

National Strategic Assessment

of Serious and Organised Crime

2018



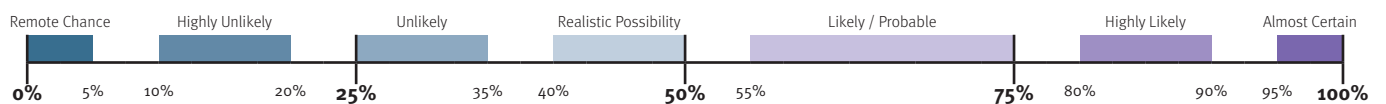


Contents

Foreword	5
Introduction	6
Profile of Serious and Organised Crime	7
Overview of SOC in the UK	8
Pathways into SOC	9
The Global Perspective	10
SOC in Scotland	11
SOC in Northern Ireland	13
Horizon Scanning: Trends to 2023	15
Cross-Cutting Threat Enablers	17
Use of Technology in SOC	18
Vulnerabilities at the UK Border	20
Prisons and Repeat Offenders	21
Corruption within the UK	23
VULNERABILITIES	24
Child Sexual Exploitation & Abuse	26
Modern Slavery & Human Trafficking	30
Organised Immigration Crime	34
PROSPERITY	37
Money Laundering	38
Fraud and Other Economic Crime	41
International Bribery, Corruption & Sanctions Evasion	44
Cyber Crime	46
COMMODITIES	50
Firearms	51
Drugs	54

Probability and Uncertainty

Throughout the NSA, the ‘probability yardstick’ (as defined by the Professional Head of Intelligence Assessment (PHIA)) has been used to ensure consistency across the different threats and themes when assessing probability. The following defines the probability ranges considered when such language is used:



Foreword

from the Director General of the National Crime Agency

I am proud to introduce the National Strategic Assessment of Serious and Organised Crime for 2018. We, at the National Crime Agency, are ambitious in our endeavours to lead the fight to cut serious and organised crime and this intelligence-based assessment builds on those previously issued, providing the most comprehensive analysis yet of the threats facing us.


Against a backdrop of a growth in the volume and complexity across the threats, this assessment highlights:

- the non-geographic locus of many threats;
- the emergence of the dark web as an enabler;
- a revised focus on illicit financial flows;
- the overlaps between the threat areas;
- the impact of technology; and
- a rapidly changing picture in some areas.

This requires us to think differently about how we build capability in response and one of the purposes of this assessment is to inform that necessary strategic refocus. This includes our ambition to build a new National Data Exploitation Capability (NDEC) to deliver a central, sophisticated data exploitation response; develop a world-class response to economic crime through a multi-agency National Economic Crime Centre (NECC) - hosted by the NCA - bringing together the public and private sectors more closely than ever before; and to create an expanded multi-agency National Assessments Centre (NAC) to articulate a deep and comprehensive understanding of the SOC threat.

Fundamentally it must also shape our operational response and we will continue to build on the outstanding operational results of the last year as we undertake investigations at the high end of high risk. In doing so, we value the support of our operational colleagues with whom we work (often in support of one another) as they help us achieve this.

I trust this assessment is useful to colleagues across central Government, Police and Crime Commissioners, operational law enforcement partners, security services and the private sector in that regard. It has been drafted with the support of colleagues across many organisations based on their experiences and the intelligence gained from them. There is no doubt that we can only protect the citizens of the UK if we continue to rise to these new and changing challenges together.



Lynne Owens CBE QPM MA



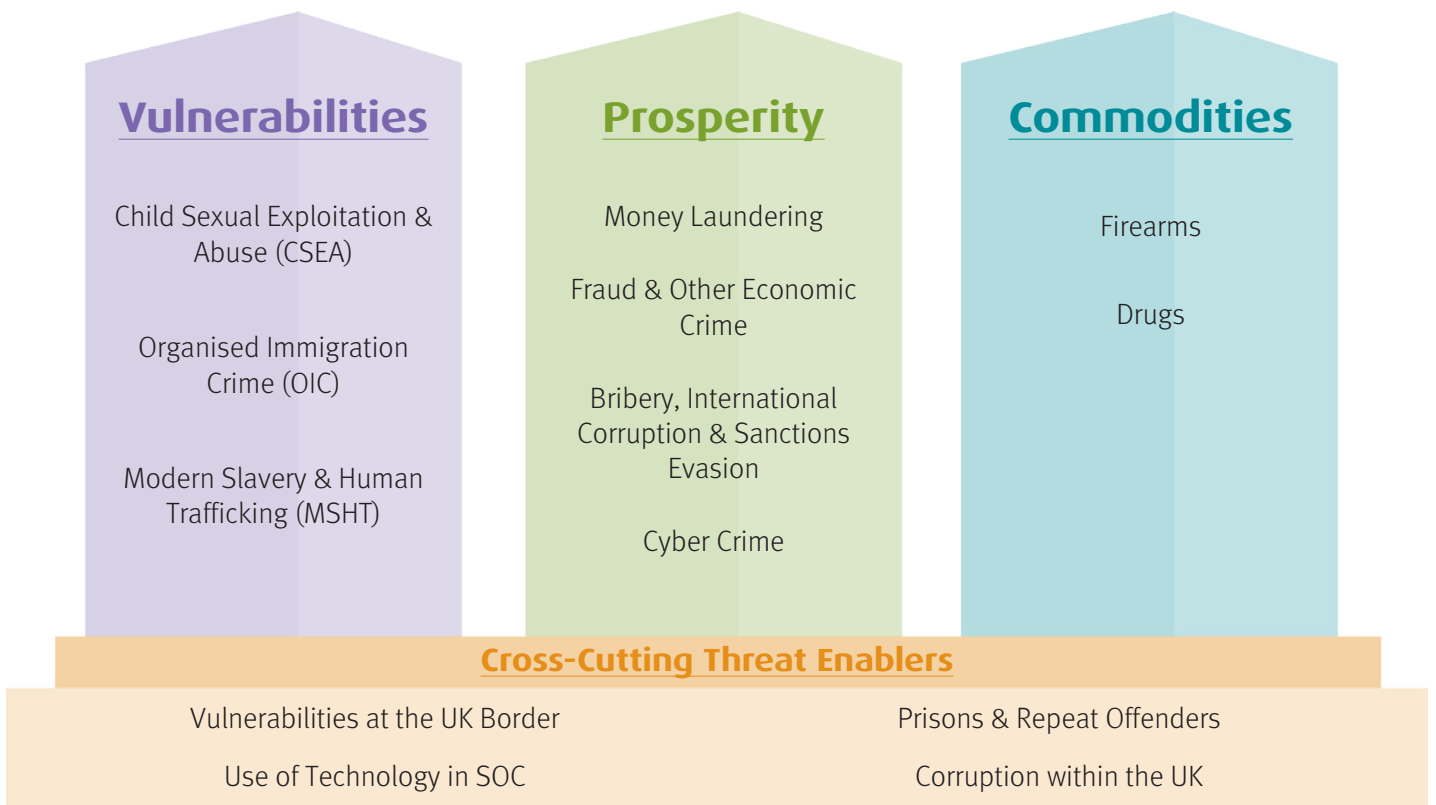
Introduction

The National Strategic Assessment (NSA) provides a single picture of the threat to the UK from 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).

On behalf of UK law enforcement, the NCA's National Assessments Centre (NAC) has articulated the threat in this NSA. The preparation of this document involved wide consultation across the law enforcement community and its partners, including (but not limited to):

- National Crime Agency
- Police forces in England and Wales
- Police Service of Northern Ireland (PSNI)
- Police Scotland
- Regional Organised Crime Units (ROCU)
- Border Force
- Immigration Enforcement
- Her Majesty's Revenue & Customs (HMRC)
- Her Majesty's Prisons & Probation Service (HMPPS)
- Serious Fraud Office (SFO)
- Crown Prosecution Service (CPS)
- Cabinet Office
- Home Office
- Foreign & Commonwealth Office (FCO)
- MI5, JTAC, SIS and GCHQ

In order to coordinate response to the threats under its remit, the NCA has grouped the threats together into three 'pillars' of response (Vulnerabilities, Prosperity, Commodities), with aspects which cut across multiple threats captured separately. The NSA is structured to reflect the threat under these groupings.





Profile of Serious and Organised Crime

Overview of SOC in the UK

1. Serious and organised crime affects more UK citizens, more often, than any other national security threat. It has a daily impact on the UK's public services, institutions, national reputation and infrastructure.
2. The threat from SOC is increasing in both volume and complexity and will continue to do so in the short to medium term. Common drivers such as technology and international conflict will continue to place the threat on an upward trajectory, creating a challenging environment for the UK response.
3. The SOC victim impact is wide ranging. We assess that the actual scale of Modern Slavery and Human Trafficking (MSHT) in the UK is continually and gradually increasing. Recorded sexual offences against children in the UK continue to increase year on year. Firearm offences increased by 27% in 2016/17 (year ending June 2017), and drugs deaths are at their highest level since comparable records began in 1993. There were 3.4m fraud offences in the year ending March 2017— almost a third of all crimes. 'County lines' drug supply networks are now reported to affect all 43 police forces in England and Wales, as well as Police Scotland and the British Transport Police, exploiting young and vulnerable people and resulting in an increase in associated violent crime.
4. Individuals and communities also feel the impact of SOC through violence and intimidation that often accompanies various aspects of crime. Victims of SOC may suffer violence directly at the hands of criminals (particularly in threats such as MSHT and CSEA). However, local communities throughout the UK also feel the impact from other SOC-related action such as organised crime groups (OCGs) maintaining control on their domains, being caught in the 'crossfire' of inter-OCG violence, and intimidation of local businesses and individuals.
5. SOC threats are increasingly interlinked. There are significant overlaps between MSHT and Organised Immigration Crime (OIC), especially in unstable states and conflict zones where large numbers of migrants are vulnerable to labour/sexual exploitation and debt bondage (both during their journeys and in migrant camps). Upstream, offenders often move seamlessly between MSHT and OIC. There is also a strong connection between drugs supply and firearms, with firearms being used for protecting and enabling the wider criminal interests of OCGs.
6. OCGs (of which there were 4,629 mapped in the UK at the end of 2017ⁱ) can also work together in criminal enterprises. New market entrants will integrate with existing criminal infrastructure such as money laundering networks and logistics providers to enable them to expand their activities and even distance themselves from the criminality. Additionally, strong ties exist between some SOC offenders through common criminal interest or affiliations formed in the prison environment.

ⁱ Organised Crime Group Mapping (OCGM) is a law enforcement tool which maps characteristics of OCGs and individuals involved in SOC. Whilst figures collected can be a useful indicator of the current state of SOC in the UK, it does not capture the totality of SOC threats facing the UK (e.g. CSEA). It is subject to data rationalisation and cleansing from year to year; it is because of this that the current number of groups mapped (4,629) is considerably lower than the previous year (5,866).

Pathways into SOC

Motivations

7. Most criminality is conducted for the purposes of financial gain. Usually, this financial motivation will coexist with other factors that influence whether an individual will become involved in organised crime. Other key motivations include threats and coercion, family and social pressure, or an attraction to what is seen as a glamorous lifestyle. Vulnerabilities such as financial hardship can also leave an individual susceptible to criminal exploitation, or motivate their involvement.
8. However, motivations can vary significantly between crime types; for example, the majority of individuals who are involved in Child Sexual Exploitation and Abuse (CSEA) undertake this criminality for the purposes of sexual gratification, with financial profit being a factor in some cases such as live-streaming of abuse. Similarly, offenders who are involved in cyber crime are motivated by money but also for other reasons including ideology, the attraction of a challenge, and standing amongst their peers.
9. Alongside established routes, different pathways into serious organised criminality are emerging, most notably where criminals seek to take up of areas of technology enabled crime. Relatively easy access to established online criminal trading sites on both the mainstream internet and dark web, together with ready access to shared communities of interest provide opportunities for new and/or inexperienced criminals. Technological advancements and an increase in the use of social media, particularly by children, also offer more opportunities for those with a sexual interest in children.

Networks

10. Serious and organised criminals tend to operate in either loose networks based

on trust, reputation and experience, or more structured and hierarchical groups (sometimes based on family links). Both loose and structured groups can cross ethnic boundaries and often have international ties which facilitate criminality.

11. Individuals become significant in their groups in many ways, often determined by the nature of the group. In family-based OCGs, the principal is often the oldest active member. Associative groups are often managed by those with the most experience. Propensity for violence and intimidation can also influence a nominal's standing.
12. Some serious and organised criminals network whilst in prison. These individuals are then released back into society with new contacts and skills to progress in more serious and organised criminality.
13. The majority of CSEA offending is committed by lone individuals, with offences involving more than one offender estimated at 10% nationally. In the online environment individual offenders can be part of a wider CSEA offending community through anonymised online forums.

Backgrounds

14. The socio-economic background of an individual is known to influence their pathway into criminality. Some individuals gain their local notoriety through years of criminal activity. Others start their careers at the higher echelons of criminality by belonging to the same networks as existing high ranking criminals or family members, by being entrepreneurial in nature or owning crime-enabling businesses. Exposure to criminality committed by family members from a formative age enables steady mentoring and normalises the activity.

15. Young people brought up in deprived neighbourhoods by fragmented families are more susceptible to members of commodity-based OCGs or street gangs looking to recruit. Initially these young people can become involved in anti-social behaviour and petty crime before progressing into more significant criminality.
16. As already noted, technological advances are giving rise to non-traditional pathways to crime and offenders with different backgrounds. Recent notable investigations of serious criminal trading on the dark web highlighted that the traders concerned had little or no previous recorded criminal history, whilst many young people involved in – or on the cusp of involvement in – cyber dependent crime in the UK are also unlikely to have been involved previously in other crime.
17. Offending by under 18s forms a rising proportion of reported CSEA offending, even when excluding incidents of self-generated indecent imagery (which have been increasing since 2014). There are emerging concerns that continued viewing of indecent images of children could lead to desensitisation, normalisation and escalation of offending.
18. Individuals possessing professional skills that can enable, conceal or advance unlawful activity in the financial/law enforcement arenas are recognised as highly valuable assets by organised criminals and can be at risk of being recruited or corrupted. The pathways into SOC for these offenders are currently not well understood.
19. Pathways into criminality and the type of criminal activity subsequently undertaken can also, on occasion, be determined by local opportunities. Evidence of human trafficking for the purposes of labour exploitation appears to be prevalent in areas where restaurants, agricultural and cleaning sectors are in abundance.

