National Crime Agency

National Strategic Assessment of Serious and Organised Crime 2015

23rd June 2015

Contents

Foreword from the Director General of the NCA

Serious and organised crime affects us all. It is a pervasive national security threat with far-reaching effects on the UK's social and economic well-being and international reputation. Its impact can be felt throughout the public and private sectors, undermining communities and destroying lives.

The threat is wide-ranging and complex – spanning everything from malware to human trafficking – and varies in depth and complexity – from simple frauds to high-end money laundering. Its perpetrators are highly innovative and tenacious in pursuing their goals; our response must be both resourceful and relentless.

To inform our response, we require a comprehensive understanding of the risk that serious and organised crime poses to the UK. The National Strategic Assessment (NSA) draws together that single picture of the risk and has been produced in consultation with a broad range of partners.

In my foreword to last year's NSA, I stressed the importance of a collaborative approach and I would like to express my thanks to all our partners for their efforts over the past year. A collaborative approach remains vital across policing and law enforcement, as we cannot solve the problem alone. Partnerships, both domestic and international, bringing together the public and private sectors, academia, charities and society as a whole, are crucial to success.

The National Strategic Assessment will inform how the NCA leads, supports and coordinates the collective national response which, I am confident, will deliver a lasting detrimental effect on serious and organised crime impacting on the UK and our interests overseas.

Keith Bristow QPM
Director General
National Crime Agency

Introduction

1. The National Strategic Assessment brings together a comprehensive picture of the risk - how serious and organised crime affects the UK and its interests. This document informs both the national response – what the priorities are and what action will be taken, and the expected results – how success will be measured.

2. On behalf of UK law enforcement the NCA's National Intelligence Hub (NIH) has drawn together the articulation of the risk. The NIH gathers and analyses all relevant intelligence material from the NCA's own sources and those of its partners and has produced this document through consultation and collaboration with partners.

3. This involved wide consultation across law enforcement, government and the agencies including police forces in England and Wales, Police Service Northern Ireland, Police Scotland, Regional Organised Crime Units, Border Force, National Offender Management Service, Her Majesty's Revenue and Customs, Serious Fraud Office, the Crown Prosecution Service, Immigration Enforcement, Cabinet Office, Home Office and GCHQ.

Strategic context

4. Serious and organised crime is a national security threat which has an impact on almost every aspect of the UK's wellbeing. Threats such as money laundering, fraud and corruption damage the nation's financial security and reputation, reducing the UK's prosperity and attractiveness as a place to do business. Cyber attacks threaten commercial activity and companies' financial stability and put the security of personal information at risk. Many of the products and services provided by cyber criminals are available for use by extremists, state actors and hacktivists, while the criminal markets supplying firearms, false documents and smuggling routes are easily exploitable by terrorists.

The impact

5. Serious and organised crime causes thousands of fatalities in the UK every year, including from drug use, high-risk illegal migration methods, and criminal use of firearms. The psychological harm from child sexual abuse is felt for years, impacting on the livelihood of children/young people and the future adult population. Individuals, often the most vulnerable, may be financially ruined by criminals stealing their life savings through fraudulent investment schemes.

6. The spread of crime can severely undermine the cohesiveness of communities and can become pervasive, with criminals trading illegal commodities without fear of discovery or being reported. In such circumstances criminal activity can become the accepted norm.

7. The cost of serious and organised crime to the UK was assessed in the past at £24 billion[1] and is now likely to be higher. The loss in tax revenue directly impacts on public finances and confidence in the Government's ability to manage them, while businesses also suffer, losing billions of pounds to fraud each year. In many cases, the crime is enabled by corruption; at the macro level this can undermine inward investment in the UK and, like money laundering, jeopardise the integrity of the UK as an international financial centre.

The changing risk

8. Technology has created a range of new opportunities for criminals. It has increased the number of ways some traditional crimes can be carried out and provided criminals with much more sophisticated enablers[2] in all threat areas. The sharing of indecent images of children, for example, is now almost entirely enabled by the internet.

9. The threat from serious and organised crime is international. Commodities such as drugs, firearms and counterfeit goods are sourced from right across the world, and Organised Crime Groups (OCGs) often have a presence in multiple jurisdictions. The global communications infrastructure enables criminals to operate across geographic boundaries, to target the UK from a distance, or to reach from the UK into other countries, undermining the UK's international reputation.

10. Although serious and organised criminals, in most cases, will not want to be associated with extremists for fear of coming under additional scrutiny, there is a risk of extremists seeking to exploit criminal contacts, for example for financial and logistical support or to source firearms and false documents.

1 Home Office (2013) *Understanding Organised Crime: Estimating the Scale and the Social and Economic Costs*. Available at: https://www.gov.uk/government/publications/understanding-organised-crime-estimating-the-scale-and-the-social-and-economic-costs

2 Enablers describe the tools and methods used by serious and organised criminals in order to pursue their criminality and include: criminal use of identity documents, professional enablers (such as solicitors and accountants) and Internet Communications Technology, etc.

The response

11. The Serious and Organised Crime Strategy has been in place for over a year. The NCA, with its mandate to lead the UK's fight to cut serious and organised crime, has introduced mechanisms to lead, support and coordinate the national response. The strategy and its delivery mechanisms are supported by the provision of new powers under new legislation for serious crime, modern slavery and counter-terrorism, and the UK Anti-Corruption Plan will bring greater coherence to tackling bribery and corruption.

12. The balance of resource against threat will need to be adjusted across law enforcement more flexibly than in the past. There is also a clear need to consider what skills and capabilities are required by police forces, Regional Organised Crime Units, and national agencies. This is particularly true in the case of cyber where the pace of technological change and the adaptability of the cyber criminal means that law enforcement will always be playing catch-up.

13. These capabilities must be placed in the agencies best able to develop and deliver them for all; and access to them must be clear, simple, and informed by shared priorities. For example, important opportunities exist, and need to be taken, to share more widely and effectively capabilities and efficiencies between the counter-terrorism and organised crime law enforcement communities.

14. Partnerships will be crucial; we will need to build on those which already exist and develop new ones. A joint operations centre is already being set up between GCHQ and the NCA to target child sexual exploitation, and we have seen genuine innovation through the creation of the Joint Money Laundering Intelligence Taskforce, bringing together law enforcement and the financial sector to tackle money laundering.

15. Such initiatives also bring opportunities to share information. With the technology available to exploit intelligence flows, relevant information needs to be shared in a timely manner to inform the tactical and strategic response.

16. Law enforcement recognises the key threats and challenges ahead and will be prioritising investment of effort and resource accordingly. An additional £10 million has been provided to fund Child Exploitation and Online Protection (CEOP) Command investigations and we will need to work hard to deliver equal effect on other threats such as organised immigration crime and modern slavery and firearms.

17. In addition there are some key legislative challenges ahead in the communications arena - were communication service providers no longer required to retain communications data, law enforcement would lose its primary and most effective tool in the fight against serious and organised criminals.

Key judgements and trends

The key points regarding the risks posed by serious and organised crime impacting on the UK and UK interests and their trends are as follows:

- Child sexual exploitation and abuse represents one of the highest serious and organised crime risks. Although we may never know the full extent of the problem, law enforcement operations and high-profile cases have given us a much better insight into the scale and the challenges it presents.
- The risk from firearms remains high. They continue to enter the criminal market through a variety of means, including direct importation through post/fast parcels and thefts from legitimate firearms holders or dealers.
- The risk from organised immigration crime, human trafficking and modern slavery has increased. The volume of migrants attempting to enter the UK illegally continues to grow and to fuel increasing labour exploitation.
- The risk from criminal exploitation of the internet and related technology remains high and continues to develop. The cyber crime marketplace presents a particular threat.
- Money laundering is now considered a high-priority risk in its own right. It is essential for the realisation of criminal proceeds across almost all types of serious and organised crime and its sheer scale presents a strategic threat to the UK's economy and reputation. High-end money laundering, in particular, is a major risk.
- Bribery and corruption (including the laundering of the proceeds of corruption, for example by Politically Exposed Persons (PEPs)) is a critical enabler to all criminality types and damages the UK economy.
- Fraud continues to cost the UK billions of pounds and remains a high priority. As more government services go online and the UK becomes an increasingly cashless society, the opportunities for cyber-enabled fraud will increase and attract growing criminal interest.
- The social and economic costs due to heroin and cocaine are still severe. During 2015 we expect supplies of cocaine and amphetamine to remain stable with demand for cocaine increasing.
- All cross-cutting threats and vulnerabilities play an important part in most serious and organised crime. False identity is used to get illegal migrants into the UK to commit fraud and to provide anonymity online; drugs, firearms and laundered money exploit border vulnerabilities; foreign nationals are involved in all types of serious and organised crime and can be difficult to track; and serious and organised criminals continue their criminality from prison.

