be motivated by **profit**, **ideology**, or simply the **challenge**. Competent individuals may **develop criminal intent** upon identifying **potential profits**.

Child Sexual Exploitation and Abuse

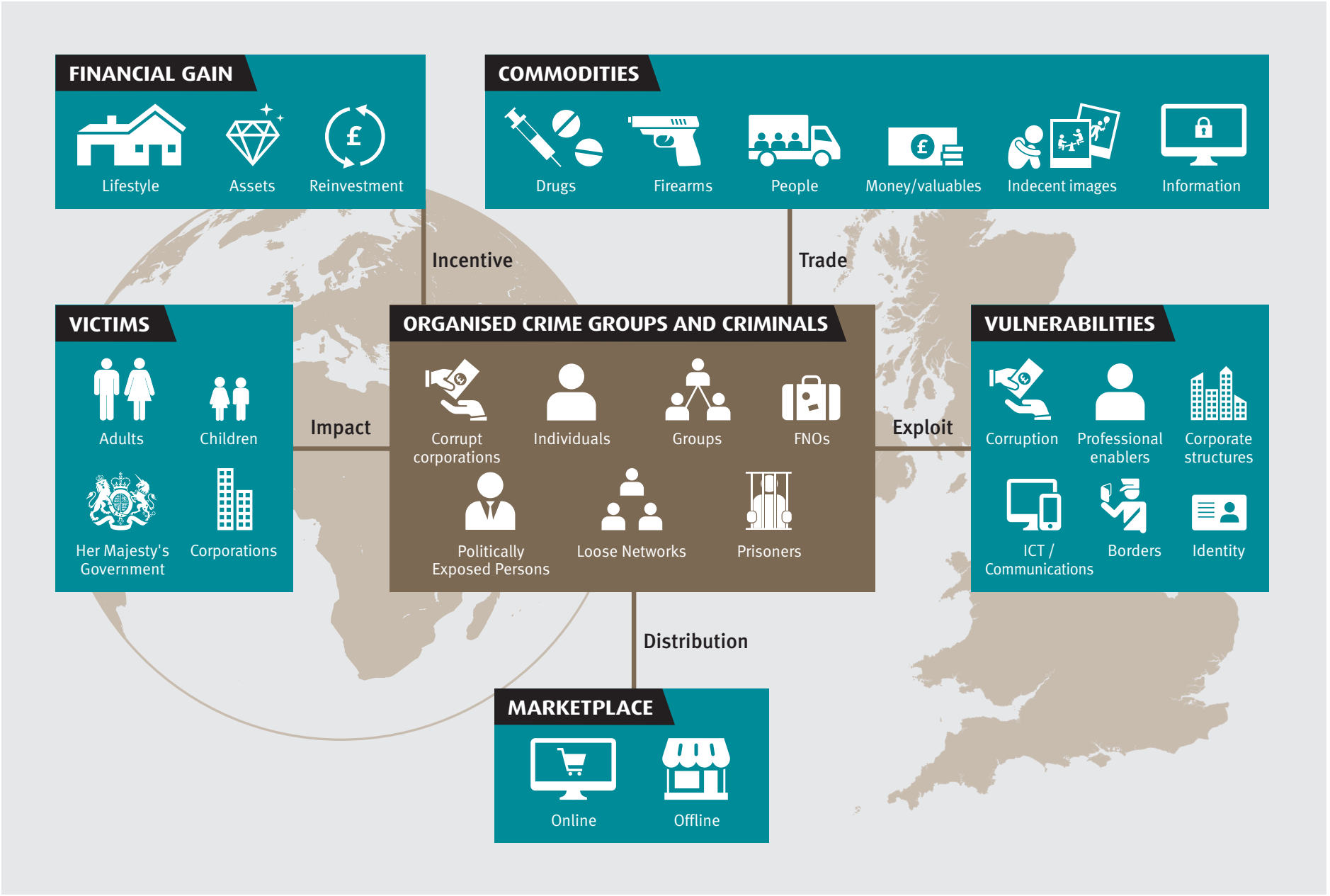
Offenders usually have a **sexual interest** in children. **Online** abuse can be driven by a desire to exert **control**.

Firearms

Possession and **discharge** is often driven by **protection/enforcement** of other criminality. **Hoarders** or those with a fascination can be **exploited**.

THREATS

Serious and organised criminals and their criminality



International

15. Many of the threats identified in the National Strategic Assessment originate overseas. For numerous illegal commodities, such as firearms, drugs and counterfeit documents, overseas countries are the beginning of the criminal supply chain. These commodities can follow many different routes to reach the UK with diverse criminal groups taking control of or facilitating their passage.

16. International OCGs exploit vulnerabilities such as inadequate law enforcement and criminal justice structures, weaknesses in legislation, corruption and vulnerable communities. Some threats, such as cyber crime or online child sexual exploitation, are by definition international in a technologically interconnected world. Foreign criminals impact on the UK from overseas and some British criminals, whether fugitive or not, often feel safest outside the UK.

17. Often the most effective response is to tackle the problem at source. Overseas interdiction addresses the international threat with maximum effect focusing on high-priority targets, the seizure of illegal commodities and the disruption of the enabling activity that underpins serious and organised crime.

18. Collaboration with international partners to influence and build capability in priority countries is essential. This ranges from developing new tools to tackle serious and organised crime, to sharing best practice, to enable local law enforcement agencies to deliver their own successful operations.

19. UK law enforcement's overseas reach is considerable. Engagement through bilateral relationships, international forums and law enforcement institutions, such as Interpol and Europol, allows the UK to collaborate with partners and coordinate operations across the globe.

20. Deploying liaison officers overseas enables UK agencies to leverage local intelligence and law enforcement assets to counter shared threats. This international presence also supports wider government objectives overseas; for example, contributing to UK efforts to foster good governance, stability and security which can influence UK prosperity.

Trends to 2021

Introduction

21. This section provides an overview of trends, and their underlying drivers and enablers, that could affect the criminal and law enforcement environment in the five-year period to 2021.

22. Crime and law enforcement do not operate in a vacuum, and the complex and overlapping trends in global change will have both direct and indirect implications for both areas.

Technological change

23. Developments in technology, especially information and communications technology, will continue to transform the future crime landscape. Whilst it is possible that there will be an increase in disruptive technology[6] in the next five years, it is more likely that existing trends will continue in some form.

24. By 2021 there will have been an exponential growth in global internet connectivity via the 'internet of things'. Previously offline areas, such as transport, will be integrated via autonomous and semi-autonomous systems. These trends, combined with the continuing growth of the online/digital economy, will increase the opportunities for the entrepreneurial criminal community, at both the cyber-dependent and cyber-enabled ends of the spectrum, to make money. Awareness of cyber crime is growing and there is a risk that as this continues there will be a corresponding drop in the public's confidence in the integrity of the digital economy.

25. There will be a further substantial shift to mobile and portable computing via smart phones and tablets, and criminals – like the public at large – will adopt new methods of communication as they are developed (mirroring the rapid adoption of VoIP platforms and WhatsApp in place of telephony and SMS texting respectively). The increased use of encrypted communications, whilst protecting the data of potential victims, will enable more criminals to communicate more securely.

26. Modern communications technology will increase its global spread, and cyber crime will very likely become more prevalent in countries which lack the capacity and/or capability to mount an effective response. This will increase the number of countries which pose a cyber crime threat to the UK and others, and will bring risks of cyber criminal activity undermining the roll-out of digital capability, and of cyber criminals spreading into more hard-to-reach jurisdictions in search of safe havens.

27. However, technological change will present opportunities as well as challenges; the trends above will stimulate international and public/private sector collaboration which, in responding to the challenge, will be leveraging the capabilities of a multi-billion dollar global industry. Moreover, awareness of the cyber crime threat will be considerably higher than it is today and will be on an upward track. Potential victims should have access to a broader information base on which to adopt appropriate protection, encouraged by means of government and, in part, law enforcement community messaging.

6 A disruptive technology is a technology that displaces an established technology and shakes up the industry or is a ground-breaking product that creates a completely new industry. For example, the PC displaced the typewriter and, amongst other things, changed the way we work and communicate.

Other change

28. In the next five years we can expect to see continuing shifts in global economic power, international trade and relations, combined with the effects of regional conflict and political instability. Nationally and internationally, there will be growth in urbanisation, population increases and, in the UK, changes in demographics (the number of people aged 65 or over is projected to grow by 23% by 2018 compared to 2010).