The Global Perspective

20. Most of the UK serious and organised crime threat has an international dimension. OCGs smuggle, traffic and exploit vulnerable people; they defraud the public and businesses from overseas through economic and cyber crime; and they source illicit goods overseas such as firearms and drugs. They seek to move, hide and store criminal proceeds within, through or from the UK. UK sex offenders abuse children in upstream locations or view CSEA emanating from overseas. Transnational OCGs exploit vulnerabilities such as inadequate law enforcement, border controls and criminal justice structures, weaknesses in legislation, corruption, and vulnerable communities.
21. As the threat from SOC changes and develops, many of the influencing factors and enablers (such as new technology, political instability, or civil unrest and war) originate away from the UK, meaning we have to take a truly global view to have any meaningful impact closer to home.
22. Collaboration with international partners both bilaterally and through multilateral institutions and forums (such as Europol and Interpol) provides opportunities to extend our reach and cooperate strategically and operationally, to tackle common threats and to share/leverage capabilities against serious and organised crime. In doing so we are able to undertake activity overseas that might otherwise be beyond our reach, and to brigade our efforts with likeminded partners to achieve more impactful and effective law enforcement outcomes.

SOC in Scotland

Written in association with Police Scotland

23. There are 164 known OCGs comprising 3,282 individuals being investigated by police and partners in Scotland. The number of OCGs is decreasing but the threat is increasing, evidenced by the rise in the number of high-scoring threat groups and an increase in the top 20% threshold threat score. We assess that the escalation in threat is, in part, linked to the ongoing feuds, violence and firearms incidents relating to OCGs in the central belt of Scotland.
24. The groups in the top-scoring 20% of those mapped are predominantly involved in violence, money laundering, and drugs (with the majority involved in more than one class of drug). Of those groups 86% have used violence and intimidation, 82% have nominals incarcerated in prison, 79% are linked to at least one quasi-legitimate business enterprise, 64% have access to firearms, and 61% are assessed to be using encrypted communication.

Drug Trafficking

25. Drug trafficking remains a high volume threat with two-thirds of OCGs in Scotland involved; cocaine, heroin and cannabis continue to be the most popular. Spain, followed by the Netherlands and China, are the main supply areas for drugs into Scotland from outside the UK.
26. Significant SOC connections exist between Scotland and the north west of England, predominantly Merseyside. This analysis is consistent with intelligence that the north west of England, predominantly Liverpool, continues to be the primary source of drug supply into Scotland. Other connections exist between Scotland-based OCGs and those in West Midlands and London.

27. There is a current threat and harm presented by feuds and rivalries between six main OCGs operating in the east and west of Scotland. The situation escalated in late 2016 resulting in the shooting and murder of an individual connected to OCGs. This then led to numerous reported and unreported acts of further violence. The risk is heightened by access to firearms, including automatic weapons. A number of the attacks have been carried out in public places. Despite recent firearms seizures, it is assessed that the OCGs continue to have ready access to firearms that some may be willing to use within public places.

Human Trafficking

28. In Scotland, the OCGs involved in human trafficking for the purposes of sexual exploitation primarily involve foreign nationals where both the perpetrators and their adult female victims share a common nationality of Romanian or Slovakian. Those involved in labour exploitation usually involve perpetrators who share a common country of origin as their victims, including Latvia, Vietnam and China.
29. Scotland-based OCGs involved in human trafficking operate largely independently of one another with no definite links or cohesion identified. They also tend to be poly-criminal in nature, engaging in criminality such as drug trafficking, violence and sexual offending.

Financial Crime

30. A variety of emerging fraud types are identified including pension fund fraud, vishing fraud and fraud where road traffic accidents are manufactured to facilitate false claims to insurance companies.

Organised Acquisitive Crime

31. Scotland-based OCGs continue to be involved in acquisitive crime where the majority of groups are also involved in drugs, violence and financial crime. The most common type of property stolen is motor vehicles, mainly for use as enablers of other criminal activity. 2017 also saw Scotland-based OCGs being involved in ATM theft, metal theft, and bogus crime.
32. Similar to other parts of the UK, Scotland-based OCGs are attempting to exploit airports to facilitate human trafficking, drug supply, movement of cash and importation of tobacco and cigarettes. Intelligence is limited regarding criminal use of air freight in Scotland, although we assess it is a continued threat.
33. Commercial maritime is also used in relation to criminality including human trafficking, immigration abuse, and potential extremist travel. Abuse of the Common Travel Area (CTA) is evident in Scotland at the ports of Loch Ryan and Cairnryan.
34. There have been instances of Roll-On/Roll-Off (RoRo) freight being abused for the movement of illegal immigrants and Class A drugs into Scotland.

Borders

32. Similar to other parts of the UK, Scotland-based OCGs are attempting to exploit airports to facilitate human trafficking, drug supply, movement of cash and importation of tobacco and cigarettes. Intelligence is limited regarding criminal use of air freight in Scotland, although we assess it is a continued threat.

SOC in Northern Ireland

Written in association with the Police Service of Northern Ireland

35. PSNI currently are sighted on a total of 83 OCGs. 58% of these OCGs are engaged in two or more categories of organised criminality, whilst 65% are involved in drugs criminality.

Cross Border Criminality

36. The Common Travel Area (CTA) is open to exploitation by criminals, illegal immigrants and extremists who use the border to facilitate and enable criminality. There is significant interaction between OCGs operating on both sides of the border, working together across a number of types of organised crime including drug trafficking, excise fraud, human trafficking, environmental/waste crime, burglary, firearms purchases/movement, plant theft, agricultural crime, and money laundering. Recent analysis identified that almost half of OCGs managed and investigated by PSNI are known to have strong links and associations with OCGs based in the Republic of Ireland (ROI).
37. A number of OCGs have recently engaged in drug-related criminality, primarily the purchase of drugs (including heroin, cocaine and cannabis) in the ROI and the subsequent importation of these drugs into Northern Ireland. Further OCGs have been engaged in tax and excise evasion (primarily the smuggling of contraband and counterfeit goods).
38. Mobile organised crime groups have been an issue across the island in recent years, with a number of groups travelling throughout the ROI carrying out burglaries of commercial and residential properties, but also travelling between ROI and Northern Ireland to commit crime. These groupings readily engage in violence, meaning victims and anyone who disturbs

their activities (including law enforcement personnel) are at risk.

Drugs Trafficking

39. Deaths as a result of drugs misuse continue to be a concern, with a variety of both illegal and prescription drugs suspected of being a contributory factor in a number of cases.
40. Drug importation is conducted via various methods:
- concealed within legitimate goods;
 - via haulage companies (used to transport drugs on land and via ferries to ROI and NI ports);
 - in personal cars/vans and by public transport (the latter is particularly prevalent in heroin imports from Dublin); and
 - via courier networks involved in postal deliveries (with an ever increasing number of customers using online services to make purchases for all types of commodities including drugs, firearms, counterfeit and contraband tobacco products and other illegal commodities).
41. We assess there is a potential for drone technology to be used in the near future to assist in the importation and, more likely, local distribution of drugs. This will allow suppliers the ability to carry out deliveries themselves, cutting out a middle man and remain 'hands off' the commodity.

Money Laundering

42. Professional enablers from the banking, accounting and legal world are used to facilitate the legitimisation of criminal finances and are perpetuating the problem by refinancing further criminality.

Extortion

43. Information held by PSNI suggests that paramilitary groups (both loyalist and republican), or individuals claiming to be from these groups, continue to be actively involved in extortion attempts, particularly the racketeering of small businesses and building sites across Northern Ireland. It is likely that significant under-reporting occurs due to an unwillingness of victims to come forward to PSNI. Illegal money lending/loan sharking is also likely to continue, with similar challenges of under-reporting.
44. Alongside local group involvement, there is an increasing number of online extortions in which money is sought by criminals by threatening to damage the reputation of an individual or business. Various social media platforms and messaging services are being used to facilitate these offences. Again, it is likely that many of these crimes do not get reported to the police.

Human Trafficking

45. During the 2016/17 financial year, the PSNI Human Trafficking Unit (HTU) conducted 308 screening assessments; an increase from the 2015/16 financial year (which saw 252 persons screened). From the 308 screening assessments in 2016/17, 34 potential victims of human trafficking were identified in Northern Ireland. The main issues for Northern Irish law enforcement continue to centre on sexual and labour exploitation.

Organised Immigration Crime

46. A key priority within Immigration Enforcement NI remains the detection and prosecution of high harm foreign national offenders who attempt to re-enter Great Britain using a circuitous route through abuse of the Common Travel Area.

47. A number of detections have been made of offenders who had re-entered the UK in breach of a Deportation Order and were intending to re-enter the mainland from a Northern Ireland port.

Excise Fraud

48. Excise fraud across the Northern Ireland/ROI border continues to be a major concern. The border represents a risk specifically in terms of oils and tobacco fraud due to the nature of OCG activity, the ease with which OCGs can conduct their business, and difficulties in enforcing border controls. Within Northern Ireland, the primary areas of concern for law enforcement are Londonderry and Armagh where interconnected and well established networks organise and facilitate excise frauds.

Paramilitary Involvement in Serious and Organised Crime

49. More than 20% of the OCGs known to and investigated by PSNI have direct links with paramilitary (both loyalist and republican) organisations.
50. These OCGs are engaged in a wide range of criminal activity including the importation and/or distribution of drugs/contraband goods (primarily cigarettes), extortion (of legitimate businesses and individuals involved in drug related crime), protection rackets, illegal lending, and money laundering. These groups have also engaged in violent activities including murder, attempted murder, paramilitary style shootings and beatings, the deployment of IEDs, and other forms of intimidation and public disorder.
51. It is difficult to assess the proportion of the proceeds of the criminality of these groups that are used to fund paramilitarism. We assess that much of this is intended for the personal gain of individuals involved in such criminality.

Horizon Scanning: Trends to 2023

52. Crime and law enforcement do not operate in a vacuum. This section provides a top-level view of some of the complex and overlapping trends, drivers and enablers that have the potential to - directly or indirectly - affect the criminal and law enforcement environment in the next five years.

Technology

53. Developments in technology will continue to transform the future crime landscape. Advances in information/communication technologies (especially the introduction of 5G), artificial intelligence, the Internet of Things (IoT), and autonomous/semi-autonomous systems all have the potential to initiate significant disruptive change to the technology landscape. It is probable that their development will present opportunities for specific areas of criminal and law enforcement exploitation.
54. The use of technologies such as the dark web, encryption, virtual private networks (VPN) and virtual currencies will support fast, 'secure' and anonymous operating environments, facilitating all levels of criminality. The increasingly ubiquitous 'by default' nature of these enabling technologies will continue to lower the barriers to entry for some types of cyber enabled crime.
55. The rapid and often unpredictable nature of technological change and its subsequent application adds further layers of complication and uncertainty for developers, users and law enforcement. Some trends will be influenced by changing user behaviour rather than the technology itself.

56. Technology will continue its complex and global spread, with cyber crime very likely becoming 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 potential threat to the UK. It is possible that cyber criminal activity will locate within 'safe havens' in more hard-to-reach firewalled and 'siloes' jurisdictions.

Conflict and Migration

57. It is almost certain that political and economic pressures and instability will continue to drive significant levels of legal and illegal migration, regionally and globally.
58. Global instability, humanitarian crises, war and persecution are likely to continue to create opportunities for criminal activity. Areas of instability, such as Libya, Syria and Ukraine are likely to continue to serve as source countries and transit routes for criminal exploitation.
59. It is probable that the number of international migrants, refugees, asylum seekers and other displaced people will continue to grow due to displacement from conflict and other tensions.
60. Displacements could also be instigated by environmental pressures and events. It is probable that in the next five years we will experience more regular extreme climate events, causing people to move - either temporarily or permanently - to more hospitable locations. The concept of climate change refugee is likely to become increasingly accepted.

61. A decrease in the scale of conflict in countries such as Syria in the period to 2023 would lead to the return of UK citizens and possibly weaponry from war zones, with potential implications for the terrorist threat and links to criminal diaspora communities.
62. It is likely that future conflict will be less confined to the traditional battlefield and will increasingly encroach on a cyber-environment, with the aim of disrupting societies, leading to a decreasing divide between cyber conflict and cyber crime.

Brexit

63. The result of the EU referendum vote has had little impact on criminal activity or international law enforcement cooperation to date, but it will be a key driver of uncertainty in the next five years.
64. Criminals are not constrained by geographical or jurisdictional boundaries and are inherently opportunistic. We expect that many will strive to take advantage of the opportunities that Brexit might present, for example from the design and implementation of a new UK customs system or from increased challenges for EU and UK law enforcement in locating and extraditing international fugitives if the UK were to lose enforcement or intelligence sharing tools. However, some of the impacts of Brexit have the potential to work in favour of law enforcement, including greater discretion over the movement of goods and people.

Conclusion

65. Excluding those crimes created by the introduction of new or changing legislation, it is unlikely that we will see any completely new types of serious and organised crime in 2023. It is likely, however, that we will see existing crime operating in new ways and in new places.
66. Global drivers and trends both causing and caused by global and regional uncertainty and instability will continue to shape public attitudes and behaviour, criminal activity and the associated law enforcement response. Both crime and law enforcement will need to operate in a more uncertain, more diverse and complex world. 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.
67. Within this complex world, much change will still be driven by technology. In an increasingly technology-dependent society, the implications of both intentional and inadvertent criminal behaviour will increase. As technology becomes increasingly autonomous, issues of responsibility and blame will also likely grow in importance.