National Control Strategy

The National Strategic Assessment informs the National Control Strategy for 2015/16, which prioritises, as high priority, priority or significant, the threats and cross cutting issues identified in this document. The National Control Strategy provides a framework that informs the deployment of the UK's resources against the highest risks; a high-level summary of those threats posing the greatest risk is shown below.

The Control Strategy outlines mitigating actions to be taken by the NCA and its operational partners in line with the Government's Serious and Organised Crime Strategy.

Summary of national priorities

	Child Sexual Exploitation and Abuse	Cyber	Drugs	Economic	Firearms	Organised Acquisitive Crime	Organised Immigration Crime	Money Laundering
Threats	Contact child sexual abuse	International cyber crime marketplace	Cocaine	Fraud against the private sector, individuals and charities	**Firearms** (including international supply, domestic supply, legitimate supply, technology and emerging trends)	Organised vehicle crime	Human trafficking & modern slavery	Money laundering
	Indecent images of children	Multinational cyber criminal (groups) targeting the UK	Heroin	Fraud against the public sector			Clandestine people smuggling	
	Online child sexual exploitation	Major UK-based cyber criminals and criminal infrastructure	Cannabis	Bribery & corruption			Facilitation of illegal immigration	
	Transnational child sex offenders	Cyber attacks targeted at UK victims	Synthetic drugs inc NPS[1]	Emerging new crimeware			Abuse of legitimate means to remain	
		Emerging new crimeware					False documents	
Cross Cutting Threats	Corruption (cross-cutting)							
	Criminal use of internet technology (cyber-enabled)							
	Prisons & lifetime management							
	Border vulnerabilities							
	Foreign national offenders							
	Criminal use of identity							

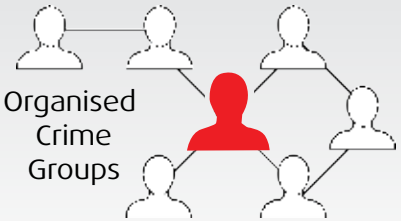
1. NPS – New Psychoactive Substances

High Priority Priority

Serious and organised crime overview

WHO

High Priority Criminals



Professional Facilitators

Foreign National Offenders

HOW

BORDER VULNERABILITIES

- Criminals **disguise** or **conceal illegal commodities** within the high volume of legitimate traffic
- Project TOYER prevented the exportation of stolen vehicles worth **£1.2 million**

Over **7,000** serious and organised criminals **in prison**

PRISONS & LIFETIME MANAGEMENT

CORRUPTION

- **Abuse of authority and systems** used for financial gain and other corrupt behaviour

IDENTITY ABUSE

Occurs through outright **theft, social engineering** and **data harvesting**

Online marketplace providing **easy access to criminal services**

TECHNOLOGY

Anonymisation tools **protect criminals** from law enforcement action

WHAT

MONEY LAUNDERING

CYBER
GameOverZeus targeted accounts worth **£100 million**

DRUGS
- UK **heroin purity** on upward trend across whole supply chain
- UK cocaine market **biggest in Europe**

ECONOMIC CRIME
- HMRC estimates UK tax revenue loss of **£5.4bn per year**
- Card & remote banking fraud losses **over £247m** Jan-Jun 2014

FIREARMS
Handguns and **shotguns** favoured by criminals

OIC & MODERN SLAVERY
Over **10,000 victims** of trafficking in the UK

ORGANISED ACQUISITIVE CRIME
- Innovation from Europe **fuels new crime types**
- CVIT sees increased **levels of violence**

COMMERCIAL CSEA

CHILD SEXUAL EXPLOITATION & ABUSE
Around **675,000 children** will have suffered sexual exploitation and abuse before they reach adulthood

Serious and organised criminals

18. Those involved in serious and organised crime work in groups or as individuals and seek to exploit vulnerabilities through a range of activities including, for example, taking advantage of legislative loopholes, bribery and corruption and employment of professional enablers such as criminally complicit solicitors or letting agents.

19. As of December 2014, organised crime group mapping identified around 5,800 organised crime groups. Serious and organised criminals continue to operate mainly in loose networks working with others based on trust and reputation. Structured hierarchical groups are often based on familial ties. Both loose networks and structured groups frequently have international links or cross ethnic boundaries. Due to the transnational nature of the internet, a feature of cyber criminality impacting on the UK is that the groups or networks responsible are often entirely located outside the UK.

20. Serious and organised criminals frequently demonstrate their adaptability, altering their modus operandi or business model in response to law enforcement activity or to the availability of new opportunities or vulnerabilities.

21. Exploitation of technology, especially the internet, is increasingly prevalent. The ready availability of criminal products and services on the internet, especially on the hidden internet, has produced a marketplace where criminals can operate with a high degree of anonymity.

22. A large majority of OCGs are involved in two or more different types of criminality. They are often reliant on several cross-cutting enablers whether it is the anonymising services the internet provides to view indecent images of children or the corruption of a port worker to facilitate the passage of illegal migrants travelling on false documents across the border. Some OCGs will use one type of criminality to fund another. Serious and organised criminals will either do their own laundering or rely on the services of specialist money launderers to cash out the proceeds of their crimes.

Pathways into serious and organised crime

23. The pathways that lead offenders to become involved in serious and organised crime often differ from those that general offenders take into other crime. Home Office research into the careers of convicted organised criminals showed that a majority (57%) of organised crime offenders received their first sanction under the age of 18[3]. Organised crime group mapping indicates that three quarters of nominals are over the age of 26.

24. Financial gain is a key motivation drawing individuals into serious and organised crime, but there are many other factors. While some threat areas may have their own pathways (such as cyber crime and child sexual exploitation) others are likely to share common pathways. Involvement in street gangs, for example, can lead to involvement in drugs distribution, firearms offences and sexual exploitation. However, the most common factor drawing individuals into organised crime is familial or social connections to established organised criminals. In some cases, individuals will have been groomed, exploited or coerced into this pathway as a means of re-paying a debt or supporting friends and family.

Foreign nationals in serious and organised crime

25. The vast majority of mapped serious and organised criminals operating in or affecting the UK and its interests are British (our mapping of criminals based abroad is still evolving). Organised Crime Group Mapping (OCGM) indicates that, proportionally, foreign nationals are no more likely to be involved in serious organised crime than British nationals[4].

3 Home Office Research Report 74 (2013) *Understanding Criminal Careers in Organised Crime.*
4 About 13 per cent of known organised criminals in the UK are foreign nationals.

26. However, foreign national offenders (FNOs) are still of particular interest to law enforcement - they are in many cases transient and involved in more than one type of criminality, making them difficult to track, and in some cases have introduced new types of criminality to the UK. They use a variety of methods to enter the UK and to extend leave once here. Some use multiple identities supported by false documents and fraudulently obtained genuine documents (FOGs).

27. The response therefore requires greater inter-agency cooperation. Often, the end goal is deportation rather than a domestic prison sentence, but more preferable is the identification of criminality before foreign nationals enter the UK, enabling refusal of entry.

The key threats

Child sexual exploitation and abuse (CSEA)

28. CSEA remains a particularly significant threat, with every UK policing region reporting cases of contact child sexual abuse (CCSA) in 2014; the proliferation of indecent images of children (IIOC) and online child sexual exploitation (OCSE) continue to subject children to risk. We have also seen a continuation of offending overseas by British nationals.