29. All of this will influence criminal activity in ways which cannot readily be predicted. It is, however, almost certain that political and economic pressures and instability will continue to drive significant levels of legal and illegal migration, globally and regionally. A further driver of migration will be the effects of climate change. It is probable that in the next five years we will experience extreme climate events more regularly, causing people to move – either temporarily or permanently – to more hospitable locations. The concept of climate change refugee is likely to become increasingly accepted.

Conclusion

30. Excluding those crimes created by the introduction of new or changing legislation, it is highly unlikely that we will see any radically different types of serious and organised crime in 2021. It is very likely, however, that we will see existing crime operating in new ways and in new places.

31. Both criminals and law enforcement will need to operate in a faster, more diverse and complex world. Much of this change will be driven by technology. As society becomes increasingly technology-dependent, the implications of both intentional and inadvertent negative behaviour will increase. As technology becomes increasingly autonomous, issues of responsibility and blame will also likely grow in importance. It is highly likely that in the period to 2021 cyber crime will continue to evolve and that much criminal activity, and much of the law enforcement response, will no longer be in the offline real world but online.

32. Global drivers and trends, political, economic or environmental, will increasingly impact on all levels of criminal activity and the associated law enforcement response. Events that previously might have seemed remote and of little consequence will be increasingly significant when viewed in terms of their implications for organised crime.

33. The increase in ethnic and social diversity caused by both migration and generational changes will present a range of challenges and opportunities for both criminal and law enforcement activity. As new risk groups develop, others will potentially decline in significance.

34. Whilst these developments will present a range of challenges the same developments will equally provide opportunities for law enforcement in collaboration with government and industry to tackle serious and organised crime in 2021.

Threat areas and cross-cutting enablers

Child sexual exploitation and abuse

Assessment of current threat

35. CSEA continues to be a prominent national issue with increasing numbers of offenders and victims coming to the attention of law enforcement and children's services. It is specifically recognised as a threat in the National Security Strategy and Strategic Defence and Security Review 2015.

Online

36. The proliferation of IIOC has continued. UK children remain at risk of serious harm from many of those who consume such material and seek to groom children. The NCA Child Sexual Exploitation Referral Bureau receives over 1,800 referrals a month, primarily from industry, compared with 400 a month in 2010. There are indications that the scale of content on open CSEA websites is significant. Law enforcement activity on Tor over the last six months may prompt offenders to seek alternative encrypted access routes to maintain their anonymity. Live streaming of abuse remains a high threat. Self-generated indecent imagery (SGII) by children and young people remains a high threat in terms of proliferation of images and the potential for persistent victimisation.

37. CSEA offenders threaten their victims with the release of explicit photos or comments made by them in order to extort money or further sexual conduct.

38. We are seeing the emergence of younger and more technologically astute offenders using online services, such as the dark web, to protect their anonymity. The use of encryption together with general technological advancement, continue to pose challenges to law enforcement's reactive and proactive capabilities to trace offenders.

Contact Abuse

39. The Children's Commissioner (England) estimates that child sexual abuse in the family environment comprises approximately two thirds of all contact sexual abuse and suggests that around 1.3 million children living in England may have been sexually abused by the time they reach the age of 18. Children are being exploited by criminal gangs as drugs runners, and in some cases they form a relationship with criminals and can become victims of sexual violence.

40. Reported crimes of child contact sexual abuse throughout the UK show a continuing upward trend, despite the likelihood that there is under reporting[7]. The high media interest in both recent and non-recent CSEA investigations together with focused proactive policing operational activity is likely to have contributed to the increase in reported crime. The true prevalence of contact offending in the UK remains unknown.

7 England and Wales 24,278 to 33,183; Scotland 1815 to 2067; and Northern Ireland 758 to 943. Figures are 2013/14 to 2014/15 validated on 31/03/2015. ONS figures contain only crimes where victim age (under 16) was specifically shown in Home Office recorded crime category. There may well be additional sexual offences in the 16 -18 year age range not captured above figures.

Forward look

41. The advancement of technology poses challenges for law enforcement. The practice of live streaming exemplifies how offenders can simultaneously create IIOC, view IIOC and contact abuse by proxy overseas. This convergence across all CSEA threat areas is an indicator of the threat evolving with new technologies.

42. The significant increases in the volume of reported crime, of intelligence generated from industry and of forensics continue to have very significant resourcing implications for law enforcement, with seized media generating intelligence on large numbers of potential new offenders.

43. More of the problem will be visible, driving up demand for law enforcement in the UK and overseas to respond. The challenges posed by technology will continue to require a proactive and agile multi-disciplinary response including in respect of, live streaming, greater use of digital media, new internet applications, and encryption services. There will continue to be a focus on non-recent contact offending.

Organised immigration crime

Assessment of current threat

Into and across Europe

44. Over one million migrants crossed the Mediterranean to enter Europe in 2015, four times as many as in 2014. Numbers remain high in early 2016. There has been an increase in the numbers detected attempting to reach the UK, despite the UK not being the first choice destination for most migrants.

45. We judge that OCGs are not driving irregular migration, but that mass migration attracts criminal individuals and groups. As a result of the implementation of border restrictions by some European countries more migrants are turning to people smugglers for all or part of their journey into and across Europe, and on to the UK. If not controlling the movement of irregular migrants from source country to final destination, some OCGs will coordinate facilitators along the route. Different nationalities have different MOs and levels of sophistication and OCGs tend to be separated on ethnic or nationality lines. Some have recruiting agents in source and transit countries; some advertise their services on social media.

Europe into the UK

46. Numbers of irregular migrants arriving in the camps in France and Belgium increased during 2015. The services of organised or opportunistic criminals may be employed to assist either spontaneous attempts to enter the UK or more sophisticated concealments.

Illegal entry into the UK using false and fraudulently obtained documents

47. False and Fraudulently Obtained Genuine (FOG) documents are used to facilitate irregular migration into the EU and UK by air and other routes.

48. Fewer irregular migrants seek to enter the UK using false documents than clandestinely. This is highly likely to be a reflection of the costs and difficulty in obtaining false documents. However the production and supply of false travel and other documents are key threats. As well as providing false documents some OCGs also help the migrants book travel tickets. The availability of false documents to migrants may drive an increase in the proportion of migrants seeking clandestine entry via these means.

49. There is a market for false European identity cards, and genuine documents are also frequently used by impostors. In addition, false supporting documents continue to be used to make applications for genuine travel documents.

50. For most migrants their journey from source countries to the UK involves overland travel and a sea crossing. However some of the more wealthy migrants use air transport. Iranian OCGs have traditionally moved Iranian nationals by air from Europe into the UK on falsified documents.

Abuse of legitimate means to enter or remain

51. OCGs are thought to be involved in the systematic abuse of the UK visa system. False documents are key enablers in the abuse of various routes to secure legitimate means to remain in the UK.

Forward look

52. Ongoing conflict and instability in the Middle East, sub-Saharan Africa and Afghanistan are highly likely to continue to be push factors for migration. As fears of migration lead to tighter security at national and external EU borders, migrants will be unable to circumvent border controls without assistance and will need to rely more on OCGs. It is highly likely that more OCGs will be attracted to this criminal market.

53. Migrants who arrive in the EU will almost certainly increasingly use the services of people smugglers to attempt clandestine entry into the UK. Migrants who can afford to do so will continue to attempt to travel to the UK using false documents produced and supplied by criminals.

Cyber crime

Assessment of current threat

Scale and cost

54. The October 2015 Office of National Statistics (ONS) analysis of public experience of fraud and cyber crime identified 2.46 million incidents of Computer Misuse Act offences over a 12-month period. However, formal cyber crime reporting through Action Fraud showed a 19% reduction in reports in 2015 to 16,349. Such a disparity reinforces the established view that there remains substantial under-reporting of cyber crime in the UK.

55. The high likelihood of widespread under-reporting affects our ability to make a robust assessment of the cost of cyber crime. HMG and industry are working closely to develop effective measures. The best estimate extrapolated from incomplete data sources would put the annual cost of cyber crime to the UK in the low billions of pounds. This cost of cyber crime includes both the cost of defending against attacks and the financial losses involved with all types of cyber crime.

International criminal threats

56. Sophisticated financial Trojan malware remains a substantial threat to UK and international interests. Direct monetary losses through theft linked to these tools are estimated at tens of millions of pounds, with further hundreds of millions potentially at risk. Three malware products were prominent throughout 2015: Dridex, Neverquest and, until November, Dyreza. Alongside the malware, bespoke criminal tools are now in place to deploy malware against victim systems.

57. Technically-advanced malwares are developed by a small number of international OCGs, with Russian-language groups heavily represented. The location of key crime group members in potentially hard-to-reach jurisdictions for UK law enforcement hinders investigation.