UK Border



Cross-Cutting Threat Enablers

Use of Technology in SOC

Criminal Use of Encryption

68. Since 2010, communication service providers (CSPs) have migrated to encrypted services 'by default'; a process that accelerated following the Snowden disclosures. Now, the majority of internet traffic is encryptedⁱ and publically available mobile device apps offer end-to-endⁱⁱ encryption as standard. Whilst this means enhanced privacy for the users, the use of encryption is impacting on law enforcement's ability to collect intelligence and evidence.
69. Encryption provides important benefits to the UK public and economy: it enables digital commerce, ensures security on the web and increases privacy. However, such technology has become an enabler to criminality, presenting serious challenges for law enforcement. We now observe the use of encryption in criminal communications across all threat areas and across all levels within criminal hierarchies.
70. Criminals will almost certainly continue to prioritise communications security. Encryption built in to mainstream products will continue to expand and will offer criminals enhanced protection by default, rather than design. The pace of these developments will continue to challenge law enforcement capability and resource, with narrowing options for mitigation.
71. While encrypted communications platforms are legitimate products welcomed by consumers and privacy advocates, they will increasingly erode law enforcement's capability to detect and deter criminal activity.

i Through HTTPS

ii End-to-end encryption is where the sending and receiving devices (e.g. two smartphones engaged in message chat) encrypt/decrypt their messages directly, rather than passing it through a central server to encrypt/decrypt for them.

Criminal Use of the Dark Web

72. The combination of encryption and anonymisation pose substantial challenges to law enforcement's collection of intelligence and evidence. The impact of anonymisation techniques is as significant as encryption: any available data that is not attributable to a user can limit law enforcement capability. This is likely to be exacerbated as criminals increasingly adopt anonymisation technology (e.g. ToR, VPNs, 'spoofing' and services with weak registration). The dark web is a primary forum for the illicit use of anonymisation techniques. The dark web is a small section of the Internet that is intentionally hidden and inaccessible through standard web browsers. It is primarily accessed through specialised encryption software, such as The Onion Router (Tor), the Invisible Internet Project (I2P) and Freenet. Whilst the dark web helps anonymise and obscure activity, the services on offer are not fundamentally different from their mainstream Internet equivalents. These include marketplaces where illegal commodities are traded, forums for the sharing of CSEA material, networking with other criminals and a number of enabling services such as cryptocurrency exchanges.
73. The range of criminal services offered on Tor cover most threat areas. Cyber crime and fraud appear to be the most prevalent, but there are also sites offering commodities such as drugs and firearms, as well as facilitating CSEA and MSHT. The majority of services offered, particularly with regard to commodities, are offered in dark web 'marketplaces' (where multiple suppliers offer goods in one place) as opposed to individual supplier Tor sites.
74. Owing to law enforcement action, fraud or commercial failure, the vast majority of dark web marketplaces have a short

lifespan. However, there have been some high profile marketplaces that have dominated the illegal commodity trade. These include the original Silk Road, Evolution, SilkRoad 3.1 and - more recently - AlphaBay. The emergence of these sites as market leaders was, in part, a result of the disruption of their predecessors, with activity being displaced rather than eradicated. 'The Dream Market' is currently the most prominent and is assessed to be benefitting from the Alphabay and Hansa law enforcement takedowns in 2017.

75. Generally-trusted, anonymous payment systems are the key enabler for dark web trade. Bitcoin is the preferred payment method, although various marketplaces and forums offer additional cryptocurrency options, including Monero and Ethereum. There are also a host of enabling services underpinning the dark web economy, including bitcoin mixing services, virtual currency exchanges, hosting services, onion web services and user confidence tools such as multi-signature wallets.
76. Drugs remain the main illicit commodity sold on dark web market places, although there is an increasingly diverse set of commodities on offer. Identity and Government Gateway credentials (both used for repayment fraud against HMRC), identity documents and compromised credit card data are also offered for sale. Ransomware and malware strains are sold on the dark web, as the 'as-a-service' model continues to lower the threshold for entry into cybercrime.
77. It is less common to see firearms for sale and extremely rare to see CSEA material on the higher profile dark marketplaces – CSEA material tends to be concentrated in niche sites. Ultimately, these marketplaces rely on availability and reputation in order to be successful and these can be jeopardised by association with this type of material; we have seen examples where administrators

have restricted or banned material linked to CSEA on their site. As high priority threat areas for law enforcement, domains that host firearms and CSEA material are also likely to attract a greater degree of law enforcement attention.

78. The volume of illegal trading on the dark web has increased since 2011, and it is likely that this trend will continue in the future. The barriers to entry to illicit dark marketplaces and specialist criminal websites are often very low making them convenient and easy to use. New users require relatively little knowledge and no previous or specialist contacts in order to access them. Recent technological developments have enabled Tor and I2P compatibility with the majority of smartphones and Internet enabled mobile devices. Additional security measures are in place for some sites within the dark web and many operate on an invite only basis for new members.

Vulnerabilities at the UK Border

79. Exploitation and abuse of the UK border enables a wide range of threats to impact the UK. The past year has shown that these threats persist, and individuals and OCGs continue to exploit border vulnerabilities with increasing levels of sophistication. OCGs are commonly involved in multiple threats and will choose the modes most suited to their commodity.

Border Corruption

80. 'Border corruption' refers to the abuse of privileged access to physical areas and corporate systems at ports and airports to facilitate serious and organised crime. It applies to both public and private sectors.
81. Corruption at the border mainly facilitates the movement of Class A drugs into the UK. However it can also facilitate the movement of other illicit commodities as demonstrated in an incident in 2017, where a UK official was arrested following a seizure of drugs and firearms in France which were being brought into the UK.

General Aviation (GA)

82. The UK has over 3,000 airstrips, presenting opportunities for criminals to use GA to exploit the UK border. Intelligence demonstrates that OCGs have made significant investments in the purchase or hire of aircraft to facilitate illegal movement of people and commodities. It is highly likely that OCGs will continue to use GA in order to facilitate the illegal entry of migrants, in particular, into the UK.

General Maritime (GM)

83. The UK, with approximately 11,000 miles of coastline and more than 950 ports, harbours and marinas, presents challenges for UK law enforcement and opportunities for OCGs exploiting GM.
84. Our intelligence has increased with regards to how criminals use commercial vessels

to exploit the vulnerabilities in GM. OCGs use commercial vessels to facilitate larger importations of illicit commodities from Europe for onward distribution.

85. Clandestine entry into the UK and large-scale drug importations present the greatest risk from the abuse of GM.

Roll-On/Roll-Off (Freight and Tourist)

86. The UK receives Roll-On/Roll-Off traffic via the Eurotunnel and ferry services from 15 ports across France, Netherlands, Spain and Ireland.
87. Roll-On/Roll-Off is the most common method by which OCGs smuggle illicit goods and people into the UK. 'Little and often' methods are commonly employed by OCGs to spread the risk of their commodities being seized.
88. Whilst there is likely to be little change in the threats seen in Roll-On/Roll-Off, the methods used by OCGs to exploit the vulnerabilities of this mode are likely to continue to become more sophisticated.

Fast Parcels and Post

89. The volume of shipments transiting the UK border via fast parcels and post continues to increase, with OCGs concealing illicit goods amongst legitimate traffic. In 2017, all known seizures of the opioid Fentanyl were made via the fast parcel and post system. Fast parcels and post also remain a significant mode of transport for the importation of single firearms. Firearms importations into the UK via fast parcels and post are facilitated almost exclusively by online purchases.
90. As with previous years, it is highly likely the volume of fast parcels and post traffic will continue to increase due to rising consumer demand online.

Prisons and Repeat Offenders

91. The threat from SOC offenders in prisons can be split into two groups: those who continue to facilitate SOC in the community from within prison; and those who are involved in organised crime within the prison environment. There can be some overlap between the two and their activities cut across all the main threat areas. There is a notable concentration of SOC offenders who are in prison because of drug trafficking and other related offences such as use of firearms, violence, and money laundering.
92. Some SOC offenders are highly capable, well organised individuals with extensive supportive networks on the outside. SOC offenders usually adopt a business-focused approach to their activities both within prison and whilst on licence. They exercise pragmatism in their dealings with authority in order to minimise impact on their enterprises. SOC-affiliated individuals are characterised by general - if superficial - compliance with rules and regulations. This means that they can establish a prison routine subject to minimal disruption whilst maintaining maximum freedom of movement and trust from prison staff.
93. These activities are further facilitated by strong ties between affiliated SOC offenders, based on common acquisitive interest and peripheral affiliations with gangs formed in prison that have a reputation for violence. Such ties between OCGs and gangs provide a pathway for gang members to be drawn into OCGs as members, leading to much more serious offending. This is one of the recognised steps on the pathway into organised crime.

Criminal Enablers

94. Mobile phones continue to be a key enabler for those in prison involved in SOC. Their illicit presence provides SOC offenders with the means to continue to play a full role in major criminal enterprises on a national and

international level, virtually unaffected by physical confinement.

95. SOC offenders on the outside often use corruption in order to facilitate their activities; this is no different to those in prison. Corrupt prison officers and auxiliary staff assist organised criminals by smuggling illicit items into the prison and by providing information to key members of the OCG, both on the inside and outside of prison. The smuggling of mobile phones and sim cards into prisons by corrupt staff allows SOC offenders to continue their operations from inside.

Drug Supply

96. Illegal drug supply within prisons is highly lucrative for suppliers, but extremely detrimental to the prison population and expensive for the state. Intelligence suggests that “Spice” is the drug of choice within prisons in England and Wales. Spice is one of several ‘psychoactive substances’ (PS) which are synthetic compounds that can cause people to experience enhanced sensations and damaging side-effects. It is also associated with increased mental health issues, as well as a strong urge to redose.
97. Some PS are available in liquid form which can be sprayed onto paper and ingested or injected, making it extremely difficult to detect when being trafficked into prisons. This also presents a significant health risk in that it may overlap previously sprayed sections meaning the recipient cannot be sure of the dosage they are ingesting. PS enter the prison estate via throw-overs, drones, corrupt staff, visits, concealments, and even correspondence.
98. PS trafficking in prisons is linked to higher levels of violence (connected to drug debts), assaults on staff, and self-harming. The extent to which the supply of PS in prisons

is controlled by organised crime is not fully understood. However, because a sprayed single A4-sized sheet can sell for upwards of £250 in prison, it is unlikely that less organised/connected criminals would be allowed to operate without the backing of organised criminals.

Cyber-enabled Offending

99. An emerging threat in prison is cyber-enabled offending. Cyber-enabled crimes are not recorded as such and so it is difficult to gauge the levels of cyber capability in prison. It is assessed that the cyber capability of criminals will continue to increase in line with that of the general population. There is a risk that cyber offenders, who tend to be younger than the average prisoner, may be exploited by serious and organised criminals in prison who may recruit them to further their own criminal activities.

CSEA Offenders

100. CSEA offenders are, in many cases, not otherwise criminally-minded and are not attempting to gain financially from activities whilst in custody; in this respect they are unlike other SOC offenders. A recent intelligence study of these offenders in custody concluded that routine, low-level networking and sharing of items relating to children such as magazine cut-outs and pictures from library books is occurring. Less commonly, electronic images of children were noted as having been discovered on computers linked to the educational intranet.
101. Whilst evidence of communication and facilitation of offending using mobile phones was not detected, it has been noted historically that prisoner-to-prisoner mail, external written communications and telephone calls have all been used to discuss and in some cases arrange further offending. It is likely that this will increase as more offenders convicted of

cyber-enabled and cyber-dependent CSEA offences enter the system. We anticipate that networking among CSEA offenders with cyber capability could result in a greater overall capability to conduct cyber-enabled offences.

Criminal Finances within Prison

102. Criminal abuse of finance by prisoners and their associates primarily takes the form of the exploitation of weaknesses in the prison banking system, and by using friends and family's bank accounts either with or without their consent. Criminals deliberately smuggle illicit items into prison to capitalise on inflated commodity values within the illicit economy. They also seek to drive other prisoners into unserviceable debt in order to exercise control over them.
103. A study of the activities of SOC offenders has shown that a business model has developed whereby items such as drugs (including PS), mobile phones, sim cards, and tobacco/associated paraphernalia are purchased with the sole intent of smuggling them into prisons, where the market value can be five to ten times higher, if not more. The mark up is further compounded where individuals do not manage their debts; a prisoner owing for an item costing £5-10 outside of prison may find themselves liable for tens of thousands of pounds of debt through punitive interest rates levied by lenders in prison. This can lead to extortion or exploitation of the prisoner, or to attempts at extortion of family members through threats and actual violence against them or the indebted offender. We judge that illicit financial activity among offenders is not heavily impacted by incarceration, due to the availability of smartphones.

Rehabilitation and Recidivism

104. The ultimate aim of the criminal justice system is to rehabilitate offenders who have paid their debt to society. This means that an offender is introduced to gradually increasing levels of freedom along their journey to release. However, SOC offenders usually have a long history of offending and, in spite of the efforts of law enforcement, HMPPS, social services, and others, they remain resistant to rehabilitation and are likely to continue to reoffend.

105. The full extent of recidivism in England and Wales - either on probation or beyond - requires further assessment; there are a multitude of examples of SOC offenders continuing their activities even whilst still on probation. However, one tool which is key in the attempt to help prevent reoffending is the Serious Crime Prevention Order (SCPO). There are currently around 800 SCPOs in England and Wales and are an effective and cost-efficient way of preventing ongoing offending. SCPOs can be used to identify aspects of criminality that may take place after an individual has been released from prison, which – if present – can be used to recall an individual to prison or even lead to new sentences.