The risk

29. Across offending methodologies, establishing an accurate understanding of the scale of the threat is made more difficult by significant under-reporting. However, the NSPCC estimates that 5% of UK children suffer CCSA during their childhood[5], indicating that around 675,000 will have suffered abuse before they reach adulthood[6].

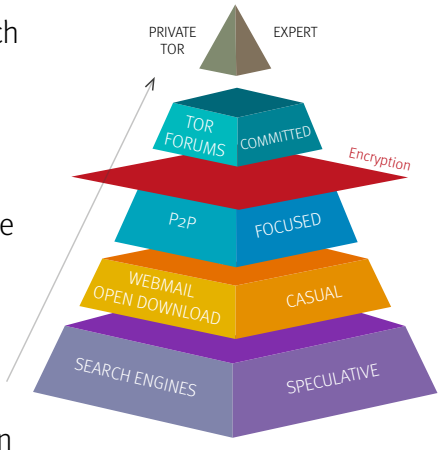
30. In the last year, Childline has seen a 168% increase in counselling sessions relating to online sexual abuse, and the NCA received 3,340 public reports of suspicious online activity, 46% of which involved some form of online child sexual abuse. In addition, NCA and policing have access to digital traces that offer the potential to identify up to 25,000 people with an interest in indecent images of children. These traces are partial or whole bits of data, rather than names and addresses and require significant resources to identify possible suspects, triage the risks they pose and develop available intelligence around them. Some traces will not be resolvable to identifiable individuals.

31. The impact of the threat extends beyond the immediate harm caused by offending. Investigating current and past cases of abuse places a considerable resource demand on law enforcement.

32. We judge that lone males known to their victims in some capacity represent the majority of CCSA offenders. Where abusers act outside the familial setting, initial contact is often made online via social networking platforms and there is a correlation in the geographical proximity of offenders to victims.

33. There appears to have been little change in the primary methods by which offenders accessed IIOC during 2014, and our understanding of these, as well as the apparent loosely defined offending pathway, remains strong. There is a continued dominance of image sharing through P2P[8] services and webmail, whilst TOR[7] services tend to facilitate networking between more sophisticated offenders, as well as access to a much smaller volume of newer imagery. We have witnessed a considerable decrease in the use of open search to access IIOC, which may be as a result of industry attempts to remove such material.

34. Known transnational child sex offenders (TCSOs) continue to be mainly males aged 40 and above. The last three years have seen a diversification in reporting of TCSOs around the world, potentially as a result of more robust procedures to combat CSEA in parts of South East Asia.



IIOC progression of offending complexity

Trends

35. Analysis of public reports to the NCA indicates that OCSE offenders rapidly migrate to new communications platforms adopted by children, and they use a range of methodologies from traditional grooming focused on romantic relationship or friendship building to more coercive techniques.

5 Radford, L. et al (2011) Child abuse and neglect in the UK today.
6 Based on an under-18 population of c.13.5 million; drawn from: Office of National Statistics (2013) *Population Estimates for UK, England and Wales, Scotland and Northern Ireland.*
7 The Onion Router or TOR is free software for enabling online anonymity and resisting censorship. It is designed to make it possible for users to surf the internet anonymously, so their activities and location cannot be discovered.
8 Peer-to-peer file sharing network (see glossary)

36. Where coercive techniques are used, an emerging trend has been identified towards more extreme, violent, sadistic or degrading demands by offenders. Whilst the reasons are unclear, we assess that for some OCSE offenders, demonstrating control over their victim is a greater driver than the pursuit of a sexual outcome.

37. We judge that, in the medium to long-term, we will see a reduction in the numbers of TCSOs due to a trend toward online offending as well as law enforcement activity and improving economic outlooks in vulnerable countries.

38. The live-streaming of abuse from the developing to the developed world is judged to be an emerging threat. We assess there are four principal factors: the presence of significant poverty in a country, widespread access to well-developed internet infrastructure, access to children and the presence of English-speakers. As access to 4G and broadband becomes increasingly widespread, we anticipate wider availability of live-streamed abuse across an ever-wider range of countries.

Firearms

The risk

39. Despite reductions in the criminal use of firearms and discharges, the risk from firearms remains serious. Overall, there were 30 fatalities in 2012/13 resulting from offences involving firearms, 12 fewer than the previous year and the lowest figure since the National Crime Recording Standard was introduced in 2002/03[9].

40. Handguns and shotguns remain the two types of firearms favoured by criminals. However, submachine guns (SMG) are also used by criminals, with an increased threat of Skorpion SMGs being imported into the UK destined for urban street gangs in south-east England. Stun devices and noxious sprays are prohibited items under Section 5 of the Firearms Act. However, significant detections and seizures continue to be made at UK borders.

41. Individuals who collect firearms and ammunition illegally pose a risk both in terms of their own intentions and the possibility of other criminals gaining access to their arsenals. These hoarders and significant firearms caches pose a risk of bulk theft of firearms, whether or not the owner is criminally complicit. This is particularly true where hoarders in some regions appear to be vulnerable individuals, which presents a risk of the collections finding their way into criminal hands.

42. Deactivated firearms continue to be reactivated for criminal use as a result of weaknesses in deactivation provisions and standards. Although UK legislation[10] has set deactivation standards these are not mandatory and this anomaly can therefore be manipulated to produce deactivations of a lower standard. There is a further risk from the current governance and oversight arrangements for proof houses. It is unclear to what extent fraudulent deactivations are occurring and whether the practicality of re-activating such firearms is enabling them to become a viable source of illicit firearms for crime groups.

Trends

43. Firearms continue to enter the criminal market through a variety of means, including direct importation through post/fast parcels and thefts from legitimate firearms holders or dealers. Criminals acquire firearms from a range of sources, including online sellers (for example, via the anonymous criminal marketplaces on the dark web[11]), at militaria fairs and through criminal contacts. Social media and TOR forums are often used as platforms for related discussions and this is of growing concern due to the challenges it poses to law enforcement monitoring.

44. The USA remains the source for over half of all firearms seized at the UK border. Smugglers are using ferry/sea ports, exploitation of the Common Travel Area (CTA) between the UK, Ireland, Isle of Man, Jersey and Guernsey, and unaccompanied luggage in coaches to import firearms and ammunition, but we have not yet identified clear trends.

45. Thefts of shotguns and ammunition from registered firearms dealers and licence holders remain low across the UK - 405 firearms were stolen from registered firearms dealers during 2013 - but in Scotland and Merseyside stolen shotguns are becoming a weapon of choice of some OCGs.

9 Office of National Statistics: Crime Statistics, Focus on Violent Crime and Sexual Offences, 2012/13.
10 UK Firearms (Amendment) Act 1998 S8.
11 The dark web is a subset of the hidden internet (see glossary). It hosts web sites, which although they are publicly accessible, hide their servers' IP addresses using anonymity software thereby making them more difficult to trace.

Organised immigration crime, human trafficking and modern slavery

46. Detections of irregular migrants attempting to enter the UK clandestinely more than doubled in 2014 with labour exploitation the most common trafficking type. This is likely to continue on an upward trend. Abuse of travel documents remains a high-priority enabler of organised immigration crime (OIC) activity with impersonation of genuine passports the most detected method of abuse during 2014.

The risk

Human trafficking and modern slavery

47. Modern slavery includes slavery, servitude, forced and compulsory labour and human trafficking. The Modern Slavery Strategy of November 2014 recognised that a large number of active OCGs as well as some opportunistic individuals are involved in its perpetration. The International Labour Organisation has estimated the total illegal profits from the use of forced labour worldwide at over 150 billion US dollars while human trafficking for sexual exploitation is estimated to cost the UK £890 million each year[12].

48. Human trafficking and wider aspects of modern slavery remain a high-priority threat to the UK. Referrals of potential victims of trafficking (PVoT) to the National Referral Mechanism[13] have increased year on year for the past three years, a trend which is likely to continue. The Home Office estimates that there may have been as many as 10,000 to 13,000 PVoTs in the UK in 2013[14].