58. International crime groups targeting the UK are highly professional, with defined organisational structures and access to specialist skills and functions. They are agile, adjusting business models at pace in response to technological development such as end-to end encryption, and to law enforcement tactics.

59. These groups use resilient and complex technical infrastructure, much of it located in European Union member states, including the UK, and in North America. Infrastructure is regularly repositioned to hinder investigation and enhance security.

UK criminal threats

60. There are technically-competent criminals active in the UK, engaging in much of the cyber crime now targeting organisations and the public. DDoS for extortion has emerged, in part driven by wider criminal understanding of its potential for profit. The threat from DDoS attacks has also increased, driven by ready access to easy-to-use crimeware tools. Recent ransomware attacks have involved threats to publish victim data online. UK criminals have both the technical competence and the access to crimeware tools required to mount these types of criminal attacks successfully, resulting in financial or reputational damage and harm to an individual.

61. Data breaches against UK organisations have been more widely reported as an area where UK cyber criminals are active. These attacks have compromised personal data and caused short-term financial and reputational damage to victims. A number of attacks took advantage of long standing technical weaknesses for which mitigation was already available. Insufficient or outdated system security continues to leave potential victims vulnerable to attack.

62. There is no intelligence to suggest that UK criminals presently provide coding or other technical services to international malware campaigns. There are, however, examples of international criminals using technical infrastructure located in the UK; and UK-based mule herders organise services in the UK to cash out and move the proceeds of crime.

Criminal markets

63. The criminal marketplace offers wide ranging services to cater for cyber criminals of all levels; from highly sophisticated tools critical to the most technical groups, to commercial services aimed at low-level, unskilled actors. The increasing availability of bespoke, as-a-service operating models also lowers the barrier of entry to emerging criminals.

64. The most competent, highly organised criminal groups often rely on trusted in-house providers for the most critical services and avoid third parties or open forums. This reduces law enforcement's ability to identify and disrupt services key to the criminal business model.

Forward look

65. The establishment of the National Cyber Security Centre[8] is planned for 2016 and will change the architecture of the UK response to cyber crime. Scoping the precise role and remit of this new organisation is underway.

66. It is almost certain that major malware-based attacks launched by international crime groups will continue. It is unlikely that an entirely UK-based group will be able to mount a similar campaign in the foreseeable future.

67. It is almost certain that international crime groups will continue to professionalise their attacks.

68. It is highly likely that the upward trend in data breaches will continue. This will be driven by an expanding criminal marketplace for compromised data and the increase in extortion. It is probable that UK and international cyber criminals will seek to exploit that stolen data.

69. It is likely that the increased threat posed by DDoS and ransomware will continue, with opportunities for international and domestic criminals.

70. The operation of efficient trading forums will likely continue to lower the barrier of entry into cyber crime.

71. The threat to the UK from mobile malware has yet to emerge in significant volume, but remains a likely threat.

72. Technical mitigation will remain an important strand of response, but should be coupled with activity against the crime groups and individual criminals to ensure a long-term disruption.

8 In November 2015 the Chancellor of the Exchequer announced that a national cyber centre (since named as the National Cyber Security Centre) would be established in 2016. The centre will serve as a unified source of advice and support for the economy making it easier for industry to get the support it needs from government and for government and industry to share information on the cyber threat to the UK.

73. The pace of response will need to accelerate and tactical options need to be reviewed and updated in order to keep pace with international crime. Proactive targeting of criminals and infrastructure combined with persistent 4P[9] campaigns against key threat vectors (such as malware, criminal services and DDoS) should deliver a more comprehensive response which begins to reduce the opportunity for criminals to quickly rebuild their capabilities.

74. Law enforcement engagement with industry, a key strand of any effective response to cyber crime, will improve understanding of the threat and leverage unique industry response capabilities.

75. The UK needs to encourage better cyber security hygiene practices by UK businesses and individuals to target-harden vulnerabilities, which cyber criminals will otherwise exploit.

76. Domestically the UK has a maturing framework of response across local, regional and national capabilities. In addition to criminal justice outcomes, collaborative activity going forward between law enforcement and industry against criminals and their enablers can have an extensive and positive impact for UK victims.

9 4P – The '4Ps' refers to the four pillars of Pursue, Prevent, Protect and Prepare in the Serious and Organised Crime Strategy.

Firearms

Assessment of current threat

77. The overall availability of firearms in the UK remains lower than in other western European countries.

78. The UK has influenced EU-level activity including efforts to standardise and tighten firearms legislation. A draft directive aims to introduce common deactivation standards across member states. Proposals have been brought forward to amend the EU weapons directive to restrict the availability of certain firearms, in particular high-powered semi-automatic firearms.

International supply

79. The vast majority of firearms used by criminals in the UK have not been previously discharged, indicating that new firearms enter the criminal marketplace either through international supply or by criminals accessing unused firearms within the UK.

80. In 2015 most seized original lethal purpose firearms and ammunition destined for the criminal market were smuggled in general maritime and Ro-Ro traffic. However individual firearms and component parts continue to be frequently detected in post and fast parcels.

81. The Channel Tunnel, passenger ferry and container ports are the busiest pedestrian and vehicle entry points into the UK from western Europe. Consequently Belgium, France and the Netherlands continue to act as key nexus points for firearms trafficking to the UK. Firearms that are detected crossing through these ports have often originated in eastern Europe and the Balkans. Routes to the UK are varied and dependent on the method used.

Criminal marketplace

82. The country in which a firearm entered the criminal market is often not known. Marketplaces can be dynamic, unfixed and spontaneous dependent on the dominant supply method and networks used at the time.

83. As handguns, submachine guns and assault rifles are prohibited in the UK, it is likely they enter the criminal market outside the UK and are subsequently smuggled into the country. Licensable firearms, such as shotguns and rifles, are more likely to have entered into criminality in the UK through thefts from legitimate holders.

84. As an island, the UK is insulated from the relatively free flow of firearms which exists in continental Europe, and the availability of weapons in the UK is more restricted.

Domestic supply, possession and use of illegal firearms

85. For the first time since 2008, ONS figures show a small rise in the number of recorded offences involving firearms in England and Wales[10].

86. In the UK, firearms are discharged more regularly by urban street gangs[11] (USG) than by OCGs. USGs use firearms in feuds with other gangs, to protect themselves and their criminal enterprises from other criminals (for example, protecting cannabis farms), in the furtherance of their criminality (for example, armed robberies), to intimidate or threaten other criminals, or as status symbols.

Exploitation of legitimate supply

87. Antique firearms, using home-loaded or converted ammunition, continue to be used in criminality. Under existing legislation, antique firearms are exempt from the controls of the Firearms Act, provided they are held as curiosities or ornaments only. There is no requirement for traders to record details of the sale, or for purchasers to hold a firearms' certificate.

10 ONS Statistical bulletin: *Crime in England and Wales: Year ending September 2015*, 21/01/2016

11 See glossary.

Money laundering

88. Money laundering facilitates and enables most types of criminality, the proceeds of which criminals look to use to further their criminality or to increase their personal wealth without detection.

89. Given the potential damage that can be done to the UK's economy, and the importance of its financial services industry, money laundering is viewed as a national security issue and is prioritised in the National Security Strategy. The risk of large volumes of criminal money being laundered through, and invested in, the UK, and the consequential criminal and regulatory penalties by UK, EU and US authorities, could lead to the withdrawal from the UK or potential collapse of major financial institutions. This would likely cause enduring reputational damage to the UK with a loss of global standing.

Assessment of current threat

90. Methodologies vary in complexity from the laundering of small amounts of cash through to professionally supported laundering of many millions of pounds across international jurisdictions. The latter often uses corporate structures set up specifically with obscured beneficial ownership to hide the nature and ownership of the funds.

91. While there are no confirmed figures for the scale of money laundering, the IMF has estimated that money laundering globally represents between 2% and 5% of GDP. This estimate is broadly in line with similar estimates by the UN and the Financial Action Task Force (FATF). If these percentages were applied to the UK economy with GDP at approximately GBP 1.8 trillion, the amount of money laundered would be between GBP 36 billion and GBP 90 billion. In addition UK banks' international subsidiaries will be exposed to money laundering risk from many other countries.

High-end money laundering

92. This is the laundering, wittingly or unwittingly, of large amounts of criminally acquired funds through the UK financial sector and related professional services. It is relevant in particular to the proceeds of major fraud and international corruption where illicit funds pass electronically through the banking system.

93. It can include any or all of:

- the use of corporate structures, nominee directors and company formation agents from multiple jurisdictions to obscure the beneficial ownership of assets;
- the use of tax havens to structure holdings;
- the use of virtual offices;
- investment in high-value goods and property through a network of companies; or
- professional enablers facilitating financial and legal activity.