Corruption within the UK

106. Certain sectors in the UK, such as borders and immigration, law enforcement and prisons, face a high threat of corruption from OCGs. Motivations for corrupt behaviour are varied and can include financial incentive, loyalty, gratuities or threats.

109. Corrupt staff that work directly at the UK border are able to use their access to undermine customs and immigration processes.

Corruption in UK Police Forces

107. Information is a highly desirable commodity for organised criminals. “Tipping off” by law enforcement officers provides criminals with knowledge of future operational activity, search warrant action or upcoming arrests, allowing them to plan and undertake tactics to counter the law enforcement response.

Corrupt Professionals

110. A small number of individuals in positions of authority - such as the accounting and legal services, trust and company service providers, or in banking institutions - have been identified as corrupt. They have played pivotal roles in complex money laundering schemes or divulged information to help bring credibility to fraudulent schemes. They are also used to assist corrupt politically-exposed persons (PEPs) investing in the UK, showing that domestic and international corruption are interlinked.

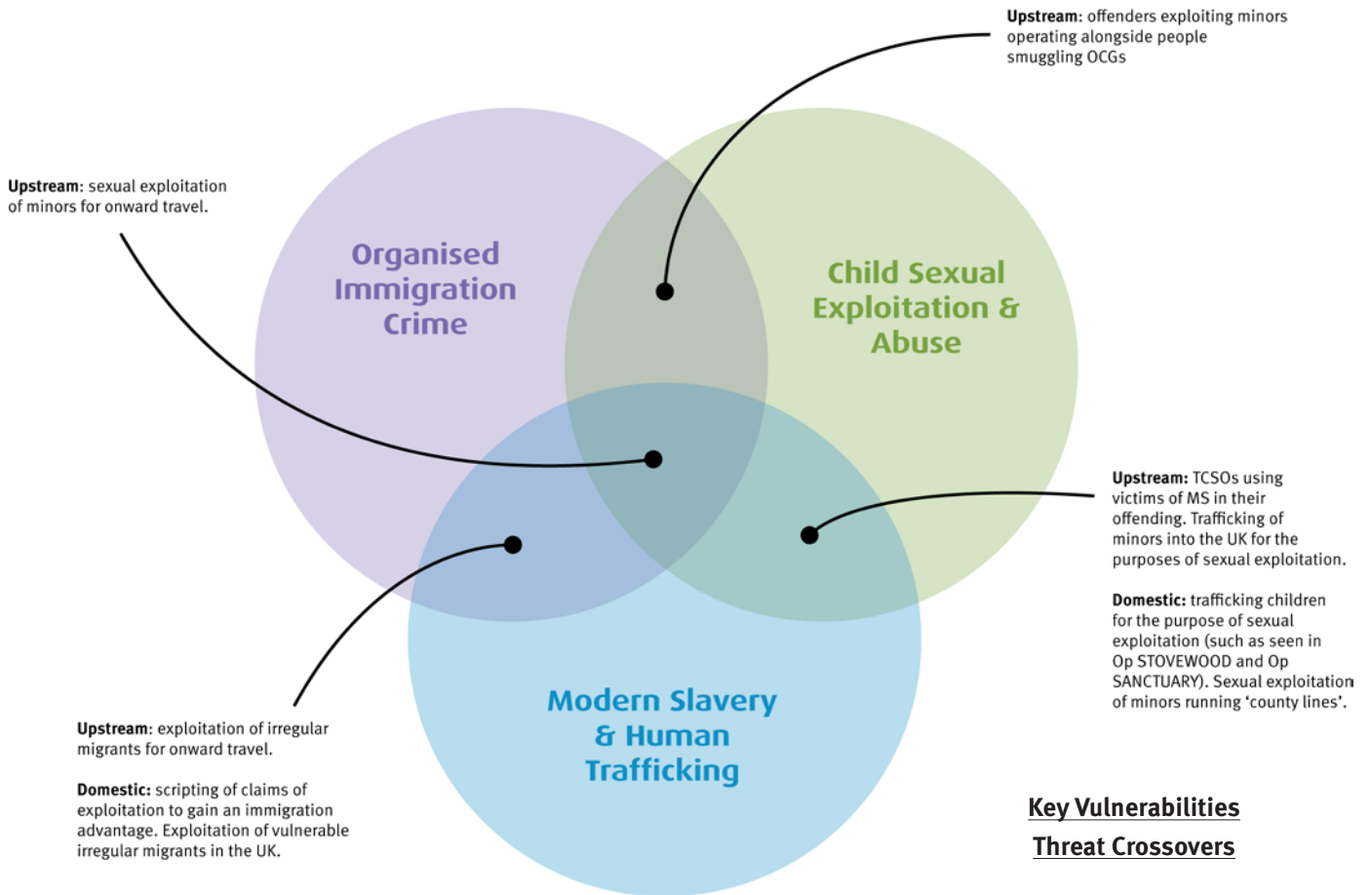
Borders and Immigration

108. OCGs use corrupt public and private sector workers to facilitate the undetected movement of illicit goods and illegal immigration into the UK. Investment in corrupt insiders is considered by organised criminals to be worthwhile in order to enable the smooth movement of a commodity into the UK.



Vulnerabilities

Child Sexual Exploitation & Abuse
Modern Slavery & Human Trafficking
Organised Immigration Crime



111. The three threats forming the Vulnerabilities 'pillar' (CSEA, MSHT and OIC) are underpinned by the vulnerability of victims and the power imbalance between them and offenders. Though the offences are distinct, the three threats share some methodologies, with MSHT particularly seen to connect CSEA and OIC.

112. The borders between the three threats are permeable, with those who are targeted as part of one threat sometimes becoming victims of another. Similarly, offenders have been identified operating across Vulnerability threats.

113. There are shared drivers across the three threats, with economic imbalances, displacement and mass migration, and social factors creating a pool of vulnerable people (both domestically and upstream) who may be exploited or may seek facilitation of migration.

114. Cultural attitudes that diminish willingness to report abuse or exploitation, the ease of movement across borders, and technological facilitators all serve as enablers across the Vulnerabilities threats.

115. Though they are largely unlinked domestically, looking forward we have been unable to identify a plausible scenario which would lead to a significant divergence between the MSHT and OIC threats upstream. We assess that the routes and methods are likely to align increasingly in the coming three years.

i 'People smuggling' and OIC refer to the facilitated illegal movement of people across national borders and represents a crime against the State. This is distinct from 'human trafficking' and MSHT which involve movement or control of location, along with forms of exploitation, and is a crime against the person.

Child Sexual Exploitation & Abuse

Key Judgements

- It is likely that the lack of moderation and regulation on live-streaming apps has helped increase their popularity among offenders.
- CSEA offenders are likely to adopt encryption, destruction and anonymisation measures in both the dark web and mainstream internet in response to law enforcement attempts to apprehend them.
- The use of end-to-end encryption as standard in social media apps means disguising CSEA activity will no longer be dependent on offender technological acumen alone.
- Educational initiatives will need to be reviewed to reach the most vulnerable children.
- Live-streaming is a growing threat with children's own use of self-broadcast live-streaming apps now being exploited by offenders. Overseas live-streaming business models suggest that this area could potentially become profitable to OCGs in the future.
- Online CSEA continues to generate considerable data presenting resourcing challenges to law enforcement. Effective triaging and preventative work is required to identify offenders posing the highest risk at the earliest opportunity.
- There are distinct offender methodologies, however all target the same high risk factors within their victims. Repeat victimisation by multiple offenders or from successive events has been noted in both offline and online CSEA.
- There are other motivations besides paedophilic sexual interest behind the commission of CSEA. Criminal gangs in niche markets are exploiting the commercial potential of CSEA overseas and there are potential for other financial models to become viable. Additionally, sex offenders engaging in CSEA as part of other non-paedophilic sexual fetishes need to be examined to obtain a full understanding of the threat.

Assessment of the Threat

116. The true scale of CSEA remains hidden, but we assess that it is greater than that recorded in official statistics. Recorded sexual offences against children in the UK continue to increase year-on-year (but at a reduced rate) as law enforcement's awareness and proactive focus on CSEA increases.

117. Home Office statistics for England and Wales show 47,224 sexual crimes committed against under 16's during the

12 months ending March 2017, excluding offences relating to indecent images. This is an increase of 15% on the same period the previous year. In Northern Ireland, sexual offences committed against under 18'sⁱ between 1 April 2016 and 31 March 2017 increased by 4% to 1,875 when compared to the previous year. In Scotland, sexual offences against under 18's constituted an estimated 44% of their total 10,822 sexual offences, or 4,762 crimes. This is an increase of 8% on the previous year.

ⁱ Northern Ireland and Scotland break this data down to under 18s.

118. The volume of offending is also measurable through the data footprint of offenders' online activities. Referralsⁱⁱ received in to the NCA from the National Centre for Missing and Exploited Children (NCMEC) have increased by 700% over the last four years and it is highly likely this will continue as the volume of internet data continues to grow.

UK Victims

119. Repeat victimisation is increasingly noted by police forces and Non-Government Organisations (NGOs) and occurs in targeting by lone offenders, group offending and gang activity. Repeat victimisation can also occur online. Some victims experience multiple grooming events by unlinked offenders whereas others are abused by multiple offenders in online or real life networks.
120. Publicity of negative victim experiences when dealing with statutory authorities in CSEA is likely to affect victim confidence in reporting. Child victims are sometimes coming to the attention of law enforcement in the first instance for drink, drugs and public order offences.
121. The victim profile for children targeted by groups (such as in Rotherham and Newcastle) identified that disproportionately high numbers of victims were looked-after childrenⁱⁱⁱ. This was also the case in similar offending groups elsewhere in the country. Placements in care homes outside of the local authority are persistently being exploited as a result of children meeting other grooming victims and being introduced to offenders.
122. Our understanding of the CSEA threat picture is impeded by a lack of reporting from vulnerable groups, including children

ii The total number of referrals received includes referrals of non-CSEA cases ('informational' referrals). The average volume of specifically CSEA referrals has increased from 990 per month to over 3,000 per month over the last five years.

iii In local authority care.

who are disabled, those questioning their sexual identity and from black and minority ethnic (BME) communities. There is no reason to believe that levels of CSEA in these communities are any lower than elsewhere.

Overseas Victims

123. If offenders are embedded in-country, they are better able to exploit victims in institutional care, in education establishments, charities and/or religious groups. Both embedded and transient^{iv} offenders target street children who are already being sexually exploited.
124. Offenders also target children in impoverished families where family members or other third parties are willing to act as facilitators. In these cases, the disparity between the financial position of the abuser and the victim/victim's family is a key factor.

Offenders

125. The internet allows for lone offending – such as viewing IIOC or sharing comments on CSEA offending (including tips on how to groom) – to take place in anonymised online forums. These forums are sometimes referred to as networks, however offline contact between these individuals is rare.
126. Offending by under 18s forms a rising proportion of reported CSEA. Reports of sexual offences on school premises have also increased. This is separate from Self-Generated Indecent Imagery (SGII).
127. From operational evidence, there are observations of extreme fetish interests amongst CSE offenders (bestiality,

iv Embedded offenders are those living in a country, possibly specifically for the purposes of offending. Transient offenders would travel abroad specifically to offend or incidentally offend whilst abroad as a tourist – for instance, by taking advantage (or being apathetic as to whether they are taking advantage of) children exploited through prostitution.

‘chemsex’^v, sadism and HIV fetishes^{vi}). Examinations of the other motivations co-observed with CSEA will increase our understanding and our ability to risk-triage these offenders.

Transnational Child Sex Offenders (TCSOs)

128. UK TCSOs are highly likely to operate in a wider range of countries than official data indicates. However, the majority of convictions and requests for consular assistance from UK nationals arrested for sex offences against children abroad continue to occur in EU and Anglophone countries. This is likely due to their sizeable British diaspora, common spoken language and reporting mechanisms or proximity to the UK and co-ordinated LE response (to aid with detections) rather than them being a preferred choice of destination by TCSOs.

Enablers: Online

129. Anonymisation, encryption and destruction tools increasingly prevent the identification and prosecution of offenders. Offenders use manipulation and rapport-building to increase their influence, either in person or via telephone, email and webcam. Offenders of all ages use anonymising methods, discussing techniques and using dark web applications such as The Onion Router (Tor) to anonymously exploit the internet.

130. As more of the internet becomes encrypted, offenders will be able to achieve anonymity simply by using everyday applications, rather than requiring any in depth technical knowledge. Offenders can use the anonymity of the dark web to groom and harm children on the mainstream internet.

v ‘Chemsex’ is the practise of sexual activity whilst under the influence of narcotics.

vi Known as ‘toxic chasing’ or ‘bug chasing’.

131. The case of CSEA offender Mathew Falder highlighted the damage that can be inflicted on victims. Falder had little or no clear internet footprint. His offending included blackmail, causing or inciting a child to engage in sexual activity, making and distribution of IIOC, and encouragement to rape. His crimes were largely accomodated through Darknet forums and by routing activity through ToR. Exerting his influence on victims through blackmail and manipulation, Falder used advanced methdologies and anonymisation techniques to evade international law enforcement efforts to identify him. In the course of his activity, he was able to identify and target more than 300 victims across the world.

132. Falder was first encountered by law enforcement after posting under various pseudonyms on so-called ‘Hurtcore’ sites on the dark web. Falder’s eventual arrest followed collaboration between UK and international law enforcement partners - led by the NCA - as well as being supported by partners in the UK intelligence community. He was arrested in June 2017, four years after his offending first came to law enforcement attention. After pleading guilty to 137 separate offences, he was sentenced to 32 years imprisonment. The Falder case demonstrates the persistence of determined offenders in achieving their goals, and the levels of harm that can be inflicted remotely over the internet.