49. Labour exploitation was the most common trafficking type in the UK during 2014, primarily in fruit and vegetable harvesting and cannabis cultivation. It is likely to remain an increasing risk in 2015. This was followed by sexual exploitation and exploitation of state benefits. Trafficking of children probably for adoption or sexual abuse in the UK may be more widespread than previously thought[15].

Facilitation of organised immigration crime

50. Serious and organised criminal involvement has enabled the number of migrants attempting to enter the EU and the UK to reach the highest levels since juxtaposed controls were introduced. The OCGs facilitating travel to the UK vary in their reach and capability, from loosely connected networks of sole traders specialising in one element of the journey to groups with members in strategic locations and extensive knowledge of border security.

51. Detections of irregular migrants trying to enter the UK clandestinely more than doubled in 2014. The biggest threat emanates from the North Africa into Italy route, use of which rose by over 300% in 2014. Greece also remains a key nexus point. The number of inadequately documented arrivals (IDAs) increased in 2014 with air routes accounting for over 70%.

12 Home Office Science Research Project 73 (2013) U*nderstanding organised crime: estimating the scale and social and economic costs.*

13 Adopted 01/04/2009, the NRM is a process to identify PVoT and provide them with protection and support as per the Council of Europe Convention on Action against Trafficking in Human Beings.

14 Home Office (2014) *Modern Slavery: An Application of Multiple Systems Estimation.* Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/381389/Modern_Slavery_an_application_of_MSE.PDF

15 Rotherham Metropolitan Borough Council, 'Independent Inquiry into Child Sexual Exploitation in Rotherham (1997-2013)'.

Use of documents to support organised immigration crime

52. The use of fraudulent documents remains a key enabler. A common method of abuse remains the use of genuine passports by an imposter who resembles the genuine holder.

Abuse of marriage and other legitimate means to remain in the UK

53. Marriage and civil partnership continue to be exploited. The Home Office estimated in 2013 that 4,000–10,000 applications[16] to remain in the UK are made annually on the basis of a sham marriage or civil partnership. It is believed that over half of these are facilitated by organised criminals. Criminality has also been exposed in English language test centres.

Trends

54. It is likely that labour exploitation will increase, whilst sexual exploitation continues as a key risk during 2015. Exploitation of EEA nationals for forced marriage is also an increasing trend, which may well extend through 2015. Across both sexual and labour exploitation, new recruitment methods (e.g. using social networking and dating sites) have opened up a cyber-enabled dimension, representing a shift away from traditional recruitment methods like newspapers and escort agencies.

55. Increasing detection of irregular migrants attempting to enter the UK clandestinely is set to continue, augmented by the sheer scale of migrants in the Nord Pas de Calais region in France.

56. North Africa to Italy is likely to remain the prominent route into the EU and the winter lull has been less pronounced this year due to increased instability and high numbers. The advance of ISIL in Iraq and Syria and growing antipathy towards refugees in the region are likely to increase the numbers of migrants from there looking to reach the EU.

57. Document abuse remains a major enabler with organised criminals heavily involved in production and supply.

58. The Immigration Act 2014 will require registrars to report all notices of marriage or civil partnerships where a non-EEA national could gain an immigration advantage. This could uncover much wider abuse than is currently estimated, but allow greater detection and prevention. It may also displace abuse to sham marriages elsewhere in the EEA and applications to remain in the UK on the basis of being in a relationship with a person already present and settled.

16 Home Office publication November 2013 - Sham Marraiges and Civil Partnerships Background Information and Proposed Referral and Investigation Scheme

Cyber crime

The risk

59. Use of internet technology in the UK continues to grow, with e-commerce and m-commerce increasing at a high rate. As of 2013, the estimated spend of the UK online was £91 billion, with 74% of the adult population buying goods and services online[17]. The G20 has stated that the UK is the most cyber-dependent economy in the G20 nations. This growth has led to a rise in the threat to the UK from cyber crime. The true scale and cost of cyber crime in the UK is unclear at present, and the criminal threat is able to change rapidly. Cyber crime is a transnational phenomenon and the threat to the UK comes from both UK and international criminals. The most damaging high-end cyber crime remains the preserve of the most skilled and technically competent criminals, but the maturing criminal marketplace is beginning to provide those with lesser skills with the tools to participate in this area of serious and organised crime.

60. Law enforcement information suggests that globally there are several hundred online criminal forums live at any one time. While not all members of online criminal forums are active, the typical scale of membership would suggest that, worldwide, active cyber criminals number in the thousands. Of these, the most significant threat to the UK is posed by a relatively small number of technically competent criminal groups and individuals with high-end skills. The numbers of such criminals/ criminal groups are likely to be in the low hundreds.

61. Competent cyber criminals can introduce new crimeware products to the marketplace rapidly and intelligence suggests that these criminals work on new products at the same time as deploying existing ones, increasing resilience to disruption efforts. This is the only crime type that operates this way. Law enforcement therefore has to tackle this threat using new techniques and practices.

62. Russian-language criminals in Russia and neighbouring states continue to be heavily represented amongst the more competent cyber criminals. Russian-language criminals are assessed to be behind the development of financial Trojans affecting tens of thousands of machines globally. Other nationals are often involved as service providers, and there is collaboration across ethnic and national groups.

63. Cyber criminals will seek to use low-cost and efficient technical service providers to host their activity and this makes cyber crime truly transnational. The criminal, the technical services used and the victim are frequently located in different countries. Advanced western economies including the UK typically host such providers, with the result that the UK is an attractive place for cyber criminals to host their services.

Trends

64. The cyber criminal marketplace has emerged as a key feature of both cyber-enabled and cyber-dependent crime. The services it provides consist of a combination of legitimate services, illegitimate services and a subset of services which can be used for legitimate or illegitimate purposes. While we do not yet often find traditional crime groups active in this marketplace, there is a threat that they will come to recognise the ready availability of these skills and services and begin to exploit them.

17 Office of National Statistics: Internet Access – Households and Individuals 2014.

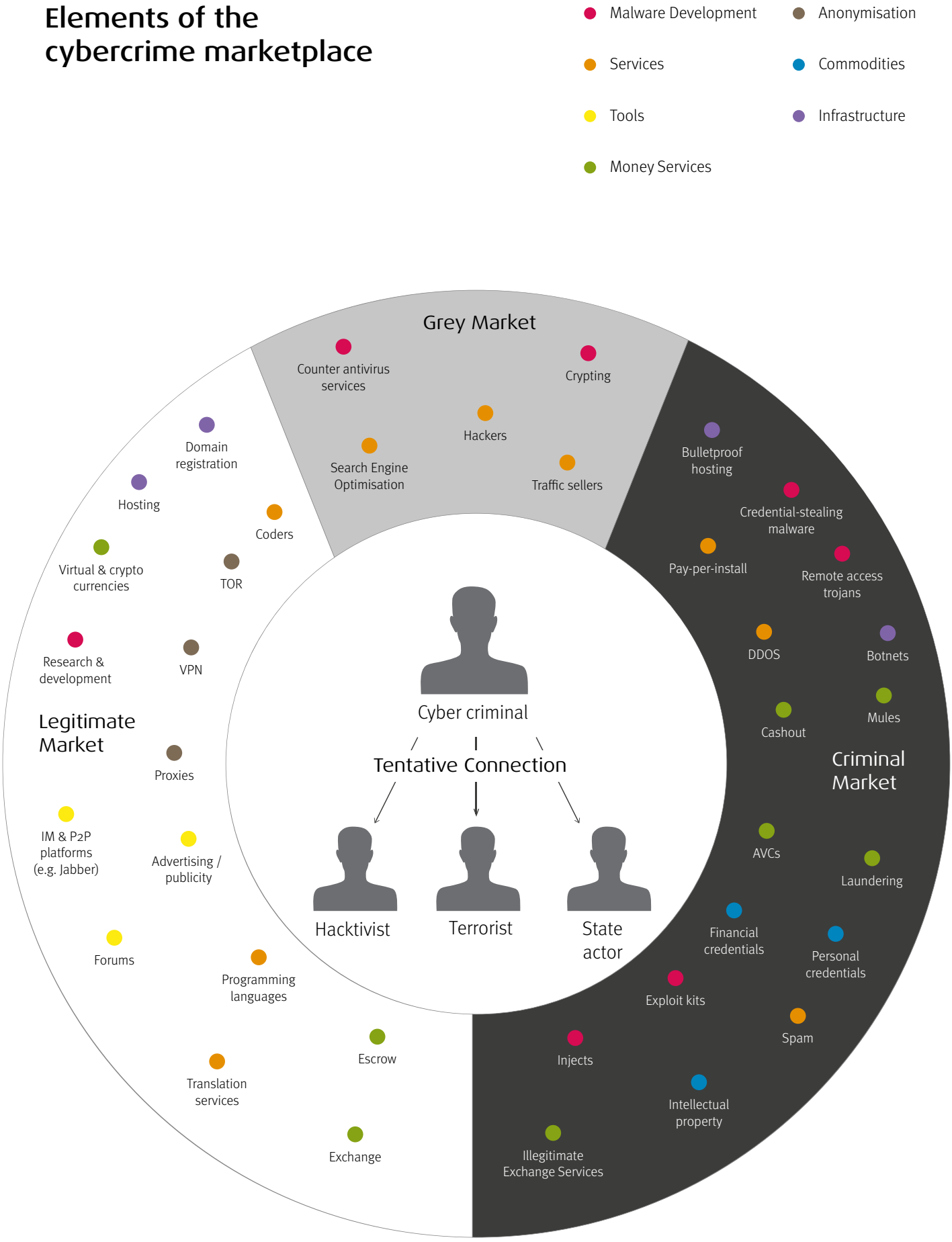
65. The following graphic on page 20 depicts the tools and services available and the area of the online marketplace where they sit.