94. Trade-based money laundering (TBML) is the movement of the value of criminal funds through the manipulation of aspects of licit or illicit trade transactions, such as by third party settlement, over- or undervaluation of goods or falsification of documents. Criminals use TBML to hide the origin of illicit funds while moving their value wherever it is needed, nationally and internationally, to further the criminal enterprise or invest profits.

Cash-based money laundering

95. Cash still plays a major part in the criminal money laundering process. Most criminality generates or uses cash at some level. Even internet-based criminals choose to cash out online proceeds to break the audit trail before re-introducing the cash into the banking system.

96. Criminal cash can be given an appearance of legitimacy by investment in or movement through cash-based, cash-rich businesses. The gambling sector also provides a cash-rich environment which can be used to break the audit trail. In conjunction with formal and informal money remitters physical cash movements form part of the laundering process. A high proportion of these cash movements are managed by a small number of international controllers based in different jurisdictions, mainly in the Middle East and Asia, and supported by networks of collectors and consolidators. In the case of UK criminality these networks operate in both the UK and mainland Europe.

Enablers

97. The skills and knowledge of a variety of professionals, such as accountancy service providers (ASP), the legal profession, estate agents, and trust and company service providers (TCSP), are used by OCGs for sometimes complex money laundering activity. They assist, wittingly or unwittingly, in creating complexity through actions such as setting up networks of corporate structures, acquiring assets to store illicit funds and providing anonymity for the criminal. Their involvement very likely gives transactions an appearance of respectability.

98. ASPs can use their position to provide false documents and records to help criminal groups to hide illicit funds within ostensibly legitimate trade transactions and business takings. Enabling in the legal profession is typified by the abuse of client accounts, the purchase of property and assets and the failure to fulfil the duty to report under money laundering regulations. The involvement of a legal professional in a transaction, and the presumption, therefore, that due diligence enquiries have been completed, may very likely lead to others (for example, banks) not challenging the legitimacy of the funds.

99. TCSPs are often the means by which criminals gain access to corporate structures that mask the true ownership of assets. Networks of such corporate structures can be central to TBML, providing the criminal with end-to-end control of the laundered money, which moves between apparently unconnected entities.

100. Estate agents, particularly those with conveyancing practitioners attached or closely linked, can help the placement of criminal proceeds into the property market. In most instances, though, the responsibility for handling monies and therefore the greater risk lies with the legal profession.

Forward look

101. Cash is almost certain to remain a major part of the money launderer's stock-in-trade with most criminality involving moving, storing or using it at some stage.

102. New payment methods, virtual currencies and mobile payment apps have yet to be adopted to any large degree by money launderers. The potential remains for this area to develop into a major risk.

Bribery, corruption and sanctions evasion

Assessment of current threat

103. The Government's UK Anti-Corruption Plan recognises the threat posed by international and domestic bribery and corruption, which damage national security, economic prosperity and the UK's international reputation.

International bribery

104. Bribery of public and private officials internationally by UK companies and individuals has political, financial, social and environmental ramifications and undermines the UK's ability to promote sustainable growth and to meet its international obligations.

105. Bribery by UK entities is rarely confined to a single country with key actors, business and payments dispersed across multiple jurisdictions. This adds complexity and time to law enforcement investigations, particularly when knowledge of and information about bribe payments is deliberately dispersed. The UK is therefore reliant on initiating and maintaining strong international relationships.

106. International bribery is typically a corporate crime driven by, or with the connivance of, management in businesses of all sizes. In some organisations corrupt behaviour has become entrenched as it is perceived as the only way to win business in certain parts of the world. UK entities which do not engage in bribery and corruption are losing out to international competitors and this adversely affects the economic wellbeing of the UK.

Corrupt politically exposed persons (PEPs) and illicit financial flows

107. Many corrupt foreign PEPs who abuse their position for personal gain choose to launder the proceeds of their corruption into the UK. The full scale of this is unknown, although case studies have shown billions of pounds of illicit money being laundered into and through the UK. The UK property market is a preferred destination for criminal proceeds. Investments are often made via offshore companies, obscuring ultimate beneficial ownership.

108. Recent examples have shown corrupt PEPs to be based in countries from the developing world and areas subject to regime change. It is assessed that systemic corruption within these countries is a significant contributing factor leading to political instability.

International bribery and corruption methodologies

109. UK criminals most commonly use intermediaries to disguise and distance themselves from the transaction when paying bribes.

110. Professional enablers such as solicitors and accountants facilitate bribery and corruption, committed by UK entities and PEPs, through their perceived respectability and integrity. Their expertise is crucial to the laundering of illicit funds internationally and into the UK. It involves drafting of documentation, dissemination of funds, creation of corporate structures, and in some cases acting as intermediaries.

111. Bribe payers and recipients, intermediaries and professional enablers create and use corporate structures such as shell, subsidiary and subcontracting companies to channel bribe payments and the proceeds of corruption, as well as to obscure their criminal activity.

Domestic bribery and corruption

112. There are limited instances of corruption in law enforcement and criminal justice, however when they do occur they have an extremely damaging impact on organisational reputation and public confidence. Information held by law enforcement is of great value to criminals who may use it in a variety of ways, for example to avoid detection, to identify and threaten rivals and to alter the outcome of trials.

Sanctions abuse

113. The UK government adopts a range of UN and EU financial sanctions in support of key foreign policy and domestic counter-terrorism objectives. Sanctions support efforts by the international community to bring pressure on those involved in serious human rights abuses, to prevent the dissipation of misappropriated state assets or to tackle funding for the proliferation of weapons of mass destruction.

114. The prohibitions in place against sanctions targets are robustly enforced. Reporting, however, indicates that individuals will try to circumvent them, motivated at least in part by financial incentives, to obtain or finance otherwise prohibited goods or services.

Forward look

115. When legislation to report beneficial ownership begins to be fully enforced in 2016 the UK will be less vulnerable to shell companies formed by professional enablers and others within the UK for the purposes of enabling bribery, corruption and money laundering. The UK will remain at risk from company formation in overseas jurisdictions where similar legislation is not in place.

116. The UK will continue to be dependent on effective global partnerships to progress bribery and corruption investigations as a significant amount of the criminal activity occurs internationally. Improving and building new relationships remains integral to a successful bribery and corruption strategy. The International Corruption Unit (ICU) has an outreach function which seeks to promote compliance with the UK Bribery Act 2010 and to encourage reporting and allegations of offences under the act. It aims to promote anti-bribery compliance to industry through support of the UK Ministry of Justice Bribery Act guidance and other educational materials, engaging with industry and identifying supporting initiatives.

117. In May 2016 the UK hosted a high-level anti-corruption summit with attendees including G20, OECD members and those countries intent on tackling corruption in their jurisdiction. A number of key deliverables, aligned along the core themes of preventing corruption, tackling impunity and support for victims were discussed. Key participating countries signed a declaration of commitment for the implementation of an International Anti-Corruption Coordination Centre (IACCC). The purpose of this centre is to assist countries to work collectively on grand corruption cases and associated recovery of assets on a global scale. The centre will initially be hosted in London by the NCA, although will remain independent, and is to be operational by April 2017.

Drugs

118. Drug trafficking is a serious threat in its own right, but OCGs involved in drug trafficking are often also involved in a range of other criminal activities. In these cases the drug trafficking commonly funds and underpins those activities.

Assessment of current threat

119. The period of low availability of heroin in the UK, experienced from around 2011 to 2013, is likely to be over. There were 952 heroin- or morphine-related deaths in England and Wales in 2014, a two thirds increase since 2012. This was the highest number of heroin- or morphine-related deaths since 2001[12].

120. Afghan heroin production is decreasing. However, stable purities at the UK wholesale level indicate that this decrease is not having a knock-on effect in consumer markets.

121. Heroin is trafficked by dhow ships from South Asia towards East Africa. Despite numerous high volume seizures in the Indian Ocean, traffickers continue to exploit this route.

122. Turkey is still an important heroin trafficking hub. The Balkans, the Black Sea, and south-eastern Mediterranean are all important onward trafficking routes.

123. The margins between upstream and domestic cocaine kilogram prices generate significant criminal proceeds capable of reinvestment across a range of other threats. Crime associated with cocaine is very often violent and exploitative; it has direct links to the criminal use of firearms, knife crime within criminal gang culture and exploitation of young and vulnerable persons. Cocaine is often perceived not to be an addictive drug and the choice to consume it provides incentive and funding to OCGs to continue to import and supply. In doing so, transport mechanisms and port security are corrupted and impoverished persons are recruited as mules – often with risk to their welfare and lives.