133. The take down of Freedom Hosting II by the ‘Hacktivist’ group ‘Anonymous’, and the uncovering of hidden service (HS)^{vii} sites dedicated to CSEA - including so called ‘hurt core’ - has confirmed the use of the dark web by CSEA offenders to visit specialist sites, only accessible via Tor. The majority of CSEA remains on the mainstream internet.

vii A Hidden Service is a service which is only accessible via the darknet and is hosted on the darknet – most commonly Tor.

134. Self-Broadcast live-streaming is a growing concern with 1 in 8 teens having broadcast on Instagram and 1 in 10 on Facebook, and children being coerced and extorted into streaming Category A-C content. Such images can be harvested and redistributed leading to blackmail and extortion for further images by sexually and financially-motivated offenders, which in turn increases the risk of self-harm and suicide by victims.

Enablers: Offline

135. The majority of contact CSEA is intra-familial or committed by an acquaintance of the victim. This has remained a fairly stable feature of the CSEA threat.
136. Law enforcement operations and independent inquiries continue to identify offenders in positions of trust. Holding positions of trust remain a common way for CSEA offenders to access victims, and the use of an institution to abuse children remains a popular modus operandi despite the access provided by the internet.
137. Group-based grooming remains a highly publicised form of CSEA offending. South Asian offenders are over-represented for this particular methodology. The methodologies are consistent with other grooming models; acting as 'boyfriends', using drugs and alcohol and moving victims for the purposes of further sexual exploitation. However, the familial and inter-generational links of these offenders and the apparent infliction of pain, humiliation and degradation on their victims beyond that required to force them to comply with sexual activity are notable.

Forward Look

138. As access to high speed internet and accessible digital technology spreads, there is an increased risk of in-country OCGs live-streaming to UK offenders and/or UK offenders using online media to arrange in country offending.
139. It is likely that coercing children to abuse other children or produce explicit material will remain a preferred method for abusers wishing to influence children. Unless children and parents are encouraged to report when this happens and can be confident that coerced children will not be criminalised (e.g. due to producing SGII), mitigation of this threat is likely to be compromised by low victim confidence.
140. There is some evidence of criminal business models within CSEA. There is a realistic possibility that live-streaming, both as an extension of overseas sex industries and as a way of coercing bespoke imagery from children, could encourage OCG involvement if sufficient profits can be generated.
141. There has been a reported increase in proactive civilian activity against online offenders which is expected to continue next year. This has been characterised by 'Paedophile-Hunter Groups' (PHGs), where civilians posing as children online attempt to deceive groomers into a meeting and then confront them. It remains to be seen what extent vigilante activity against sex offenders can be said to represent a more general civic concern for child safety and child protection. In the event that it does, concerns about how vigilante activities may affect safeguarding of child victims and law enforcement evidence collection would need to be addressed.

Modern Slavery & Human Trafficking

Key Judgements

- Based on analysis of the drivers of MSHT, we assess that the actual scale of MSHT in the UK is continually and gradually increasing and, if drivers remain at their current levels, will continue to do so over the next three years.
- An increasing proportion of potential victims are claiming exploitation upstream; this is likely to reflect the growing risks in transit countries, principally in North Africa.
- It is highly likely that a large quantity of upstream MSHT offending is carried out by looser, unstructured networks collaborating and committing opportunistic exploitation. However, within Europe and the UK there is evidence of greater levels of organisation.
- Though technology is critical to many forms of exploitation, most recruitment still takes place face-to-face. The expected increase in online recruitment has not materialised, and is judged unlikely to in the coming year.
- Within the UK, Adult Services websites (ASWs) continue to be the most significant enabler of adult sexual exploitation.

Assessment of the Threat

142. The term ‘modern slavery’ refers to the offences of human trafficking, slavery, servitude, and forced or compulsory labour. This can then be considered as five sub-threats: the sexual exploitation of adults; the trafficking of adults into conditions of labour exploitation; the trafficking of adults into conditions of criminal exploitation; the trafficking of minors into conditions of sexual, criminal or labour exploitation; and other forms of exploitation.

143. It is highly likely that numbers of MSHT incidents and potential victims identified via the National Referral Mechanism (NRM) and Duty to Notify (DTN) statistics will continue to increase in the coming three years. However, it is not possible to determine to what extent current increases in numbers are due to improved awareness, reporting and recording, rather than an increased incident rate.

144. Based on analysis of the drivers of MSHT, we assess the actual scale of MSHT in the UK is continually and gradually increasing and will continue to do so over the next three years.

Victimology

145. Potential victims’ vulnerability to MSHT is a product of a range of factors including geography (proximity to conflict and instability), cultural norms and beliefs, language, demographics (such as age, gender, economic status), and family cohesion and stability. Geographic factors such as instability and conflict exacerbate the situation for already vulnerable people. These factors not only affect the source countries of vulnerable people, but also those that migrants pass through en route to the UK or elsewhere.

- 146. UK victims of MSHT are frequently vulnerable in terms of homelessness or financial difficulties. These also often go hand in hand with other factors that further exacerbate the situation, such as lack of support from their families, mental illness, and dependency on drugs or alcohol – which also act as means of control.
- 147. Exploitation of victims commonly requires other criminality in order for the offender business model to operate successfully. This ranges from financial offences such as laundering money to immigration offences by non-EU potential victims arriving in the UK – such as clandestine entry, presenting false travel documents or sham marriage.

Offender Profiles

- 148. Offenders are most likely to target individuals of either their own nationality/ethnic group or nationalities with close or historic links, likely exploiting linguistic, national, cultural and ethnic ties in order to recruit and control victims. However, British national offenders remain the most likely to target victims from a broad range of national and ethnic origins.
- 149. Although most MSHT criminality is carried out by male offenders, the proportion of female offenders has increased. Female offenders are most commonly encountered in cases of sexual exploitation - where they can act as ‘madams’ or ‘alphas’ (victims of exploitation who become complicit in the trafficking/exploitation of others), and in domestic servitude.
- 150. Technology is a key enabler of MSHT. The majority of online MSHT offending takes place on the mainstream internet, using well known and publically accessible websites and apps, including ASWs and social media.
- 151. There are a number of different models for how groups of offenders offend and interact. Although we see evidence of larger organised crime groups impacting on the UK and abroad, a large quantity of MSHT offending is carried out by looser, unstructured networks which interact and collaborate with each other dependent on the exploitation type and across different stages of MSHT (e.g. transit, recruitment).
- 152. Within Europe and the UK there is evidence of greater levels of organisation, with MSHT directed by over-arching OCGs, who operate an end-to-end service, controlling the recruitment, transit and exploitation of victims.

Recruitment

- 153. The promise of a better life underpins the majority of recruitment methods used by offenders, whether in attracting victims to the UK or in targeting vulnerabilities such as financial difficulties, substance abuse, family breakdown and homelessness in UK nationals.
- 154. Although some offenders use the internet to target, attract or make initial contact with potential victims, the majority of recruitment still takes place face-to-face.
- 155. EU nationals seeking work in the UK are at risk of recruitment through bogus UK agencies offering employment opportunities that are subsequently paid below the National Minimum Wage and outside of agreed terms. In such cases, potential victims are misled in relation to their employment and legal status within the UK, increasing their vulnerability to exploitation.
- 156. Irregular migrants arriving in the UK (either via facilitation or independent travel) may be targeted by offenders, often within their diaspora community who exploit victims’ vulnerability as a result of their irregular status in the UK.

Transit

- 157. Offenders often move victims around the UK, both accompanied and unaccompanied, in order to exploit them. Victims are moved using public transport, private vehicles, taxis and hire cars.

158. Victims originating from the EU continue to arrive in the UK through both travel arranged by offenders and independently. Non-EU victims travel to the UK both on legitimate documentation and as clandestines.

159. Irregular migrants remain vulnerable to exploitation en route. Victims are regularly placed into debt bondage for their travel and exploited at various stages of their journey. Migrants travelling through areas of instability and conflict are also frequently at risk of kidnapping and detention leading to sexual and labour exploitation.

Exploitation

160. The exploitation of victims - primarily for profit - manifests itself in a number of forms, with sexual and labour exploitation being the most commonly experienced in the UK and overseas.

Labour Exploitation

161. Car washes, construction and factories continue to be the largest sectors in which labour exploitation takes place; however, identification of exploitation within agriculture has increased.

Sexual Exploitation

162. The use of ASWs continues to be the most prevalent method for advertising victims of sexual exploitation. We continue to see the exploitation of victims through on-street prostitution, but the online market provides more opportunities for offenders to maximise profit.

Criminal Exploitation

163. Criminal exploitation includes theft, fraud, drug distribution and production, however the larger portion of identified instances relates to the production of cannabis.

164. Where victims are from the UK, some are coerced into drug distribution through the county lines operating model. Homeless

and otherwise vulnerable victims are targeted and forced to commit thefts on behalf of offenders to pay off debts accrued through drug use.

Exploitation of Children

165. Child victims have been identified across all exploitation types, although they are most commonly reported in cases of child sexual exploitation (CSE). Many such cases involve UK minors transported short distances domestically before being forced to engage in sexual activity by an offender they consider their boyfriend.

Other Exploitation

166. Due to difficulties identifying potential victims and the nature of the crime, victims of domestic servitude are highly likely to be under-represented in estimates of potential victims.

167. The benefits and credits system is used as another revenue stream by offenders, who use the identities of those they have trafficked to submit claims.

Control

168. Control of victims is common to all MSHT criminal operations and can be present at any stage of the process – although it is more commonly exerted during the exploitation and transit of the victim in order to ensure continuous criminal gains. Control of victims is maintained through a number of different means, including debt bondage, physical intimidation and promoting a psychological dependency on the offender.

169. Technology is used in the control of victims, with social media and messaging platforms used in both the blackmail of victims of sexual exploitation through threats to release compromising images or information and in the extortion of families of victims subject to mistreatment and exploitation in unstable transit countries.

Forward Look

170. We assess that in the next three to five years it is highly likely that the numbers of global victims of MSHT will gradually increase, and that this will be mirrored in the UK. There is a realistic possibility that the demographics of victims and offenders of MSHT in the UK will gradually change due to the arrival in the UK of migrants displaced by current upstream events. In particular, it is likely that the numbers of South Sudanese and Eritrean victims identified in the UK will continue to increase.
171. We assess that consumer demand for services in which MSHT is evidenced (e.g. agriculture, construction, car washes) is likely to remain high. If this demand were combined with continued decreased migration from the EU to the UK, and the return of EU workers from the UK to Europe, it is likely that this would result in a change to the demographics of victims and offenders, particularly in labour exploitation. Both irregular migrants and vulnerable UK nationals would likely be at greater risk of exploitation.
172. Any reduced access to victims as a result of decreased numbers of vulnerable EU migrants is likely to see offenders use increasingly coercive methods of recruitment and control as the most easily available victim pool reduces.

Organised Immigration Crime

Key Judgements

- The nature of people smuggling is subject to regular change caused by political and legal developments in source, transit and destination countries as well as high impact events such as humanitarian crises.
- Smuggling methods frequently involve significant physical and mental suffering to the migrants involved. However, certain methods require special attention due to their life-endangering nature where victims are at high risk of hypothermia, exposure, suffocation and drowning.
- The closure of the Calais and Dunkirk migrant camps has reduced the opportunities for opportunistic attempts to enter the UK via the juxtaposed controls, but has had little impact on overall levels of OCG-facilitated migration from the near Continent. With the current decline in opportunist clandestine migrant detections in the near Continent, we assess a greater proportion of clandestine detections to be OCG-facilitated.
- The implementation of agreements between the EU or EU states and transit countries have caused bottlenecks where migrants are trapped. This could cause the displacement of people smuggling routes or humanitarian concerns.

Assessment of the Threat

Clandestine Entry (Near Europe)

173. The closure of the Calais and Dunkirk camps and enhanced cooperation by French and UK authorities have made northern France a more hostile environment for OCGs.
174. The nationalities of clandestine migrants detected by UK authorities in 2017 remained largely the same as 2016. Belgium has become a location of greater focus for the activities of organised people smugglers in the past year where smugglers of various nationalities operate. The number of smugglers located there increased after the closure of the migrant camp at Dunkirk in March 2017.
175. The closure of the camps at Calais and Dunkirk has made it more likely that migrants who are still determined to reach the UK will turn to organised crime groups as the options for opportunist illegal migration are reduced. Intelligence indicates that some migrants are returning to the Dunkirk and Calais areas with small impromptu camps emerging where migrants can contact facilitators, but it is not clear what effect this will have on organised people smuggling.
176. People smugglers continue to favour hard sided refrigerated lorries to transport migrants to the UK. They also attempt to smuggle migrants in concealments in vans. Opportunist migrants attempt entry in soft-sided vehicles. These preferences are reflective of the capabilities of each group.
177. A recent NCA operation disrupted a cross-continental Iraqi-Kurd people smuggling OCG which was based in the north east of England. The OCG was capable of providing an end-to-end service from Iraq to the UK, including travel within the EU and across the Channel using complicit lorry drivers and constructed concealments. The migrants

would be dropped off at pre-arranged times and places in the UK for collection. Payments were made using ‘hawala’ (and other similar) providers.

178. The large transportation capability of this OCG made the disruption of it significant: the group had the capacity to transport hundreds of migrants into the UK illegally. The case also demonstrates the effectiveness of cross-agency cooperation, both with UK agencies/forces and partners in Belgium, France and the Netherlands.

Clandestine People Smuggling

179. Large-scale maritime people smuggling to the EU in the Mediterranean region continued into 2017. The overall figures were lower than in 2015-16, largely because the flow of migrants through the Eastern Mediterranean, specifically by sea from Turkey to Greece, has greatly reduced. The main reduction occurred following the closure of borders in the Balkans and the EU-Turkey deal in March 2016, and has also been affected by increased security on Turkey’s eastern borders.
180. People smuggling in the Central Mediterranean was severely disrupted from July 2017 due largely to fighting between militia groups in and around the Libyan coastal town of Sabratha.
181. The mistreatment of migrants in Libya, or on their way there, appears to have become systematic to the point of becoming part of the people smugglers’ business model. Migrants are frequently robbed, or detained in camps and extorted, with their relatives being threatened with the migrant being imprisoned, tortured or killed. Mistreatment has included torture, rape, and murder, with some migrants coerced into forced labour or prostitution.
182. The financial aspects of people smuggling comprise a number of elements including migrant payments, the consolidation

and transmission of funds, investment and protection of criminal assets, people smuggling logistics, and predatory activities. Hawala (and other similar service providers) and money transfer services are popular in source and transit countries for irregular migration and often feature in people smuggling finances.