66. Targeted intrusion attacks, like the November 2013 attack on the US supermarket chain TARGET and the August 2014 breach of JP Morgan Chase, which resulted in the theft of large amounts of data, are likely, we assess, to become increasingly significant in scale and damage. We assess that there is considerable under-reporting of such breaches within the UK.

67. Bespoke mobile malware already exists and is well-established outside the UK. International groups already deploying mobile malware elsewhere may start to target the UK, and groups currently targeting western markets by other means may adopt mobile malware deployment. The increasing use of apps designed for legitimate financial transactions will, over the next 12 -18 months, provide new opportunities for criminals.

68. There is a growing threat from multistep, blended attacks (i.e. a series of attacks by a mix of attack tools). Examples include the use of distributed denial of service (DDoS) attacks as a deliberate tactic to divert a victim organisation's system defences. Under the cover of the diversionary DDoS, a more damaging network intrusion or exfiltration attack is then launched.

Elements of the cybercrime marketplace



Money laundering

69. The UNODC[18] estimated that global proceeds of crime amounted to 3.6% of worldwide GDP in 2009 – equivalent to 2.7 trillion US dollars for the latest available GDP figures if the proportions remain unchanged[19]. The total amount of money laundered into and through the UK is unknown. However, it will include the proceeds of virtually all serious and organised crime in the UK as well as the proceeds of a significant amount of international serious and organised crime (including corrupt Politically Exposed Persons (PEPs) seeking to launder the proceeds of their corruption and hide stolen assets in the UK). We assess that hundreds of billions of US dollars of criminal money almost certainly continue to be laundered through UK banks, including their subsidiaries, each year.

70. The scale of the laundering of criminal proceeds, despite the UK's leading role in developing international standards to tackle it, is a strategic threat to the UK's economy and reputation. Some of the same financial transfer systems used by serious and organised criminals in the UK are also used by terrorist groups both domestically and overseas.

The risk

71. Criminals use various methods to launder money. These methods fall into two subsections; high-end and cash-based money laundering. High-end money laundering[20] is specialist, usually involves transactions of substantial value, and involves abuse of the financial sector and professional enablers. Cash-based money laundering can involve the physical movement of currency over national borders, as well as the use of companies with high cash throughput as a cover, with payments being broken down into smaller amounts to avoid detection.

High-end money laundering

72. The UK is an international financial centre, processing trillions of pounds of transactions every year. Together with the presence of a highly developed professional services industry, this increases the attractiveness and vulnerability of the UK's financial system to exploitation by those engaged in money laundering. The large number of users and volume of transactions across the entire financial sector provides many opportunities to disguise and conceal illicit funds. The banking sector continues to be the biggest producer of suspicious activity reports (SARs)[21].

73. High-end money laundering is particularly relevant to major frauds and serious corruption, where the proceeds of the crime are electronic and cash is only used further down the process to disguise audit trails or extract profits. Methodologies include the use of company structures, tax havens and investment in high-value luxury goods.

74. The laundering of criminal proceeds is reliant on access to the professional skills of, among others, lawyers, accountants, investment bankers and company formation agents. Professional enablers can also be highly organised criminals who develop products and services specifically to facilitate criminal enterprises. The use of professional enablers increases the complexity of money laundering activities, for example with the setting up of shell companies, trusts and other instruments providing anonymity. We believe the professions posing the greatest risk are within the financial and legal sectors, for example accountants and solicitors.

18 United Nations Office on Drugs and Crime.

19 Based on a nominal Gross World Product of 74.7 trillion US dollars in 2013, from IMF *'Report for Selected Country Groups and Subjects', World Economic Outlook*, October 2014.

20 For this assessment, we are defining "high end" money laundering as laundering which is conducted as a service by the UK financial sector and related professional services.

21 National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2014*, p.8.

75. Criminally complicit solicitors can effectively act as private banks to individual clients. Client accounts offer criminals relative anonymity, the ability to obscure the origins and beneficiaries of criminal proceeds, and the perceived protection of legal privilege. Some Accountancy Service Providers (ASPs) facilitate money laundering and sometimes act as active members of a criminal group or provide consultancy to one or more groups. This sector is one of the most fractured in terms of membership of professional bodies, making compliance with the Money Laundering Regulations of 2007 more difficult to enforce.

76. Purchasing property as a method of money laundering provides the criminal with the opportunity to clean large amounts of illicit funds in a single transaction. It is likely that a significant proportion of criminals purchase property through estate agents to launder the proceeds of crime; where a criminal group owns or controls an agency, criminal cash can be mixed with rental income and disguised as legitimate profits.

Cash-based money laundering

77. Many criminals use cash as an anonymous and untraceable financial instrument. Cash smugglers show a preference for high-denomination euro and US dollar notes. Smuggling of the euro is particularly prevalent due to its availability in low-bulk, high-denomination notes, and because it can be concealed within the European monetary system with ease.

78. Gambling proceeds can provide money launderers with a credible explanation for a source of wealth. Casinos can operate 24 hours per day, with high volumes of large transactions taking place in short timescales[22]. A number of cases show large sums of criminal proceeds being split into smaller amounts, exchanged into casino chips, gambled at up to a 10% loss and then cashed out.

79. International controllers are relied upon by many OCGs to arrange the collection and delivery of criminal street cash in return for a commission. Controllers orchestrate the movement of many millions of pounds across the world, and their loose networks give them the resilience to absorb losses from law enforcement intervention.

80. Trade-based money laundering: the destination of criminal proceeds is disguised by using the funds for separate payments through various trade sectors.

81. Money service businesses (MSBs) continue to be attractive to criminals. A minority of the sector is complicit in banking and remitting money but the entire sector is vulnerable to abuse. The NCA assesses that at least £1.5 billion of UK criminal proceeds go through MSB remittances each year, with the actual figure likely to be significantly higher.

Trends

82. The use of virtual currencies to launder funds is currently mainly the preserve of cyber criminals and has not yet been adopted by the wider criminal community. We assess that this is, in part, due to a lack of familiarity with virtual currencies, and the relative difficulty of exchanging them into hard currency without some degree of exposure to the regulated sector. However, if they embed themselves in the public consciousness and become more widely accepted as a payment method, law enforcement can expect to see a corresponding increase in their adoption by traditional (non-cyber) criminals, both as a vehicle to launder funds and as a means of payment for illicit goods and services.