124. Container traffic continues to be a key method of trafficking bulk quantities of cocaine from South America to Europe. The top origin country for container seizures is Ecuador. Belgium is the top destination country for drug shipments in containers.

125. Sailing yachts and other smaller boats are another important method of trafficking bulk quantities of cocaine from South America to Europe. Shipments of this size require high levels of investment and are likely to have been coordinated by well resourced, sophisticated OCGs. The seizure of 3.2 tonnes of cocaine from the MV Hamal, interdicted in the North Sea in April 2015, was the largest seizure of class A drugs in the UK. On the transatlantic route, Cape Verde has emerged as an important hub.

126. West African OCGs have the ability to source bulk quantities of cocaine in South America. Drug shipments are typically broken up in West Africa for onward transit to Europe.

127. Ecuador, Venezuela, Panama, Costa Rica and the Caribbean remain prominent gateways for cocaine to Europe and the UK, with Guyana being particularly significant.

12 ONS (2015) *Deaths related to drug poisoning, England and Wales – 2014 registrations*, 3/9/2014. Available at: http://www.ons.gov.uk/ons/rel/subnational-health3/deaths-related-to-drug-poisoning/england-and-wales---2014/index.html

128. Urban Street Gangs (USGs) continue to play an important role in the distribution of class A drugs (heroin and crack cocaine) into county and coastal towns outside the major big cities where they normally operate. In these scenarios, groups from large cities are taking control of local markets outside the city, supplying high frequency deliveries of mid-market quantities. This form of criminality almost always includes the exploitation of children and vulnerable adults coerced to assist with accommodation and supply.

129. There is a high level of involvement by organised criminals in domestic cannabis production. Many drugs OCGs are involved in cannabis supply in some way, often as a means to fund other criminal activity. There is a crossover between cannabis production and human trafficking, with many examples of victims of trafficking being kept as live-in gardeners on cannabis growing sites.

130. Synthetics (ecstasy and amphetamine) are predominantly supplied to the UK from production in Belgium and the Netherlands with NPS supplied from China and ketamine from India.

131. The following indicates UK law enforcement's prioritisation of countries in terms of the risk posed to the UK either as a source for the production or transit route for the trafficking of drugs:

- High Priority: Colombia, Afghanistan, Turkey, Pakistan, South Africa, the Netherlands, Spain and Albania.
- Priority: Venezuela, Ecuador, Guyana, Eastern Caribbean Islands, Dominican Republic, Nigeria, Ghana, Morocco, Belgium, France, Bulgaria, Romania, Iran and China.
- Significant: Jamaica, Brazil, Panama, Costa Rica, Peru, Guinea, Guinea-Bissau, Senegal, Mali, Mozambique, Tanzania, Kenya, Madagascar, Somalia, Uganda, UAE, Poland, Germany, Portugal, Ukraine, Greece, Republic of Ireland and India.

Forward Look

132. The demand for cocaine by UK consumers is likely to remain high, generating a highly profitable market for international drug traffickers, domestic distribution groups and gangs alike.

Economic crime

Assessment of current threat

133. Serious and organised economic crime affecting the UK frequently involves international networks with an increasing reliance on technology. The impact of economic crime for the UK is far reaching causing financial and reputational damage to the UK economy and individual wealth.

Fraud against the public sector

134. The exact scale of fraud in the public sector is unknown. The last estimate from June 2013 reported fraud against the public sector to be GBP 20.6 billion each year[13]. HMRC estimates that GBP 5.1 billion in annual tax losses is due to organised crime[14]. In addition UK-based criminals are also known to target the public finances of other jurisdictions.

135. Cyber-enabled threats to the public sector vary, involving for example the use of malware, denial of service attacks and targeted phishing.

Fraud against the private sector

136. Complex fraud against the UK private sector can involve losses of hundreds of millions of pounds by businesses but the overall scale is unknown. Private and public sector organisations recorded 241,317 frauds to the Cifas National Fraud Database in the first nine months of 2015 – an increase of 13% from the same period last year. The UK financial sector is a particular target as it processes vast amounts of financial transactions.

137. Threats to the private sector are increasingly cyber-enabled with the use of phishing emails to install malicious software onto computer systems an increasing concern. During 2015 the number of reported data breaches increased. Insiders, who can be exploited wittingly or unwittingly for the purpose of fraud, also present a significant threat to companies.

Fraud against the individual

138. Fraud against the individual is under-reported. Estimates of fraud based on the Crime Survey of England and Wales and released in October 2015 suggested there could have been over 5 million[15] cases of fraud in England and Wales in the last year but only a small percentage was reported to Action Fraud[16].

139. Individuals continue to be targeted through a range of fraud types with techniques constantly evolving. Technology is a key enabler with victims receiving phishing emails that appear to come from trusted sources. Social engineering[17] fraud, where victims are duped into handing over confidential information is an ongoing issue.

140. The changes in pension legislation that took effect in April 2015 have given criminals more scope to target investors with fraudulent or high-risk investment schemes resulting in high individual losses.

---

13 An updated estimate is being produced by an independent third party, with the government represented through a steering group.

14 Organised criminals evade duties on tobacco, alcohol and oils and create fake international supply chains to fraudulently claim or avoid paying VAT (missing trader intra-community (MTIC) fraud). They also continuously target HMRC's online tax/repayment services.

15 Just over half of these frauds resulted in financial loss to the individual.

16 234,123 frauds were reported to Action Fraud in 2014/15 with a total loss of GBP 1.48 billion.

17 Social engineering is the art of manipulating people so they give up confidential information.

Market abuse

141. OCGs involvement in market abuse appears to be increasing with insider dealing remaining the most prominent method. Groups operate across multiple jurisdictions worldwide and profits from the most sophisticated and capable OCGs can be in the high hundreds of millions of pounds a year. The UK is a key location for these networks as certain derivative products are only available through UK firms.

142. Recent prosecutions, such as for the LIBOR rate manipulation, have highlighted the potential for large-scale abuse. Cyber-enabled market abuse is an emerging threat involving network intrusion techniques to obtain confidential market sensitive information. Whilst we are currently aware of data breaches of US firms it is highly likely that UK entities have also been targeted.

Intellectual property crime

143. Trading in counterfeit goods is estimated to cost the UK economy at least GBP 1.3 billion per year in lost profits and taxes, but the true scale is unknown. This is believed to be a growing threat involving OCGs that are also committing other serious crimes. There are indications that the trade in counterfeit goods, like other criminal activity, is also used to raise funds for extremist groups and terrorism.

Forward look

144. A new Joint Fraud Task Force has been launched which will combine the work of law enforcement, government and all of the main banks and other financial institutions to help protect the public from becoming victims of fraud and to improve the collective response to and understanding of the fraud threat.

145. In the last year, HMRC's response in tackling organised criminals has made it more difficult for fraudsters to successfully target the UK. The introduction of a new chemical marker, for example, will make it difficult to launder rebated fuel. In addition, HMRC have changed the VAT charging process, introducing reverse charges[18] in 2015/16 for high-risk sectors which have stopped MTIC fraudsters targeting the UK within these sectors.

146. The threat from cyber-enabled fraud is likely to increase with the growth in the use of online access to financial and public sector services.

147. The planned introduction of polymer banknotes in the UK and security changes to the pound coin are likely to reduce the threat from counterfeit currency, at least in the short term.

148. Advances in technology and the use of social media have helped criminals develop more sophisticated ways of targeting the private sector. Social engineering techniques, as well as the spoofing or hacking of emails, used by criminals as a means to convince individuals to divert funds, continue to evolve. This will present a challenge to law enforcement to keep up with these changes and develop the innovative techniques required to counter them.

18 The VAT cost is transferred from the person making a sale to the person receiving the sale.

Modern slavery and human trafficking

Assessment of current threat

149. Coercion, violence, threats and deception are used to manipulate and control victims of modern slavery and human trafficking. OCGs and opportunistic individuals are involved in this type of criminality, primarily for profit.

150. The number of potential victims referred to the NRM continues to rise. In 2015 there was a 40% increase on 2014 to 3,266, largely a reflection of increased awareness and interventions by law enforcement and non-governmental organisations. Many victims are unwilling or unable to come forward and the true extent of this criminality is almost certainly much greater than the NRM data suggests[19].

151. Adult labour exploitation and adult sexual exploitation remain most prevalent forms of exploitation referred to the NRM. NRM referrals relating to labour exploitation continue to increase. Though we cannot rule out a greater incidence rate, it is likely that this is as a result of greater awareness and increased law enforcement activity.