Air Facilitation

183. Air facilitated migration remains a major threat to the integrity of the UK border, although there are far fewer detections of irregular migrants arriving in the UK via this method than is the case with clandestine entry. Air facilitated migration is necessarily more reliant on OCGs than clandestine migration: a clear route (and potentially false, fraudulently obtained, or illegally modified documents) would be required to enter the UK in this way, thus increasing the cost and limiting the likely market.

False Documents

184. False identity documents remain a key enabler of OIC with counterfeit, forged or fraudulently obtained documents regularly detected at the UK border.

Abuse of Legitimate Entry and Leave to Remain

185. Abuse of legitimate routes of entry continues to be a major threat, evidenced through asylum and human rights claims after arrival and detections of migrants working in breach of their visa conditions or overstaying their leave. Facilitation by OCGs and other facilitators (including overseas travel agents, visa agents and UK-based immigration representatives) continues to be the key enabler for migrants attempting visa fraud. Most migrants facilitated this way intend to remain in the UK indefinitely.

186. There has been a reduction in the overall number of migrants attempting to fraudulently obtain legitimate leave to enter or remain in the UK using deception. This is attributed to the tightening of immigration rules, improved entry clearance decision making, and the revocation of the sponsor licences of many abusive sponsors.

Forward Look

187. OCGs facilitating illegal migrants will continue to be an issue for the UK. The hotspots both in the near Europe area and further upstream are unlikely to change in the next 12 months. However, we assess that single events have the potential to radically shift patterns of migration upstream.



Prosperity

Money Laundering

Fraud & Other Economic Crime

International Bribery, Corruption & Sanctions Evasion

Cyber Crime

Money Laundering

Key Judgements

- There is no reliable estimate of the total value of laundered funds that impacts on the UK. However, given the volume of financial transactions transiting the UK, there is a realistic possibility the scale of money laundering impacting the UK annually is in the hundreds of billions of pounds.
- The ease with which UK companies can be opened, and the appearance of legitimacy that they provide, means they are used extensively to launder money derived both from criminal activity in the UK and from overseas.
- Criminal exploitation of accounting and legal professionals, particularly those involved with trust and company service provision, continues to pose a significant threat.
- Money laundering through the capital markets is an evolving threat.
- Trade based money laundering (TBML) is a complex global issue and a key method of money laundering impacting on the UK.
- A small but growing number of criminals are laundering money using cryptocurrencies.

Assessment of the Threat

188. There is no reliable estimate of the total value of laundered funds that impacts on the UK. However, given the volume of financial transactions transiting the UK, there is a realistic possibility the scale of money laundering impacting the UK annually is in the hundreds of billions of pounds.

189. The UK's large, open financial sector is a global centre for legitimate business. This is also attractive to money launderers because of the plethora of professional services and the complex and varied ways available to launder money. Although the majority of financial services and professional providers are not criminally complicit or negligent with regards to money laundering, these are areas of high risk and remain crucial enablers for disguising the origins of funds.

190. Law enforcement agencies are more frequently observing criminal funds progressing from lower level laundering being accumulated into larger sums to be sent overseas through more sophisticated methods, including retail banking and money transmission services.

191. The risk to regulated sectors from money laundering is heightened when interacting with the unregulated sector, where similar money laundering risks exist from a lack of due diligence and awareness.

192. The overseas jurisdictions that have the most enduring impact on the UK across the majority of the different money laundering threats are: Russia, China, Hong Kong, Pakistan, and the United Arab Emirates (UAE). Some of these jurisdictions have large financial sectors which also make them attractive as destinations or transit points for the proceeds of crime.

High-End Money Laundering (HEML)

193. HEMLⁱ using corporate structures and financial markets to launder billions of pounds of illicit funds, continues to come to the attention of law enforcement and regulators.
194. HEML is facilitated by the abuse of legitimate processes and services. UK corporate entities, such as Limited Liability Partnerships (LLPs) and Scottish Liability Partnerships (SLPs), have been specifically set up and exploited by UK and overseas criminals to facilitate money laundering.
195. In 2016, to make beneficial ownership more transparent, the UK introduced the People with Significant Control (PSC) registration requirements for UK companies. In 2017, each UK Overseas Territory and Crown Dependency was required to establish, where one did not already exist, a centralised register or platform of beneficial ownershipⁱⁱ. It is too early to judge the impact of the registers.

Capital Markets

196. The aspects of London's capital markets that make them successful for legitimate business are also attractive to criminal enterprises including international money launderers. The sheer scale of trading is a vulnerability, challenging relevant firms (including banks, brokerages and investment management firms) and regulators to identify instances of money laundering.

i High end money laundering (HEML) is defined as the laundering of large amounts of illicit funds through the financial and professional services sectors. It exploits the global nature of the financial system, often transferring funds through complex corporate vehicles and offshore jurisdictions.

ii All British Overseas Territories with financial centres and Crown Dependencies now maintain registers of beneficial ownership (name, address, DoB, nationality) of which requests can be made by anyone in law enforcement. This information is shared under standards agreed in the Exchange of Notes signed in 2016.

FX Trading and ABPs

197. The threat of criminals abusing foreign exchange (FX) services for money laundering remains. HMRC have introduced a new registration system to better identify those FX businesses under its supervision. The new registration process differentiates the financial services provided by businesses and, as a result, HMRC's understanding of the sector will increase.
198. Some criminals are using Alternative Banking Platforms (ABPs)ⁱⁱⁱ to launder money whilst avoiding scrutiny from the regulators.

Property Markets

199. Criminals continue to purchase property in the UK, in particular within the London super-prime property market, through companies and trusts. It is legal to use a special purpose vehicle (SPV) to buy property; this is a commonly used method to reduce the level of tax owed, however like many areas of the legitimate business world it is open to abuse.

Professional Enablers

200. Professional enablers (PEs) can be complicit, negligent or unwitting but are key facilitators in the money laundering process and often crucial in integrating illicit funds into the UK and global banking systems. Some types of money laundering, and in some instances the predicate offence e.g. fraud, necessitate the services of professionals, who may not necessarily be complicit in the criminality.
201. The criminal exploitation of accounting and legal professionals, particularly those involved with trust and company service provision, poses the greatest money laundering threat, as these professionals

iii ABPs are a form of shadow banking that uses bespoke software to provide online banking services without the regulated and auditable assurance. Accounts can be accessed from anywhere in the world. They are an effective way of transferring ownership of money to multiple individuals within a single regulated bank account, without the transfers being reflected in traditional banking transactions.

are used to set up corporate structures which are often key enablers in high-end money laundering. Corrupt individuals inside financial institutions also pose a threat.

Trade-Based Money Laundering (TBML)

202. TBML is a complex global issue shared by and affecting jurisdictions across the world; criminals engaged in TBML take advantage of the jurisdictions' varying standards and regulations.
203. Almost any kind of goods, service or sector can be used for TBML. Criminal funds from known jurisdictions of money laundering risk, including jurisdictions with a high risk of bribery and corruption, are being invested in UK businesses. Businesses dealing in high value items, such as gems and precious metals, have been complicit in laundering criminal funds, masking criminal monies with the business' naturally high turnover.

International Controllers

204. International controller networks continue to be used by UK criminals to move cash and value. Controllers based overseas coordinate collectors in the UK and across the globe using satellite networks.
205. International controllers make use of a number of methodologies to transmit value including cash smuggling, MSBs, TBML, third party UK bank accounts and bank accounts held in the name of front companies.

Cash

206. Cash is a frequently used tool in money laundering, offering anonymity and providing a break in the audit trail at any stage of the laundering process. Cash intensive businesses, such as scrap metal wholesalers, nail bars and takeaways, and some firms in the regulated sector (e.g.

MSBs), continue to be used to disguise illicit money.

207. As UK banks and financial institutions continue to de-risk business, including the remittance industry, it is likely that criminals will increasingly use other methods to move illicit funds.
208. Money laundering from cash being smuggled by air passengers and Ro-Ro^{iv} traffic remains a significant threat. Some OCGs use sophisticated concealment methods to move cash across borders, whilst others make no attempt to hide their cash. Cash is seized from air passengers frequently journeying to known jurisdictions of risk for money laundering and other criminality.

Forward Look

209. As the UK moves towards exiting the EU in March 2019, UK based businesses will almost certainly look to increase the amount of trade they have with non-EU countries. We judge this will increase opportunities for criminals to carry out TBML.
210. We assess that criminals will increasingly use cryptocurrencies to move illicit funds across borders. The value of cryptocurrencies is significantly volatile, but their relatively high price (of Bitcoin - BTC - in particular) makes it easier to transfer large amounts of fiat currencies^v in smaller volumes of cryptocurrencies.
211. The UK will start to introduce Unexplained Wealth Orders (UWOs)^{vi} in 2018. The effect this will have on the UK being viewed as a safe place to launder illicit funds is likely to depend on the amount of assets successfully recovered as a result of UWOs. In many cases the assets may have to be recovered through civil litigation under the Proceeds of Crime Act.

iv Roll-on/Roll-off. Vehicles transported by ships at UK ports.

v 'Fiat currencies' are those which governments have declared to be legal tender but are not backed by a commodity (e.g. gold). Fiat currency (also known as 'real money') examples are US dollars and GB pound sterling.

vi Unexplained Wealth Orders were a key element of the Criminal Finances Act which received Royal Assent in April 2017.

Fraud and Other Economic Crime

Key Judgements

- Fraud is the most commonly experienced crime in the UK. The Crime Survey of England and Wales 2017 indicated that there were 3.4 million incidents of fraud in the financial year ending March 2017.
- Our understanding of fraud in the UK is hampered by under-reporting; less than 20% of incidents are reported to the police.
- Data breaches continue to be a key enabler of fraud. Personal and financial information obtained in a breach can be used to commit frauds affecting individuals, the private and public sector.

Assessment of the Threat

212. Fraud continues to be the most commonly experienced crime in the UK and the Crime Survey of England and Wales indicates that there were 3.4 million incidents of fraud in the financial year ending March 2017. The 2017 Annual Fraud Indicator (AFI) estimates that fraud costs the UK economy £190 billion per year with the private sector being the worst affected with an estimated loss of £140 billion. The public sector could be losing £40.4 billion per year and individuals £6.8 billion per year.
213. Our understanding of fraud in the UK is seriously hampered by under-reporting with less than 20% of incidents believed to be reported to the police. Most fraud in the private sector is believed to go un-reported as businesses are concerned about the adverse publicity or may simply not be aware of the fraud. The harm is not just financial; some frauds against the individual can cause significant psychological damage.
214. Large-scale data breaches have continued to be reported during 2017 along with more frequent lower level attacks. Information from data breaches is sold via online marketplaces with cryptocurrencies being the preferred method of payment.

215. Some investment frauds and the majority of computer software service fraud are known to be perpetrated from overseas.

Fraud against the Individual and Private Sector

216. Analysis of all data sets submitted to National Fraud Intelligence Bureau (NFIB) indicates that the most commonly reported frauds in the six months ending September 2017 were cheque, plastic card and online banking frauds, application fraud (exc. mortgages), online shopping frauds and advanced fee frauds. Organised crime groups have been identified conducting these fraud types and we judge that a significant proportion of these frauds are likely to be conducted by groups or networks.
217. Business email attacks used to conduct mandate fraudⁱ, CEO fraudⁱⁱ and

i Mandate fraud is where fraudsters obtain details of direct debits, standing orders or account transfer details and amend them to transfer monies to other accounts.

ii CEO fraud is where a member of an organisation receives correspondence from someone purporting to be a senior member of the same organisation requesting for a payment to be made from the business bank account.

conveyancing fraudⁱⁱⁱ are increasingly one of the major reported fraud threats facing UK businesses. They use phishing emails as a means to compromise customers' security and personal details and gain access to email accounts.

218. Cyber-enabled crimes are becoming increasingly complex with fraudsters using more sophisticated techniques to target victims. The rise in impersonation and deception frauds, where a criminal approaches a customer purporting to be from a legitimate organisation, is an increasing concern. When fraud involves multiple victims there is highly likely to be a network behind the crime.

Fraud against the Public Sector

Fraud against the UK tax system

219. Organised crime groups undertake coordinated and systematic attacks on the tax system. Losses related to tobacco fraud are the highest with an estimated £2.4 billion lost in 2015/16, while alcohol fraud led to an estimated loss of £1.3 billion. Missing Trader Intra-Community (MTIC) fraud, an aggressive and organised VAT fraud that costs £0.5-1 billion per year is also a significant threat. It is conducted through contrived trading chains and can involve any commodity which is liable to VAT.
220. Other current threats include labour fraud in construction (fraudsters infiltrating the construction sector and using contrived chains of subcontractors to avoid the payment of VAT and direct taxes to HMRC on large construction projects) and payroll company fraud (organised criminals taking on the role of an outsourced payroll provider to complicit or unwitting genuine businesses and not paying employees or remitting taxes to HMRC).

ⁱⁱⁱ Conveyancing fraud is where a conveyancer or their client involved in the buying/selling of a property receives an email purporting to be from the other party confirming a change to bank details into which any monies should be paid.

Fraud against the UK benefit and tax credits system

221. The Department for Work and Pensions (DWP) final estimates show that the total monetary value of fraud in the benefit system in 2016/17 was £2 billion, or 1.2% of total benefit expenditure. This represents a slight increase on the previous year. It still remains difficult to estimate how much of this is opportunist fraud and how much is carried out by organised criminals.