22 Financial Action Task Force (FATF) Report: Vulnerabilities of Casinos and the Gaming Sector, 2009, pp26-7.

Drugs

The risk

83. Illegal drug use in England and Wales has fallen over the last decade, but the social and economic costs of drug supply remain significant - an estimated £10.7 billion annually[23] and, in 2013, 1,957 drug-related deaths[24], up from 1,636 in 2012. The number of cannabis farms and new psychoactive substances (NPS) detected in the UK has grown. The amount of cocaine reaching UK streets remains high, while the supply of heroin from Afghanistan is likely to increase over the next few years.

84. Organised crime group mapping indicates that around 2,300 OCGs are involved in drug trafficking, often multi-commodity. A significant proportion of these are also involved in violent criminal activity and specialist money laundering. London and the north-west region of England are significant distribution hubs for the UK. Some OCGs are comprised of UK based foreign nationals.

85. The high-priority threats of cocaine and heroin, including source countries, transport routes and distribution hubs, are well understood, with regular disruptions against UK and overseas OCGs. The intelligence picture on synthetic drugs, NPS and cannabis is less developed, including UK OCG involvement.

86. Meanwhile, the distribution and marketing of controlled substances continue to develop via the dark web/hidden internet, with anonymous access enabled through TOR.

87. The market for illegal drugs in the UK remains vibrant. Cocaine and NPS are prevalent across the UK and there is a stable heroin market. The UK is a primary market in the EU for amphetamines and we are seeing increasing levels of processing. Cannabis represents the majority (76%) of police and Border Force drug seizures in England and Wales[25].

88. 'County Lines' is a national issue that generates substantial illicit revenue. Typically, urban criminal groups establish telephone numbers in rural areas outside of their normal locality, to sell Class A drugs at street level. These operations are dependent on phone lines which represent a brand and are used for years without being changed. Intelligence indicates that 'county lines' enterprises almost always exploit vulnerable persons. Criminal groups use violence and exploit drug addictions in order to establish bases in vulnerable people's homes, and force their assistance. Young people are also commonly exploited, being recruited to work as runners. Children are perceived as inexpensive, easily controlled and less likely to be detected by law enforcement.

Trends

89. We assess that in 2015 there will continue to be stable supplies of cocaine and amphetamines with increasing demand for the former. It is likely that there will be an increase in availability of heroin with a record Afghan opium harvest and the withdrawal of western military forces from the country.

90. Cocaine - Colombia, Peru and Bolivia remain the main sources of cocaine for European and UK markets. Shipments continue via key transit regions as well as direct. Cape Verde has been identified as an important transit and storage location off West Africa, whilst cocaine is now trafficked via Morocco, using established cannabis trafficking routes.

91. Heroin – Pakistan, Iran, Turkey and the Balkans remain primary upstream transit routes for heroin from Afghanistan. East Africa has emerged as a key transit route towards Europe and Greece as another significant transit country within Europe. UK heroin purities continue on an upward trend across the supply chain.

23 Home Office (2013) Understanding Organised Crime: Estimating the Scale and the Social and Economic Costs.
24 Office for National Statistics (2014) Deaths Related to Drug Poisoning in England and Wales, 2013.
25 Home Office Statistical Bulletin - Seizures of drugs in England and Wales, 2013/14.

92. Synthetic drugs, including NPS - Whilst the UK remains a prime market for Dutch and Belgian-produced synthetic drugs, there are strong indications of significant amphetamine processing in the UK, particularly in north-west England. Associated risks include fire, explosion, intoxication and waste dumping. China remains the principal source of NPS, although intelligence gaps exist on evolving supply methods and routes, including via European hubs.

93. Cannabis - Cannabis (plants, herbal and resin) represents three quarters of drug seizures in England and Wales[26]. Whilst substantial importations continue, domestic cultivation is frequently identified, often involving illegal immigrant workers.

26 Home Office Statistical Bulletin - Seizures of drugs in England and Wales, 2013/14.

Economic crime

94. Economic crime covers a wide range of activity, including fraud against the individual, public, private and charitable sectors, intellectual property crime and market abuse/insider dealing. The UK's welfare and tax regimes continue to be vulnerable to highly capable and well-funded OCGs, and forged identity documents continue to be a significant risk to the banking industry.

The risk

Public sector fraud

95. Serious and organised criminals defraud central and local government of billions of pounds each year against the tax and welfare systems.

96. HMRC estimates that £5.4 billion of UK tax revenues are lost per annum to organised crime. OCGs attack the UK tax system through evasion of duties on alcohol, tobacco and oils, Missing Trader Intra-Community (MTIC) VAT and tax/benefit repayment fraud. This risks a loss of confidence in the Government's ability to manage public finances.

97. The key threats to the Exchequer from fiscal fraud continue to comprise excise fraud (chiefly the smuggling of cheap white cigarettes[27] and the inward diversion of alcohol fraud) and MTIC or carousel fraud against the VAT system. These threats are promulgated by highly capable and well-funded OCGs. Fuel laundering (particularly in Northern Ireland) and attacks against the payment and repayment regime, including the tax credits system, are also significant threats.

98. The Department for Work and Pensions (DWP) estimated the total monetary value of fraud in the benefit system in 2013/14 as £1.2 billion[28], 0.7% of total benefit expenditure of £164 billion . Whether this is due to opportunist fraud or that carried out by organised criminals is hard to measure and not fully assessed. In 2012/13 it was estimated that £1.1 billion - 3.9% of the total tax credit budget - was lost to fraud[29]. Fraud in local government is considered to be under-reported.

99. These crimes are facilitated by cross-cutting enablers common to other crimes. Identity crime and cyber crime are key enablers for payment and repayment fraud used by organised criminals to facilitate attacks across the public sector.

Fraud against the private sector, individuals and the charity sector

100. Individuals, the private sector and, to a lesser extent, the charity sector are estimated to lose many billions of pounds to fraud each year. The total loss reported to Action Fraud for the period 1 September 2013 to 31 August 2014 (excluding cyber crime) was £1.73 billion.

101. Figures for cyber-enabled fraud show a year-on-year increase, although it is difficult to judge how much of this is due to better reporting across all sectors. Cyber-enabled banking and card fraud against the UK are widespread due to the high volume of online banking and retail transactions, high card limits, similar security methods by the UK's few large banks and ease of opening accounts.

102. The large volumes of personal and financial data sold online through criminal forums, often accompanied with instructions on how to use the data to commit fraud, are an increasing concern. The cyber criminals who specialise in different aspects of online fraud meet in online forums and work peer-to-peer in relationships of trust but with no hierarchy.

27 Illicit white cigarettes are non-UK brands legally made in other countries but transported to the UK without paying tax and duties
28 https://www.gov.uk/government/statistics/fraud-and-error-in-the-benefit-system-2013-to-2014-estimates
29 https://www.gov.uk/government/statistics/fraud-and-error-in-the-benefit-system-2013-to-2014-estimates

103. Reported fraud losses on UK cards and remote banking have increased in 2014, according to Financial Fraud Action UK. Between January and June 2014 reported losses totalled £247.6 million for fraud losses on UK cards, up from £216.1 million during the same period in 2013. Research conducted by the National Fraud Authority amongst a representative sample of 500 (non-financial services) businesses across the UK in 2013 suggested 1 in 4 businesses were a victim of fraud, losing an estimated £15.9 billion (1.6% of total UK turnover). Abuse of identity documents continues to be a key enabler used by criminals and therefore a significant threat to the banking industry.

104. Victims are continuing to lose large sums of money from investment fraud (e.g. boiler room fraud or ponzi schemes). The call centres from which these frauds are perpetrated are typically but not exclusively based in locations such as Spain, Thailand, Indonesia and Philippines. These frauds can have a significant financial, social and emotional effect on victims.

105. Insider fraud[30] is increasingly seen as a high risk area for the private sector domestically and globally. The targeting by OCGs of an organisation's staff members to coerce them into providing sensitive information and/or to facilitate criminal activity is of concern.