Trafficking of adults for labour exploitation

152. The trafficking of adult victims into conditions of labour exploitation continues to increase (by 53% from 2014 to 2015), surpassing sexual exploitation. Labour traffickers operate across the UK and exploit workers in low-skilled areas of work such as nail bars, car washes, cleaning services, seasonal agricultural work and off-shore fishing. Victims' wages, as well as any state benefits fraudulently claimed in their names by traffickers, are paid into bank accounts controlled by traffickers.

Trafficking of adults for sexual exploitation

153. The trafficking of adult victims into conditions of sexual exploitation also continues to rise (by 28% from 2014 to 2015).

Trafficking of children and young adults for all forms of exploitation

154. The trafficking of children and young adults under 18 into forms of exploitation (including sexual exploitation, domestic servitude, labour or criminal exploitation) within, into or through the UK is also a major threat. Referrals into the NRM relating to the exploitation of minors increased by 46% from 2014 to 2015[20]. Due to existing safeguarding procedures the number referred to the NRM is likely to be a fraction of those encountered and investigated by law enforcement[21]. The duty introduced by the Modern Slavery Act 2015 to refer suspected cases of trafficking of under-18s should increase reporting.

155. Traffickers often work across boundaries and jurisdictions, requiring a collaborative response by UK and international law enforcement, government and NGOs.

156. The UN estimates that, globally, modern slavery is one of the most profitable criminal activities[22]. Targeting the money flows could significantly disrupt it: the Modern Slavery Act

19 Professor Bernard Silverman, Chief Scientific Advisor to the Home Office (November 2014), 'Multiple Systems Estimates and Human Trafficking'.

20 According to NRM yearly reporting figures rose to 982 in 2015 from 671 in 2014.

21 In CSE cases where trafficking is an element, not all potential victims are referred to the NRM.

22 UN ILO (International Labour Organisation) report from 2014 – http://www.ilo.org/global/topics/forced-labour/lang--en/index.htm

2015 allows law enforcement to seize cash and assets from traffickers under the Proceeds of Crime Act.

157. The Modern Slavery Act 2015 enables the courts to restrict the activities (for example, travel) of those involved in or convicted of modern slavery offences, through prevention and risk orders.

158. Analysis of data from previous years indicates that approximately 50% of NRM referrals receive a negative outcome, with the referred individuals not deemed to be victims of modern slavery.

Forward look

159. The increase in irregular migrants into the EU, some of whom will enter the UK, is highly likely to increase the pool in the UK of those vulnerable to exploitation by criminals. Human traffickers will be able to move refugees who obtain EU passports easily within the EU.

Organised acquisitive crime

Assessment of current threat

160. The key threats under OAC are organised vehicle crime, commercial robbery, commodity crime[23] and wildlife crime. The majority of OCGs involved in OAC operate across a broad range of other criminal activities.

161. OAC offenders are often also active between regions, challenging law enforcement coordination. FNOs and criminals from within the traveller community are commonly involved in OAC.

162. An upward trend in motor vehicle theft, often as a precursor for other criminality, has been observed in the majority of regions. Electronic compromise[24], a theft MO aided by the availability of enabling technology, is particularly prevalent in London. Stolen high-value vehicles and plant machinery are frequently exported to overseas markets.

163. The number of ATM attacks has increased, along with financial losses. Plant and other vehicle theft is often an enabler for ATM offending.

164. Use of violence and weapons is common to cash and valuables in transit and high-value gold/jewellery offending.

165. Available figures indicate that metal theft is on the decline. It is a realistic possibility that this trend will continue to reflect falling global commodity prices.

166. The illegal international trade in endangered species is facilitated by UK criminality.

Forward look

167. An ongoing assessment of the national nature and scale of the electronic compromise of vehicles will inform the public and private sector response.

168. The theft of leased vehicles through fraud is potentially an emerging issue.

169. Under the Illegal Wildlife Trade (IWT) Challenge Fund, up to GBP 5 million in UK funding will be made available in 2016 to support global initiatives to tackle the trade in rhino horn, elephant ivory and other IWT items and products.

170. An updated strategic assessment has been commissioned to better understand the threat posed by heritage and cultural property crime.

171. There are a variety of multi-disciplinary working groups, including with the private sector, which address the broad range of OAC threats. Such public-private collaborative approaches will become increasingly valuable.

23 Now includes metal theft.

24 Various forms of vehicle theft by technical means and without the use of a legitimate key; for example, generic jamming, lock-breaching, key cloning and re-programming technology.

Border vulnerabilities

Assessment of current threat

172. Many forms of serious and organised crime require circumvention of the UK border to some degree. Criminals have continued to demonstrate that they are capable of adapting to changes in law enforcement activity at the border.

173. The consequences of this criminal exploitation may be felt throughout the public and private sectors, undermining or destroying legitimate business, communities and trade.

174. Corrupt workers within both the private and public sector facilitate the movement of illicit goods into the UK and the circumvention of border controls by irregular migrants.

175. The coastline of the UK and its principal islands extends for more than 19,000 miles, and includes thousands of ports, marinas, inlets and bays. The UK is also serviced by in excess of 3,000 private airfields. Criminals use yachts, tug boats and other small vessels, as well as light aircraft, to facilitate the smuggling of illicit commodities into the UK.

176. Border controls at UK ports have been improved in response to increasing levels of attempted clandestine entry (the mass migration encountered during 2015 exceeds levels previously seen). However, criminal groups continue to develop new methods for concealing the movement of illicit commodities and people in order to avoid detection.

177. More than 2.3 million tonnes of air freight enter the UK annually, including consignments weighing hundreds of kilograms. Air freight enables goods to be shipped quickly between countries, especially relative to other freight modes. The smuggling of illicit goods within legitimate consignments is a method that continues to be used by criminals.

178. The number of passengers arriving in the United Kingdom increased from 108 million in the twelve months to the end of August 2014 to 121 million in the twelve months to the end of August 2015. Document abuse occurs across all passenger modes including Ro-Ro, rail and air travel.

Forward look

179. OCGs are highly likely to continue adapting to improved port controls at Calais and Coquelles and it is likely that their activity will be displaced to other locations on the near continent.

Criminal use of identity

180. Identity crime, encompassing identity theft and document abuse, facilitates serious and organised crime across a wide range of threats, making it a prevalent cross-cutting issue.

Assessment of current threat

181. FOG or false documents are used extensively for immigration purposes, to facilitate crime and to hide criminal assets. As well as being an enabler for a range of illicit activity, these documents are themselves valuable commodities that provide a low risk/high profit to those producing and supplying them.

182. The production and supply of false documents are key enablers for migrants looking to illegally enter or remain in the UK. The industrialisation of the process means that they can be produced on a mass scale.

183. Criminals use FOG or false documents to acquire further identity documents. Some criminals may use multiple false identities to avoid or to reduce the risk of law enforcement detection. However there has been an increase in detection levels of identity crime at the application stage due to improvements in prevention messaging, processes and data sharing.

184. Despite the increased use of internet-based applications and services, for example mortgage applications, physical documents remain critical to identity confirmation.

185. The supply of false or genuine documents online occurs mostly on the dark web, though also on the open internet. It is believed that open sites offering false documents for sale are largely scams.

186. Personal data is also a valuable commodity as highlighted by recent online bulk data breaches of companies. The scale of cyber-enabled identity crime is believed to be increasing, in part due to the magnitude of data available online. Data is harvested and then used for criminal identities or to commit fraud.

Forward look

187. The move to largely paperless online processes in the financial sector and other public services is likely to provide greater opportunities for criminals to commit fraud using false or abused documents. As online processes are strengthened in reaction to this, higher quality false documents are likely to become more valuable, with greater profit coming from their production or acquisition.

188. The extent of identity crime is very likely to increase due to criminal mass production of false documents. Multi-agency initiatives will be imperative in combatting this.

189. Greater collaboration and knowledge sharing between agencies would assist in building the intelligence picture on criminal use of identity.

Criminal use of internet technology

190. The use of the internet continues to revolutionise the way we communicate and conduct business. Surveys indicate around 80% of the UK population now use the internet daily. Criminals – irrespective of their crime area – will follow this trend, using a variety of online services, on the open internet and the dark web, both as part of their daily lives and to facilitate their crimes.

191. This chapter focuses on those internet technologies criminals use to increase the scale of their activity, to improve anonymity, and to access criminal services and trade in commodities; that is, mainly, encryption, the dark web, and virtual currencies. These technologies are changing the landscape of traditional criminal activity. This chapter will focus on the technologies themselves, rather than their specific use in relation to particular crime types.