Fraud against other areas of the public sector

222. Fraud against other central government departments, outside of DWP and HMRC, is less well understood. Government departments have improved their reporting mechanisms with total detected fraud increasing from £29.7 million in 2014/15 to £73.6 million in 2015/16. This is likely to be the tip of the iceberg with the NHS alone estimating that fraud cost at least £1.25 billion in 2015/16.

Market Abuse

223. The FCA broadly defines three types of behaviour as market abuse: the misuse of inside information; the manipulation of markets; and the issuing of misleading statements. The challenges in distinguishing trading based on inside information or trading that is manipulative from the large volume of legitimate trading undertaken each day is complex, highly technical work which makes it difficult to quantify the overall scale of market abuse, although its prevalence in UK markets is not considered to be out of line with other major financial centres.
224. As well as cases involving traditional insider dealing and market manipulation activity, we continue to see examples (mainly in the US) where market-sensitive information has been stolen by cyber criminals - a practice known as 'outsider trading' because it negates the need for a human

insider. Historically, the main targets have been financial and legal firms but several recent attacks suggest that this threat is diversifying to other sectors which may be less experienced and/or effective at protecting the sensitive information they hold. The use of the internet to disseminate misleading information about companies also appears to be a developing market abuse threat in major financial centres across the world.

Counterfeit Currency

- 225. Organised crime groups based in the UK continue to be involved in the counterfeiting of Bank of England £20 notes. Both Scottish and Northern Irish notes have also been targeted. Bank of England notes are most at risk in terms of the total volume of counterfeits. Scottish and Northern Irish notes are most at risk in terms of vulnerability & relative volume.
- 226. The new style £1 coin and polymer £10 notes that have been issued during 2017 have increased security features.

Forward Look

- 227. It is highly likely that reporting of fraud will continue to show a steady rise over the next 12 months. The continued push for easily accessible online services will continue to provide opportunities for fraudsters. Large organised networks will continue to target UK victims constantly adapting or changing their methodologies to deceive their victims.
- 228. The large data breaches in 2017 will fuel an increase in fraud in 2018, however the General Data Protection Regulation (GDPR) will apply in the UK from May 2018 and will introduce significant fines for businesses that suffer data breaches due to inadequate protective measures. The intention is this will make businesses more responsible with the personal data they hold eventually leading to a reduction in the instances of data breaches.

International Bribery, Corruption & Sanctions Evasion

Key Judgements

- The UK remains a prime destination for foreign corrupt Politically Exposed Persons (PEPs) to invest in. Russia, Nigeria and Pakistan are the most commonly seen source countries for PEPs investing in the UK.
- Some UK registered companies pay bribes overseas in order to conduct business.
- The ease of opening UK companies means they are used frequently to enable corrupt activity. Companies based in British Overseas Territories are also used both to disguise ownership and to conceal corrupt payments.

Assessment of the Threat

Corrupt Politically-Exposed Persons

229. The UK is a prime destination for foreign corrupt PEPs to launder the proceeds of corruption. Investment in UK property, particularly in London, continues to be an attractive mechanism to launder funds. The true scale of PEPs investment in the UK is not known, however the source countries that are most commonly seen are Russia, Nigeria and Pakistan.

230. Companies registered in British Overseas Territories and other offshore jurisdictions offering secrecy and low taxes continue to be used to disguise ultimate beneficial ownership of UK based assets owned by corrupt PEPs. The use of accounts in family members' names is also a common method to launder corrupt funds. UK property is also used to move money, either for the purposes of money laundering or bribery.

231. A small number of UK-based professional enablers (solicitors, accountants, estate agents and trust and company service providers) continue to assist corrupt

PEPs to invest in the UK. In the majority of instances professional enablers are complicit although some may be unwitting or negligent.

232. Regime change in developing countries may appear to bring opportunities to work with new governments, but where the underlying infrastructure relies on bribery and corruption to function efficiently, similar problems remain and incoming governments become susceptible to corruption.

International Bribery

233. UK registered companies continue to bribe overseas to improperly secure new business, extend existing contracts or to obtain sensitive information about competitors. As well as being a crime in its own right bribery can lead to other societal harms, for example, bribes paid to secure a contract using sub-standard material could have health and safety consequences.

234. Intermediaries, or 'agents', remain the most common method through which UK entities pay bribes overseas. It is assessed that

some intermediaries wield significant power and influence in a region such that their role is greater than simply facilitating bribe payments.

Sanctions Evasion

235. Sanctions evasion undermines foreign policy objectives and poses a significant risk to the UK's reputation. The scale of financial sanctions breaches is unknown however the expanded use of high profile international sanctions, strongly backed by the UK, against regimes such as the Democratic People's Republic of Korea (DPRK), has increased the risk to the UK of sanctions evasion.

Forward Look

236. As the UK moves towards exiting the EU in March 2019, UK-based businesses may look to increase the amount of trade they have with non-EU countries. We judge this will increase the likelihood that UK businesses will come into contact with corrupt markets, particularly in the developing world, raising the risk they will be drawn into corrupt practices.

237. To meet the UK's future sanctions obligations, new legislation is being prepared before the UK leaves the EU. The public and private sector in the UK will have to incorporate any new requirements that this legislation brings.

Cyber Crime

Key Judgements

- UK cyber crime continues to rise in scale and complexity. 2017 witnessed a significant expansion in the visibility of cyber crime. High profile attacks such as the WannaCry ransomware campaign, which impacted heavily on UK NHS services, emphasised the real world harms resulting from such attacks, including impact on collateral victims.
- The distinction between nation states and criminal groups in terms of cyber crime is becoming frequently more blurred, making attribution of cyber attacks increasingly difficult.
- Cyber crime groups, many of which operate internationally and are Russian-speaking, continue to pose a threat to UK interests. International groups are behind high impact attacks by credential-stealing malware and many of the most damaging confrontational malware variants. The threat from UK domestic cyber criminals continues to mature, and these domestic actors are capable of damaging attacks.
- The technical capabilities of malware have evolved, increasing the impact and threat posed by these criminal tools. Criminals, however, continue to exploit long-standing and well-known vulnerabilities in victim infrastructure.
- Under-reporting of data breaches continues to erode our ability to make robust assessment of the scale and cost of network intrusions. Many companies are not disclosing data breaches, putting victims at risk.

Assessment of the Threat

238. Indicators of the scale and complexity of UK cyber crime point to a continued rise, with 2017 witnessing a significant expansion in the visibility of cyber crime through high profile ransomware campaigns.

239. Under-reporting of cyber crime is a continuing problem. Just 38% of people in a survey said they had confidence in the law enforcement response to cyber-dependent crime. Those that do report may on occasion not be prepared to support prosecution, hampering the ability of law enforcement to act.

240. Recent case examples have highlighted the wide variation in sentencing for Computer Misuse Act (CMA) offences. Whilst courts acknowledge the seriousness of the

crimes committed, the level of sentence passed does not necessarily reflect this seriousness, and can appear low. As many convictions are under the Fraud Act rather than the CMA, this compounds the problem and furthers the perception of 'cyber crime without consequence'.

Victimology

241. 2017 saw cyber crime financially disadvantage and cause tangible disruption to the UK public and commerce. The Equifax breach leaked personal data of around 700,000 UK victims, failing customers and placing victims at risk of frauds. WannaCry, meanwhile, had a tangible impact on the operation of the NHS, forcing some hospitals to divert ambulances and cancel operations.

242. Our 2017 assessments noted the changing tactics of cyber criminals, increasingly targeting businesses over individuals and we continue to see this. Additionally, the WannaCry and NotPetya ransomware campaigns have highlighted the risk of falling victim as collateral damage to attacks primarily targeted elsewhere. Whilst the NotPetya campaign focussed on Ukraine, significant victims in the UK and other countries were impacted, with costs to those victims reported to run to between US\$200–300 million.
243. Businesses in the supply chain are a noteworthy victim type. A software update for CCleaner, a popular software utility, was hijacked with malicious code. The reason CCleaner was targeted for attack appears to be its role as a trusted third party for larger companies, making it especially effective as a Trojan horse.
244. Even an organisation that has invested heavily in defending its own networks can still be vulnerable to a compromise of its third party suppliers. Moreover, from a criminal perspective, attacking through compromise of a third party product opens up a wider range of potential victims, as all users of the compromised services can be impacted. Those impacted organisations need not have been intended as victims by the criminals, but become collateral victims.

Criminals

245. The UK-based cyber threat is diverse and ranges from internationally-connected OCGs to individuals (often teenagers, who only have low-level technology at their disposal, but nevertheless are capable of causing critical national incidents - e.g. the 2016 Mirai botnet attacks on the UK banking industry). Such individuals can have relatively limited knowledge, but have ready access to forums from which to learn methodologies. They are unlikely to have been involved previously in other crime and in many cases are not driven by financial reward, but rather the acquisition of reputational kudos amongst their peers.
246. Our understanding of UK-based criminals has developed and intelligence now points to organised cyber crime groups operating in the UK that communicate directly with international criminal groups behind the most impactful malware strains. These UK groups are themselves capable of significant international disruption, and appear to be motivated by profit.
247. Different OCGs have been seen deploying the same malware. In some cases this is because the malware is available as-a-service and traded online, but in others the reasoning for shared use is an intelligence gap.

Criminality

Financial Trojans

248. The most prolific banking Trojans impacting on the UK in this period have been Dridex, Carbanak, Trickbot and Emotet. The emergence of two relatively new financial Trojans (Trickbot and Emotet, both of which emerged as significant threats in 2017) is unusual; the technical complexity and costs of developing malware of this type makes them difficult to bring to market. The emergence of Trickbot and Emotet so close together in time is likely to be an anomaly rather than indicative of a fundamentally broadening criminal marketplace.

Network Intrusion

249. Network intrusion remains a key threat and represented the most reported category of cyber crime incidents directly into the NCA. A general increase in scale is becoming apparent: 2017 saw the full extent of the 2013 Yahoo breach disclosed when Yahoo confirmed that the network intrusion exposed information related to one billion accounts, making it the largest ever to be disclosed. The largest breach of 2017

occurred in May when credit monitoring agency Equifax experienced a breach of records of around 700,000 UK residents, with around 29,000 having their driving licence details stolen.

Ransomware

250. Action Fraud observed ransomware continuing as the main threat facing the UK public. In 2017 we assessed it likely that the number of new strains would plateau, but industry figures indicate growth in new strains continues.
251. The WannaCry ransomware infections in May 2017 were a watershed moment for the perception of the ransomware threat. The most high profile UK impact was on the NHS services and treatment plans. Also, small-medium sized enterprises (SMEs) were heavily impacted by WannaCry, with many saying it took weeks to return to normal. NotPetya attacks in June, though not strictly ransomware, further highlighted the threat.

DDoS Attacks

252. After dipping somewhat earlier in 2017, the volume of DDoS (including DDoS for extortion) incidents reported both formally as a crime and through the NCSC and NCA industry engagement channels have increased markedly through the second half of 2017. The severity of DDoS is also increasing with an industry survey suggesting that large DDoS attacks of over 50 Gbps have quadrupled between 2015 and 2017, with an increasing number of companies reporting attacks over 1 Tbps.
253. 'Internet of Things' (IoT) devices represent the greatest emerging botnet threat. The Mirai botnet, in 2016, delivered one of the largest DDoS attacks ever witnessed. The Mirai malware has since been overtaken by the Hajime malware, which has amassed a compromised network of devices much larger than even Mirai at its peak.

Exploits

254. Cyber criminals have increasingly incorporated existing exploits into their malware in this period. In April 2017 the OCG known as 'Shadow Brokers' released onto the open Internet the 'EternalBlue' exploit (amongst others) that in May was used to facilitate the widespread WannaCry ransomware infections. This illustrated clearly the threat of exploits being provided as-a-service.

Exploit Kits

255. There has been a significant downturn in the exploit kit market, with very few new exploit kits emerging. A number of factors are likely to have contributed to the decline of exploit kits, including the diminished availability of suitable browser exploits. Exploit kits, however, remain a potent tool for cyber criminals, and even rudimentary ones still represent a threat, especially if security updates are not regularly applied.

Botnets

256. Botnets are noteworthy for the longstanding threat they have posed for DDoS attacks and the delivery of malware. In the past few years, where other delivery mechanisms - such as exploit kits - were disrupted, a correlated uptick in spam activity from botnets would be seen. This suggests that criminals view them as a safe and reliable backup.
257. Necurs continues as the largest active spam botnet, delivering a range of payloads. With over 1 million active bots online at any given time, it plays a pivotal role in the delivery of malware worldwide. The botnet has been used to launch spam campaigns containing credential-stealing malware, as well as ransomware variants. Necurs also has the capability to launch DDoS attacks.

i National Cyber Security Centre - a part of GCHQ

Social Engineering

258. Social engineering as a facilitator of cyber crime continues to be used by both low-skilled cyber-enabled fraudsters and highly technically skilled cyber criminals. Criminals have addressed some of the previous weaknesses in their social engineering campaigns – we can no longer rely on criminals making the types of basic mistakes – such as poor grammar or spelling in cover documents – that were previously a pointer to a social engineering attack.

Spamming and Phishing

259. Overshadowed in the focus on software vulnerabilities after WannaCry, spamming and phishing continues as a significant threat. An industry survey of 100 UK IT professionals has found that over 75% had dealt with a security incident that was traced back to a phishing email.
260. Cyber criminals continue to exploit current events for their phishing hooks. Action Fraud note phishing emails warning supposed victims about the Equifax breach and emails relating to WannaCry, purporting to be sent by BT.
261. HMRC has seen an increase in the number of phishing emails with HMRC branding from approximately 263,000 in the first half of 2016 to 553,000 in the equivalent period in 2017. Despite this increase, the percentage falling victim to phishing emails through disclosing personal information or downloading malware has declined, indicating an increase in customer awareness.