Intellectual property crime

106. Intellectual property crime is estimated to cost the economy at least £1.3 billion per year in lost profits and taxes[31] but it is difficult to give a precise figure on the scale. The majority of counterfeit goods still originate from China and the increasing use of the internet, particularly social media sites, has created a wide-reaching marketplace to facilitate the sale of counterfeit goods. The public's perception of obtaining a bargain may blind them (if they are even aware) to the dangers of the counterfeit goods, such as medicines.

Insider dealing/market abuse

107. The number of notifications of suspected market abuse has increased over recent years, although this could be due to the improved supervision, awareness raising programmes and increased use of enforcement penalties for failing to report suspicious transactions. The total cost to UK markets from OCGs committing market abuse and insider dealing may be hundreds of millions of pounds per annum, although no definitive study has been undertaken to determine exactly how much market abuse costs the UK economy or how systemic it is within UK markets.

Trends

108. As government payment services increasingly come online, they are certain to attract extensive criminal interest. Additionally, the move towards an increasingly cashless society will cause a continuing rise in opportunities for cyber-enabled fraud and money laundering. The next two years are likely to see a greater range of electronic payment methods become integrated into personal items and commerce.

30 An insider threat is a member of trusted personnel (e.g., employee or contractor) that uses their privileged access for some unauthorised purpose such as revenge or financial gain, and to the detriment of their enterprise

31 Intellectual Property Crime Report 2013/14

Organised acquisitive crime

109. In terms of serious and organised crime, organised acquisitive crime (OAC) consists of commodity crime, organised vehicle crime, commercial robbery, organised metal theft and wildlife crime. Some of these crime types have seen an increase in the levels of violence involved. Cyber- and technologically-enabled acquisitive crime remains an issue, as illustrated by criminals using specialised equipment to identify vehicles that can be stolen.

The risk

110. Many OCGs involved in OAC operate across a broad range of criminal activities. Groups may engage in multiple types of acquisitive crime, or may be concerned with the importation of narcotics or the commission of economic offences. The transient and potentially violent nature of some groups engaged in organised acquisitive crime requires a cross-agency approach.

111. Organised crime group mapping indicates that vehicle crime is the most prevalent crime type amongst OCGs engaged in OAC. This offers the greatest potential synergies with other crime types and, we assess, often serves as a facilitator for other criminal acts.

Trends

112. The use of violence by OCGs involved in OAC has increased during 2014, notably across cash and valuables in transit (CViT), commercial robbery and gold theft. In particular, we assess the growth of violence in CViT to be linked to more opportunistic attacks by gangs, especially in the London area.

113. Technology and cyber-enabled crime present a continued and developing threat. Malware has been utilised in ATM attacks; an emerging trend not previously identified. Organised vehicle crime has also benefitted from the deployment of technology, with technical solutions being used to steal vehicles.

114. An emerging threat exists around fuel theft from pipelines. Initially identified as a threat in April 2014, instances of this offending methodology continue to be identified.

115. There has been a marked change in the focus of organised metal theft. Whilst some regions report a reduction overall, London and the South West have noted that criminals increasingly target catalytic converters. The effect of the Ebola epidemic on mining in the African continent continues to drive the market for precious metals, indicating that this trend in criminality will continue.

116. International illegal wildlife trading continues to be a threat, with OCGs or individuals increasingly flexible in their ability to generate new income.

Cross-cutting threats

Corruption

117. In a serious and organised crime context corruption is defined as 'the ability of an individual or group to pervert a process or function of an organisation to achieve a criminal goal'. It is a critical enabler, without which serious and organised crime would not be able to operate to its present extent and scale. The impact of corruption is disproportionate to the level and frequency at which it occurs, and often has serious ramifications across the public and private sectors.

118. The precise extent to which corruption affects the UK is hard to assess and remains an intelligence gap. As a result it can be difficult to measure the true impact of law enforcement actions in this area.

119. The UK Anti-Corruption Plan reflects the importance the Government places on tackling the threat to the UK from corruption, both domestically and internationally. It presents an action plan for tackling corruption in all its guises for the first time, with NCA leading the law enforcement response.

The risk

Corruption in the public and private sectors

120. In the public sector, criminal groups use corruption to access sensitive information and corrupt elected officials and procurement systems for financial gain. They also target local government to manipulate processes such as housing or planning, and have been known to target local officials in order to consolidate their status in communities. Corrupt private sector professionals provide organised criminals with access to the legitimate economy, enabling them to launder proceeds of crime and establish front businesses.

Corruption in law enforcement and the criminal justice system

121. Anyone who works in the law enforcement and criminal justice environment is likely to be an attractive target to OCGs seeking to use corruption. Corruption in this sector does not occur on a large scale, but individual instances can have a disproportionate effect, as one corrupt individual can cause considerable damage, for example, by perverting the course of justice to alter the outcome of a trial. It is not just those with coercive powers who may be targeted, but anyone within the sector who may be able to access information. Disclosure of information is the primary concern and most reported consequence of corruption in law enforcement.

122. Criminals at all levels seek information about themselves, competitors, investigations, tactics, prosecutions, witnesses and intelligence sources, including the identity of police officers and informants. This information is used to undermine law enforcement operations, evade arrest and facilitate serious criminal activity. Generally, serious and organised criminals will seek to exploit personal connections to corrupt those in law enforcement.

123. Misuse of systems and the abuse of authority to identify and exploit vulnerable persons for sexual gratification is a major concern. In some police forces it is the most common form of corrupt behaviour, and frequency of reporting in this area has been increasing nationally. Sexual misconduct cases are high-risk to communities and to law enforcement, and require considerable resources and specialist skill to investigate.

Politically exposed persons (PEPs) and sanctions

124. The actions of corrupt foreign PEPs who abuse their positions of entrusted power for private gain have a detrimental effect on their own domestic economies and citizens. Those who seek to launder the proceeds of corruption through the UK economy pose a significant reputational risk to the UK's financial institutions and professional services industry. Their impact is disproportionate to their numbers as one PEP can be responsible for the theft and laundering of billions of pounds. PEPs are known to favour the UK as an attractive place to invest, meaning significant sums run through the UK economy[32].

125. Current government efforts to actively encourage foreign investment in the UK need to be coordinated more closely with law enforcement to ensure that investments are being made with legitimate funds. This can prevent costly court cases and law enforcement/recovery operations at a later date.

126. Cross-governmental cooperation is also needed with regard to seizing assets from sanctioned individuals. As HM Treasury does not prosecute criminally, a process has been developed by which referrals to the NCA are now made.

127. A more integrated and coherent approach is needed between law enforcement and other government agencies to tackle corrupt PEPs and the issues around international corruption.

32 PEPs use professional enablers to move their money – see Money Laundering chapter for more.

Criminal use of internet technology

The risk

128. The internet is used by criminals to communicate, organise, conspire, incite, trade and otherwise facilitate criminal offences, and many traditional offences (such as fraud) are now largely committed online. Using the internet offers criminals the advantage of no physical risk, greater anonymity and a wider range of targets. This presents law enforcement with increasing challenges, which require new investigative and evidential skills and capabilities.

129. The internet continues to host the advertising and selling of weapons, parts and ammunition, drugs, compromised credit cards and other criminal commodities as well as providing a communications platform to discuss their import and export.

130. Both the surface and hidden internet are used to supply and source firearms. The hidden internet offers platforms/tools such as The Onion Router (TOR) and other anonymisation programs, such as The Invisible Internet Project (I2P) and the Free Network (Freenet), to enable users to maintain anonymity. A search engine called Grams has been launched on TOR which is specifically designed to search for illicit commodities across a range of online marketplaces and there are other search engines being developed for this purpose. It also allows users to find sites that have been taken down and moved to a different address.

Trends

131. Traffickers involved in labour and sexual exploitation are increasingly using social networking to recruit potential victims in addition to traditional methods, such as websites and newspapers.

132. Virtual currency systems provide a cheap, quick, unregulated and almost anonymous method of transferring value between individuals or groups anywhere in the world. They have rapidly become the payment system of choice for a large number of individuals and organisations engaged in cyber-dependent and some areas of cyber-enabled crime, though as yet there has been limited take-up of virtual currencies as a medium for moving large quantities of money across the broader criminal community.