192. It should be noted that criminal use of internet technologies not covered here includes:

- The use of internet technologies for everyday business (e.g. to book travel, send messages) to support criminal activity. Criminals in this category tend to benefit from secure by design technologies (those that allow businesses and the public to secure or anonymise their communications, transactions and data);
- criminality which is solely dependent on the internet, e.g. hacking, which is covered in the cyber crime chapter.

Assessment of current threat

193. **Encryption**: There are indications of a considerable increase in the use of encrypted communications by criminals across all threat areas and across all levels within crime groups, which can impact on our ability to gather evidence from devices seized as a result of arrests. Criminal uptake of encrypted communications is part of a broader trend of encryption as a default in everyday commercial services, although criminals also seek out PGP (Pretty Good Privacy) devices, reflecting a concerted demand for secure products. Some storage devices are also now encrypted by design.

194. **Dark web**[25]: Within the dark web, individuals can both host and visit services anonymously. Criminals currently prefer Tor hidden services, but I2P and Freenet are also used to facilitate criminality, and other decentralised networks are in development.

195. Within Tor, a variety of cross-commodity marketplaces trade in illicit goods. The size of the overall marketplace has increased dramatically since 2013, growing from three markets to around 30 markets as of January 2016.

196. Drugs remain by far the main commodity being sold on dark web markets, although there is an increasingly diverse set of commodities being offered. Firearms represent a small percentage of dark web sales, although the risk presented remains high. Identity and Government Gateway credentials (both used for repayment fraud against HMRC), identity documents, compromised credit card data and cyber crime tools are also offered for sale.

25 A darknet is a network where connections are only made between trusted peers using non-standard protocols and requiring specific software/configurations/authorisations to access it (e.g. Tor). The dark web refers to the website content hosted within darknets. "Hidden services" is a Tor specific term for services, including websites that are provided within the Tor network. The Invisible Internet Project (I2P) and Freenet are darknets also used to host services.

197. The CSEA community on Tor hidden services is very distinct from marketplace activity, with IIOC considered a red line within the general marketplaces. Research indicates that although the number of CSEA-related hidden services sites is very low, the traffic to these sites dwarfs that of traffic to other services, including the marketplaces.

198. Criminals are increasingly aware of law enforcement tactics online, and, in addition to the anonymity that Tor affords, criminals are now employing additional protection such as encryption, as well as the use of Tails[26] and Bitcoin tumblers, to bolster their security within this environment. Within the cyber area, some criminals have switched to using Tor and I2P to obfuscate their botnet command and control infrastructure.

199. **Virtual currencies**: Virtual currencies have a growing place within the legitimate sector, although the regulatory climate is still evolving. For criminals, trusted, anonymous payment systems are a key enabler for dark web trade as well as cyber crime extortion via ransomware and DDoS. Bitcoin remains the virtual currency of choice.

Forward look

200. While encryption, virtual currencies and darknets like Tor are legitimate products welcomed by consumers, they can also benefit criminals. Undermining criminal exploitation of these technologies has the potential to impact across multiple threat areas, so requires a coordinated approach. This should include targeting those criminals providing the services and infrastructure, building capabilities to keep pace with the threat and working with industry and regulators in relation to security by design.

201. **Encryption**: Encryption will continue to be offered as standard within products, and criminal use will increase in line with this.

202. **Dark Web**: Change in legislation around NPS in May 2016 effectively banning so-called 'legal highs' is likely to see a large increase in these drugs being offered through the dark web instead.

203. **Virtual currencies**: The Home Office is now leading a working group focused on digital currencies which will seek to address knowledge and skills' gaps across the law enforcement community. Successful management of this issue will lead to enhanced capability across a number of crime types providing a stronger evidential process and an increased chance of successfully seizing criminal proceeds within Bitcoin.

26 Tails is a live DVD or live USB that routes all connections to the Internet through the Tor network. It leaves no trace on the computer unless explicitly requested, and it uses state-of-the-art cryptographic tools to encrypt files, email and instant messaging.

Foreign national offenders

Assessment of current threat

204. There are foreign national offenders (FNO) involved in most areas of criminality that impact on the UK, in particular drugs and firearms smuggling, immigration crime, human trafficking, document forgeries and CSEA offences. They have also often been important in developing new areas of criminality and responding flexibly to market demands. FNOs in the UK are also potentially able to use personal connections to criminal enterprises abroad to facilitate their offending in the UK.

Forward Look

205. The approach to FNOs thus far has assessed a wide range of individuals involved in serious crime that are known to law enforcement. In future, this work will be more targeted towards the most serious and impactful OCGs, identifying the key figures within these groups, to establish what immigration disruption options may be available and appropriate. Work will continue on expanding information sharing between key departments and agencies, such as the Home Office, the NCA, regional and international partners to prevent serious criminals from entering or re-entering the UK and committing crime here.

Prisons and lifetime management

Assessment of current threat

206. Some organised criminals continue to offend whilst in prison. Illicit communication devices, corruption and coercion are key enablers to this activity. The continuation of criminal activities from prison is potentially harmful to the public. It also damages the reputation of prison as the UK's ultimate sanction against criminal activity and consequentially erodes its deterrent effect.

207. In September 2015 there were just over 6,000 prisoners associated with OCGs in England and Wales, approximately 1,000 of whom had been members of priority or high priority groups. This is approximately 7% of the prison population in England and Wales as a whole. As examined in a recent study on the pathways into serious and organised crime, this high concentration of varied offenders in close proximity facilitates the maintenance of existing groups, the forming of new networks, and the identification of experienced offenders to enable future crimes[27].

208. The NCA recently carried out research into investigations of OCGs involved in drugs trafficking that had been facilitated by an individual in prison. In each case under review, the common factor was that the prisoner had access to an illicit mobile phone. This strongly suggests that the availability and use of illicit mobile phones within prison is a key enabler for serious and organised criminals to continue their involvement in crime.

209. NPS are being used in prisons. Further intelligence is needed in order to assess the extent to which the supply of these substances may be linked to organised crime.

210. The NCA is working with partners to identify commonalities amongst prisoners who continue to be involved in serious organised crime whilst in prison. This includes a demographic of the offenders identified and common enablers and methodologies.

211. Current engagement between NOMS and NCA CEOP Command concentrates on specific issues relating to CSEA offenders. Initial work has been agreed to assess the extent to which these offenders network in prison to increase their ability to carry out crimes.

Forward look

212. The Ministry of Justice predicts an increase in the prison population over the next five years as a result of more serious cases, including sexual offences, coming before the courts and offenders receiving longer custodial sentences[28].

213. Section 80 of the Serious Crime Act 2015 provides that regulations can be made to prevent or restrict the use of communication devices in custodial institutions using telecommunications restriction orders. There will be no requirement to firstly take possession of the device before making an application. These new powers will add to and improve existing measures to tackle unauthorised mobile phone use in prisons.

214. The National Prison Intelligence Coordination Centre was launched as a multi-agency response to better understand, manage, and disrupt the threat posed by high priority offenders in prison. It will lead a programme to strengthen regional and local prisons

27 0217-HO: Pathways into Serious and Organised Crime (OFFICIAL), February 2016.

28 Projection of sentences from Ministry of Justice published Prison Population Projections 2015-2021, https://www.gov.uk/government/statistics/prison-population-projections-ns for that and more data.

intelligence capabilities. It brings together counter-terrorism and organised crime expertise and capabilities:

- to develop a comprehensive picture of the threat;
- to identify and manage the cohort of offenders who represent the highest risk of harm to national security and public protection;
- to ensure the effective collection, use, and management of intelligence relating to that cohort of offenders; and
- to provide oversight and direction of law enforcement assets in prisons.

215. The Home Office, together with national, regional, and local partners, is developing guidance to improve the lifetime management of high harm offenders across the country. The guidance will draw on best practice from around the country to provide detail and clarity on roles and responsibilities for partner organisations, highlighting the range of powers available to disrupt offenders and examples of how they can be used. This will ensure that NOMS, law enforcement, probation, and other partners use the full suite of powers available to keep the public safe.

216. Data sharing agreements between the partners will enable further intelligence sharing which will help to identify foreign nationals involved in serious organised crime. Once identified, steps can be taken to ensure that risks they may represent are managed appropriately both in the UK and abroad.