Money Services

262. Cryptomining malware, which infects a victim device and surreptitiously mines cryptocurrencies, has increased during this period. According to industry, more than 1.65 million computers worldwide were infected with cryptomining malware

during the first nine months of 2017. We assess it is highly likely that deployment of cryptomining malware has increased even further in the period since October 2017 – driven to a large extent by the general increase in exchange rates of cryptocurrencies such as Bitcoin.

263. The majority of cyber crime continues to be undertaken for financial gain and in these cases the ability to cash out forms a critical aspect of the criminal business model. We have identified money exchange services (that operate similarly to PayPal) that facilitate predominantly criminal-to-criminal payments. Whilst not explicitly criminal, they often additionally promise greater anonymity and an unwillingness to cooperate with law enforcement.

Forward Look

264. The General Data Protection Regulation (GDPR) comes into force from May 2018. The provision of the regulation allows for significant fines against organisations responsible for a serious breach. The effect of GDPR is likely to be a much richer picture of the true scale - both size and regularity - of data breaches in the UK. Recent industry surveys (October 2017) suggest that awareness of and preparedness for the introduction of GDPR is limited, particularly amongst small and medium sized enterprises.



Commodities

Firearms

Drugs

Firearms

Key Judgements

- Handguns and shotguns are the most commonly used criminal firearms in the UK. Recoveries of automatic weapons are increasing, albeit from a low level.
- There has been an upward trend in criminal discharges, with the majority of weapons not having been previously used. This indicates a fluid illicit supply via UK and overseas sources.
- Converted, modified and reactivated firearms represent a sizable proportion of the illicit firearms market.
- Risks remain around the importation and criminal use of antique and obsolete revolvers, with adapted/'home-loaded' ammunition.
- Discharge and seizure data point towards an increasing availability of ammunition on the criminal market.
- Whilst the vast majority of Registered Firearms Dealers are law abiding, a number of high profile investigations have identified vulnerabilities for criminal exploitation.
- A strong connection between drugs supply and the use / recovery of firearms illustrates that firearms are used to protect and enable wider criminal interests.
- Whilst firearms make up a small proportion of commodities sold via the dark web (drugs are the majority), it remains a viable avenue for acquisition and supply.
- Upstream supply from eastern Europe presents an ongoing threat, including via the near-Europe nexus.

Assessment of the Threat

Criminal Possession, Use and Supply

265. The level of firearms crime in the UK remains one of the lowest in the world with offences accounting for less than 1% of reported crime. However, the Office for National Statistics (ONS) indicates a 27% increase in offending for 2016/17 (year ending June) and the National Ballistics Intelligence Service (NABIS) reports an upward trend in discharges since 2013/14ⁱ. Discharges per incident and large ammunition seizures

also indicate an increasing availability of ammunition on the criminal market.

266. The vast majority of criminal firearm discharges in 2016/17 again involved weapons not previously discharged in crime, suggesting a sufficiently fluid supply. This trend is assessed as largely due to firearms entering the UK from overseas and previously legal weapons entering criminal hands after being stolen, diverted or modified within the UK.

267. The majority of criminal firearms are handguns (pistols and revolvers), which also cause the majority of fatalities. The

ⁱ ONS statistics include offences with noxious sprays, stun devices, imitation guns and other non-lethal firearms whereas NABIS figures refer only to discharges from lethal barrelled weapons.

second most popular criminal firearm is the shotgun, with increasing incidents reported. Fully automatic firearmsⁱⁱ are seldom used in the UK.

268. Firearms converted, modified or reactivated constitute a sizable proportion of the illicit market. In addition to legislative, availability and pricing factors, this is likely to reflect the existence of illicit facilities within the UK and/or acquisition of already 'upgraded' weapons from overseas.
269. The geographical concentration of firearm recoveries and discharges continues to be in the main metropolitan areas, with some provincial forces also having significant issues (often relating to 'county lines'ⁱⁱⁱ drugs supply and community demographics).
270. There remains a strong connection between drug supply and firearms use and recovery, further indicating that firearms are used to protect and enable other criminal interests. When automatic weapons are recovered, they are usually linked to drug supply.
271. Firearms make up a small proportion of commodities sold via the dark web, with drugs being the majority. However, the dark web remains a viable avenue for acquisition and supply, including for individuals with limited or no known criminal association.

Lawful to Unlawful

272. NABIS assesses the threat to the public from lawfully-held firearms being used in crime as low. However, most shotguns used criminally in the UK are likely to have been held legally on certificate and subsequently lost, stolen or diverted before entering the criminal market. They are also modified with the barrel, stock, or both being shortened.

ii A fully automatic firearm is one that continuously discharges bullets until the trigger is released or magazine/chamber is empty and includes assault rifles and submachine guns.

iii The supply of Class A drugs from urban hubs to provincial towns.

273. The significant use and recovery in criminal circumstances of imported antique and obsolete-calibre firearms highlights continued risks around their onward supply to criminal groups (often with adapted and home loaded ammunition). Their illicit supply, including via Registered Firearms Dealers (RFDs), has led to high profile and complex operations and prosecutions. Whilst the vast majority of RFDs are law abiding, vulnerabilities for criminal exploitation have been identified. Following a Law Commission Review and new definitions under the Police and Crime Act 2017, a Home Office consultation is also underway.

International Supply

274. There remains an ongoing supply of firearms into the UK from overseas. In this regard, trafficking from eastern Europe through near Europe is a key concern. Facilitated by international transport and trading infrastructure, Belgium and The Netherlands are key nexus points of consolidation and onward trafficking of illicit commodities, including drugs and firearms. Trafficking to the UK is enabled by ferry and Channel Tunnel routes. Firearms detected entering the UK on Roll-On/Roll-Off ('RoRo') services through ferry ports are concealed in private/tourist cars (and, historically, motorcycles) or commercial vehicles.
275. In October 2017, a vehicle was used to attempt to smuggle 10 handguns, a quantity of ammunition and three sound moderators (concealed in a holdall, together with 37kg of cocaine and 7kg of heroin) into the UK via Dover on behalf of a UK-based OCG. This seizure, linked to the arrest of a UK official, is unusual in that the firearms were from more than one manufacturer and were of various models, indicating onward supply capacity.

276. Detections of firearms trafficked via general maritime (small boats/private marinas) or sea/air freight, air passenger or general aviation (light aircraft/private airfields) are uncommon. However, they remain exploited for smuggling other commodities and are viable ways of smuggling weapons into the UK.

277. Considering the current Common Travel Area (CTA)^{iv} and historic access to firearms within Northern Ireland and the Republic of Ireland, the land border between them provides another viable route for trafficking firearms to the UK.

3D metal handguns have been printed elsewhere, but their viability is uncertain and complexities and costs are prohibitive. However, technological developments and cost reduction over time, as anticipated with thermoplastics, may encourage experimentation.

Forward Look

Upstream Risks

278. The Czech Republic parliament has agreed to alter its constitution to allow for firearms to be legally held when national security is threatened. This amendment represents a challenge to EU gun control rules which typically restrict civilians from possessing certain kinds of semi-automatic weapons. As an EU Member State bordering Germany, Austria, Slovakia and Poland, there is a risk that firearms and ammunition held legally under this provision may be diverted to other countries, including the UK.

279. Other upstream firearms supply risk areas include the Western Balkans. Firearms from the region, including automatic weapons, are commonly identified in mainland Europe, including near Europe. Other more recent conflict zones such as Ukraine, Libya and Syria are considered potential threats.

Advancing Technology

280. In 2017, the first known UK seizure of 3D printed firearms was made in London, together with component parts for a firearm and a digital guide on how to produce 3D printed firearms. Complete

^{iv} The CTA is a travel zone that comprises the Republic of Ireland, the United Kingdom, the Channel Islands, Isle of Man, Jersey and Guernsey.

Drugs

Key Judgements

- Drug misuse-related deaths in the UK increased in 2017. The emergence of Fentanyl, Carfentanil, Analogues and Precursors (FCAP) has contributed to this rise: current reporting states 122 FCAP related deaths. FCAP are currently being seen in overseas drugs markets causing high numbers of deaths; their emergence in the UK is of significant concern.
- Our improved understanding of the significant harm caused by 'county lines' drug supply networks has led to an increased prioritisation to counter the threat. These groups are causing significant harm, including violence and firearms use, impacting on all police forces. The county lines groups continue to exploit young and vulnerable people, who are exposed to physical, mental and sexual harm. Groups have a proven ability to adapt their operating methods and practices in order to evade intervention and strengthen their criminal enterprise.
- OCGs are using new links with source countries to streamline their activity and provide end-to-end services. Profits are high at all stages of drug trafficking but maximised for those with upstream access.
- It is likely that the UK drugs market and the associated crime will continue to grow and cause increasing harm to the UK.
- Cocaine and heroin production have continued to rise in 2017. Demand for all common drug types remains high in the UK and the use of crack cocaine has increased. Crack cocaine is linked to county lines drugs supply networks and has been identified as a driver for an increase in serious violence.

Assessment of the Threat

281. Demand for all common drug types remains high in the UK. Profits are high at all stages of drug trafficking but maximised for those with upstream access. Increased production and supply has reduced the need for suppliers to adulterate. Consequently, cocaine and heroin purity at street level remains high.

282. British traffickers remain a significant threat and remain active within the UK wholesale market. However criminals from the Balkans continue to dominate within the wholesale cocaine market, with a presence in all major UK cities and towns and operating supply networks reaching back to source and transit countries.

283. The Office for National Statistics (ONS) report that in 2016 there were 3,744 drug poisoning deaths registered involving both legal and illegal drugs in England and Wales. This is an increase of 2% and the highest since comparable statistics began in 1993. Of these 3,744 deaths, 69% (2,593) were drug misuse deaths. 54% of all drug related deaths involved heroin and / or morphine.

Fentanyl, Carfentanil, Analogues & Precursors (FCAP)

284. In early 2017 an unusually high number of heroin overdoses occurred in the north of England. The detection of FCAP in some

post mortems led to toxicology retesting of overdose fatalities in the area, resulting in a total of 122 deaths (as of March 2018) being identified as linked to FCAP abuse. The emergence of FCAP in the UK drugs market is of concern. It has previously been seen in US and Canadian drugs markets, among others, where it has contributed to an ongoing synthetic opioid epidemic.

County Lines

285. 'County lines' relates to the supply of Class A drugs (primarily crack cocaine and heroin) from an urban hub into rural and coastal towns or county locations. County lines drug supply networks are reported to be impacting on all 43 police forces in England and Wales, Police Scotland and British Transport Police. Criminal groups continue to pose a significant threat to young and vulnerable people, who are exposed to physical, mental and sexual harm. The groups use a range of methods to identify potential victims. The consequences of county line markets include serious violence and physical harm, incidents of kidnap, use of weapons (including firearms), ruthless debt control, turf wars and homicide.
286. Gang members and those they exploit continue to be transient between urban hubs (exporting) and non-urban areas (importing) such as rural, coastal and market towns, but with an emerging trend for some offenders to settle within the community in which the county lines market is established.
287. London continues to be the predominant urban source of county lines offending, although a number of other export hubs, including Liverpool, Manchester, Birmingham and Wolverhampton (as well as other towns and cities), have been reported across the country reflecting the growth and evolution of the threat.

Upstream Production

288. Opium production in Afghanistan increased by 87% to a record level of 9,000 metric tonnes in 2017. The area of opium poppy cultivation also increased to a record 328,000 hectares in 2017, up 63% compared with 210,000 in 2016.
289. Cocaine production in Colombia has increased by 120% since 2012. Production in 2015 was 646 metric tonnes and rose 34% to an estimated 866 metric tonnes in 2016. 2017 production is estimated to be in the region of 1,000-1,100 tonnes. Coca cultivation has also surged over recent years with a 52% increase in cultivation area from 96,000 hectares (ha) in 2015 to 146,000 ha in 2016.

The Supply Chain

290. Cocaine seizures across Europe reached a record high in 2016, with 60 tonnes being seized from containers alone. We assess that the largest volumes of cocaine continue to be trafficked via canalised maritime traffic.
291. South American ports remain key locations for the loading of drug consignments via container. During the period January to June 2017, Santos in Brazil was the port of origin for over a third of all European cocaine seizures from containers.
292. Heroin continues to be trafficked in large quantities via the 'southern route' through the Indian Ocean towards Europe via South Africa and West Africa. The amount of heroin transported on the southern route appears to be growing.
293. Heroin and cocaine generate significant competition between rival OCGs from production to user. Feuds over drugs in transit, control of markets and protection of assets / income are common, often resulting in violence, kidnap and the criminal use of firearms.

294. Corruption exists at every stage of the drug supply chain. The use of corrupt port and airport officials to circumvent normal customs controls is a key aspect of all 'rip-off' activity.

Synthetics and Cannabis

295. Since January 2017, two tonnes of precursor chemicals have been seized. These chemicals are primarily used in the illicit manufacture of amphetamine and methamphetamine. Estimates suggest that this volume of precursor chemicals has the potential yield of somewhere between 1,000-1,200kg of unadulterated amphetamine sulphate with a street value of up to £40 million. During the same period methamphetamine street prices have decreased significantly; there is a realistic possibility this indicates an increase in availability. In relation to New Psychoactive Substances (NPS), China remains the predominant source of supplies entering the UK.

296. We continue to see significant seizures of cannabis at the UK border. Additionally there are regular disruptions of domestic cannabis grows, varying from as few as ten plants, up to warehouse quantities.

Forward Look

297. In order to establish a better understanding of the scale of the FCAP threat to the UK, it will be necessary to start to consistently capture intelligence from treatment providers, police forces (including testing in custody), prisons, and in post-mortem testing.

298. Reporting on global drug purchases over the dark web in the UK has increased by 7% in 2017; the United States dropped by 1.8% whilst the overall global average increased by 0.3%.