Glossary

ACRO	ACPO Criminal Records Office. Founded in 2006 following a decision by the then Association of Chief Police Officers (now replaced by the National Police Chiefs Council (NPCC)) to establish an operationally focused unit that would organise the management of criminal record information and improve links between criminal records and biometric information.
Action Fraud	Action Fraud is the UK's national fraud and internet crime reporting centre.
ASP	Accountancy service provider
Bitcoin tumblers	An online service used to mix an individual's Bitcoin funds with other Bitcoins in order to confuse the fund's original source.
Botnet	A network of private computers infected with malicious software and controlled as a group without the owners' knowledge. Can be used to send out spam for example.
Contact sexual abuse	Any physical sexual contact with a child in person; the opposite of non-contact **CSEA**, which includes grooming, non-contact exploitation and persuading children to perform sexual acts via the internet.
Cifas	A UK fraud prevention service.
Crimeware	Crimeware is a class of **malware** designed specifically to automate cyber crime.
CSEA	Child sexual exploitation and abuse (cf. **IIOC**, **OCSE** and **TCSO**).
Cyber-dependent	Cyber-dependent crimes are crimes such as the creation, dissemination and use of **malware** for financial gain, hacking to steal personal or industry data and denial of service attacks to cause reputational damage. They require the use of computers, computer networks or other forms of information communications technology.
Cyber-enabled	Crimes such as fraud, child sexual exploitation and the purchasing of illegal drugs can be conducted online or offline. Where they are conducted online they are described as cyber-enabled.
Darknet	A darknet is a network where connections are only made between trusted peers using non-standard protocols and requiring specific software/ configurations/authorisations to access it (e.g. **Tor**). The **dark web** refers to the website content hosted within darknets.
Dark Web	A subset of the **hidden internet** comprising the content of websites that are publically accessible but which hide their servers' IP addresses using anonymity software, such as **Tor**. Like the **hidden internet** this material is not necessarily criminal (e.g. anonymous news submissions) but criminals do take advantage of the difficulty in identifying sites' origins and the dark web is used to host illegal online marketplaces.
DDoS	Distributed denial of service attack: multiple compromised systems – usually infected with a **Trojan** – are used to target one system causing a denial of service attack. This generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the internet, typically on high-profile web servers, such as banks or credit card payment gateways.
End-to-end encryption	A method of secure communication that prevents third parties from accessing and reading data along the entire route while it is being transferred from one system or device to another.
FATF	Financial Action Task Force. The FATF is an intergovernmental organisation founded in 1989 on the initiation of the G7 to develop policies to combat money laundering. In 2001 the purpose expanded to act on terrorism financing. It monitors countries' progress in implementing FATF recommendations by peer reviews of member countries
FOG documents	Fraudulently obtained genuine documents.

Freenet	The Free Network, an internet anonymisation programme.
General maritime	This includes vessels such as yachts, tugs, rigid hull inflatable boats (RHIBs), small motor boats, and small commercial vessels used solely for smuggling purposes.
Hidden internet	The hidden internet (or deep web) is the portion of the worldwide web that is not indexed by standard search engines and constitutes approximately 96% of the entire web. In most cases, this is not for sinister reasons and is simply due to the sheer size of the internet. The **dark web** is a subset of the hidden internet.
I2P	The Invisible Internet Project, an anonymisation programme.
ICU	International Corruption Unit.
IIOC	Indecent images of children: offences include the possession, taking, making, distribution and sharing of indecent photographs of minors. These can include moving images and pseudo-photographs (e.g. computer generated images that look like photos).
Internet of things	'The internet of things' describes the interconnection of uniquely identifiable embedded computing devices with the existing internet infrastructure. Connection to the internet is being designed into more and more devices in the home and those affecting our daily lives. Examples include microchips for animals, heart-monitoring implants and built-in sensors for cars.
LIBOR	The London Interbank Offered Rate is the average of interest rates estimated by each of the leading banks in London that it would be charged were it to borrow from other banks. It is usually abbreviated to LIBOR, or more officially to ICE LIBOR (for Intercontinental Exchange LIBOR)
Malware	Malicious software. Software specifically designed to disrupt or damage a computer system.
MTIC fraud	Missing Trader Intra-Community VAT fraud. **MTIC** fraud is the theft of VAT from a government by criminals who exploit the way VAT is treated within multi-jurisdictional trading, where the movement of goods between jurisdictions is VAT-free. The fraudster charges VAT on the sale of goods and then absconds instead of paying it to the government.
Mule herder	A mule herder (or drop organiser) coordinates the realisation of criminally acquired funds. The individuals they employ are referred to as mules. A mule (or drop) is a holder of a means of payment who, on command from the mule herder or drop organiser, cashes the money received into their/an account, or transfers it to another account as specified by the mule herder.
National Cyber Security Centre	In November 2015 the Chancellor of the Exchequer announced that a national cyber centre would be established in 2016. It has since been named as the National Cyber Security Centre. The centre will serve as a unified source of advice and support for the economy making it easier for industry to get the support it needs from government and for government and industry to share information on the cyber threat to the UK.
NPICC	National Prison Intelligence Coordination Centre
NPS	New psychoactive substances. Commonly known as legal highs, these are drugs designed to mimic the effects of illegal drugs, but are sufficiently structurally different to avoid being classified as illegal substances. This, however, does not necessarily make them safe to use.
NRM	National Referral Mechanism. The NRM is a process set up by the Government to identify and support victims of trafficking in the UK.
OAC	Organised acquisitive crime: consists of organised vehicle crime, commercial robbery, commodity crime and wildlife crime

OCSE	Online child sexual exploitation: use of the internet to offer a child or an exploitative third party 'something' (e.g. money or a service) in exchange for the performance of sexual acts, either by or on the child.
Original lethal purpose	A firearm originally manufactured with lethal purpose as opposed to weapons converted to be capable of live firing with lethal effect.
PEP	Politically exposed person. There is no fixed definition, but in financial regulation PEP describes someone who has been entrusted with a prominent public function, or an individual who is closely related to such a person. A PEP generally presents a higher risk of involvement in bribery and corruption due to their position and influence.
PGP	Pretty Good Privacy. A data encryption and decryption programme that provides cryptographic privacy and authentication for data communication.
Phishing	An attempt to get users to divulge sensitive information, such as credit card details and login credentials, by masquerading as a legitimate company or person. This is mainly done through emails, instant messages or websites that are designed to look genuine.
Ponzi fraud	Ponzi schemes are 'get rich quick' investment scams which claim to pay returns to investors from their own money, or from money paid in by subsequent investors. There is no actual investment scheme as the fraudsters siphon off the money for themselves.
Ransomware	Malicious software which prevents a victim from using their computer or from accessing their files, unless they pay a ransom to the attacker.
Ro-Ro	'Roll-on, roll-off' ports tend to service freight vehicles and some passengers and subject them to very limited controls.
SGII	Self-generated indecent imagery.
Shell company	A non-trading company with a separate legal entity with little or no assets and no physical presence in the state of incorporation.
Sinkholing	A technique used to redirect internet traffic away from criminal control often with the assistance of industry partners.
Tails	Tails is a live DVD or live USB that routes all connections to the Internet through the **Tor** network. It leaves no trace on the computer unless explicitly requested, and it uses state-of-the-art cryptographic tools to encrypt files, email and instant messaging.
TBML	Trade-based money laundering: an alternative remittance system that allows illegal organisations to earn, move and store proceeds disguised as legitimate trade. Value can be moved through this process by false invoicing, over-invoicing and under-invoicing commodities that are imported or exported around the world.
TCSO	Transnational child sex offender: an individual who travels overseas to commit sexual offences against children.
TCSP	Trust and company service providers. Examples of the services provided by TCSPs include: • forming companies or other legal persons • acting as a director or secretary of a company • acting as a partner (or in a similar position) for other legal persons • providing a registered office, business address, correspondence address or administrative address for a company, partnership, or other legal person or arrangement

Tor	The Onion Router is free software for enabling online anonymity and resisting censorship. It is designed to make it possible for users to surf the internet anonymously, so their activities and location cannot be discovered by government agencies, corporations, or anyone else.
Trojan	A type of computer programme that hides or disguises another programme usually designed to do harm to the system on which it runs.
Urban street gang	There is no formally agreed definition of an urban street gang (USG). However a January 2016 Home Office study into USGs – 'Local perspectives in Ending Gang and Youth Violence Areas: Perceptions of the nature of urban street gangs' – used the following definition. "A relatively durable, predominantly street-based group of young people who see themselves (and are seen by others) as a discernible group, and engage in a range of criminal activity and violence. They may also have any or all of the following features: identify with or lay claim over territory; have some form of identifying structural feature; are in conflict with other similar gangs."
Virtual currency	Virtual currencies were defined in 2012 by the European Central Bank as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community".
VoIP	Voice over Internet Protocol. VoIP is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks, such as the internet.
WhatsApp	An internet communication service using **end-to-end encryption** enabling the exchange of text and voice messages and images.