133. The increasing use of encrypted communication devices and apps poses a growing challenge to UK law enforcement. Although the devices and apps are legitimate, their adoption by criminal groups can enable attempts to evade law enforcement detection.

134. The ongoing rollout of IPv6, the next generation of IP addresses, will offer added complexity and an exponential increase in the number of unique addresses[33]. The sheer volume of possible addresses alone will present a threat to law enforcement's ability to trace offenders' online activity. Take up of IPv6 has so far been slow but increased demand for device connectivity, especially with the rise of the Internet of Things, is beginning to force the pace.

33 IPv6 is based on a hexadecimal system and will increase the number of unique addresses from the 4.3 billion that the IPv4 currently offers to a total of 340,282,366,920,938,463,463,374,607,431,768,211,456.

Prisons and lifetime management

135. Serious and organised criminality perpetrated from within the prison estate continued to be a threat in 2014, though more intelligence is required to properly quantify the specific risk. Whilst imprisoned, offenders have coordinated conspiracies to import Class A drugs, expanded their networks and markets, hidden their criminal assets and threatened enemies or those perceived to have betrayed them. It is highly likely that developments in technology and potentially greater access to smart phones will present a threat to law enforcement disruption efforts.

The risk

136. There are 119 prisons in England and Wales of which 14 are run by the private sector. There are approximately 85,500 prisoners in custody[34]. Prisoners are assessed against the risk they pose in terms of the likelihood of escape, the risk of harm to the public in the event of an escape and any control issues that impact on the security and good order of the prison and the safety of those within it.

137. As of September 2014, there were over 7,000 serious and organised criminals in prison, and about 40% of known organised crime groups had at least one member in prison.

138. Those criminals who pose the highest risk – demonstrating the intent to continue their criminality whilst imprisoned – are likely to be significant or principal members of OCGs.

139. There is a risk that extremists could seek to exploit criminal contacts in prison to gain access to criminal assets or capabilities. The extent of associations and the nature of relationships between extremists and serious and organised crime prisoners are, however, complicated and to date there has been little evidence that such exploitation has occurred.

Trends

140. The available intelligence suggests that serious and organised crime prisoners often adopt the role of coordinators or planners from within prison, and their activities whilst in custody mirror their actions before arrest. Whilst on remand or newly sentenced, serious and organised crime offenders engage in activity designed to secure criminal proceeds, mitigate problems caused by debts or threaten enemies – acts which also serve to maintain their reputation whilst in prison. We believe they may then seek to give the impression of settling as they work to present themselves as model prisoners in an attempt to secure a place in a lower-category prison before again escalating their criminal actions in anticipation of imminent release; but more intelligence is required.

141. Continued criminality from within the prison estate is hampered by disruptions to communication. However, external contact can be facilitated by mobile phones that are smuggled into the prison environment by friends, family, criminal associates, or corrupted staff, both directly and indirectly employed across the prison estate. Criminals also exploit the legitimate use of the prison PIN phone system to enable their criminal business.

142. Smart phones have the potential to provide greater communications opportunities for prisoners and we assess that this, combined with technological developments, means they may become more desirable to prisoners. This could give prisoners access to potentially more secure and diverse communications platforms, hampering law enforcement disruption efforts. The techniques used to smuggle mobile phones and other contraband into prisons vary in sophistication, ranging from simple personal concealment, to the use of commercially available drones.

34 The Ministry of Justice prison population bulletin 27 February 2015

143. Smuggling may also involve the direct corruption of a wide range of people involved across the entire prison estate. Principal OCG nominals are often experienced influencers and manipulators, and the unique prison environment provides an incentive to attempt corruptive activity.

144. When engaging with other offenders serious and organised crime prisoners are able to develop or augment their networks. Whilst new contacts do not always translate immediately into active conspiracies to commit serious and organised crime, they may represent opportunities to draw upon a range of skill-sets, contacts, suppliers, or markets not previously available. Similarly, offenders maintain existing criminal associations with prisoners from OCGs in the same prisons, wings and cells.

Border vulnerabilities

145. Most forms of serious and organised criminality require, to some degree, circumvention of the UK border security controls. Over the past year, criminals have continued to demonstrate that they can exploit vulnerabilities in border security, that they are capable of adapting to changes in law enforcement activity at the border and that they are innovative in developing new methods of concealment for illicit commodities and people, and of their recovery after arrival in the UK.

The risk

146. The high volume of traffic entering and exiting UK ports presents opportunities for organised criminals to disguise or conceal the movement of illegal commodities and migrants. The highest levels of detections therefore typically occur at those ports with the highest volumes of legitimate traffic.

147. Typically, criminals will transport commodities from source countries to hubs in continental Europe before using Ro-Ro freight services to move them to the UK. Bulk consignments of heroin are often transported to the near continent via the Balkans before shipment to Dover. Cocaine from South America and the Caribbean is often transported by container and commercial vessel to European hubs, particularly at Antwerp and Rotterdam, before transportation to eastern and south-eastern UK ferry ports.

148. Criminals are agile in adapting their behaviour in response to law enforcement activity at the UK border. Successful law enforcement interdictions at certain ports can subsequently lead to displacement, where criminals seek new entry points to bring in illicit commodities and people.

149. Criminal use of air passenger and freight services continues to present a significant threat to the UK border. Air passenger services provide the most common means of entry for potential victims of trafficking, predominantly London airports. Furthermore, commercial flights, used in conjunction with false travel documents, can facilitate the entry of criminals to the UK undetected.

150. Containers are used widely by organised criminals to import drugs, cigarettes, tobacco, alcohol and counterfeit goods. In September 2014 the multi-agency Project TOYER highlighted the use of containers to export high-value vehicles stolen in the UK and Europe to overseas markets via UK container ports, with 44 vehicles and parts with an estimated value of £1.2 million recovered. The use of containers for exporting illicit goods out of the UK is highly likely to remain a threat in 2015.

151. In some cases, the smuggling of illicit commodities into and out of the UK is facilitated by corrupt drivers and port workers.

Trends

152. Multi-kilo shipments of cocaine from South America and the Caribbean transported using general maritime vessels usually land in mainland Europe rather than direct in the UK. In the last year, however, seizures of cocaine from yachts bound for the UK suggest direct importation as a potential emerging trend. There is also some suggestion that the use of general maritime as a mode for facilitating OIC may be increasing.

153. We assess that a high-profile attempt at Tilbury where irregular migrants were detected inside a sealed shipping container in August 2014 does not represent an emerging trend in the use of containers to facilitate clandestine entry. It may, however, indicate that irregular migrants are now prepared, on occasion, to take greater risks.

154. Fast parcel and post remain key modes by which drugs and firearms are transported to the UK. In the last year, there has been a significant increase in detections of NPS from China, a trend which is expected to continue. The USA remains a major source country for firearms.

Criminal use of identity

155. Identity crime, encompassing identity theft and document abuse, facilitates serious and organised crime and allows criminals to evade law enforcement detection.

The risk

156. Identity crime will commonly take the form of identity theft, the creation of counterfeit documents, or the misuse of genuine documents. Once a criminal has illicitly created or stolen an identity, they can use this typically to commit fraud and attempt to cross the border undetected.

Identity theft and fraud

157. Identity theft occurs when criminals access enough personal information about an individual to commit fraud. They use various techniques to steal these details, from outright theft and social engineering to harvesting data through cybercrime. With this information, criminals can impersonate the victim in order to access bank accounts, fraudulently claim benefits or obtain genuine documents in the victim's name.

Document abuse at the border

158. The fraudulent acquisition, production, distribution and use of false travel documents are key enablers for criminal activity at the UK border. The biggest threats are the acquisition and use of fraudulently obtained genuine (FOG) UK passports by criminals and the production, distribution and use of counterfeit and forged EU identification to conceal identity and facilitate irregular migration to the UK.

159. Impersonation based on the use of genuine passports is the most common method of abuse detected at the UK border, largely due to the improved security features of many new travel documents.

160. The threat from lost and stolen passports used in OIC remains significant; however, a full assessment cannot be made as migrants often arrive at UK ports without any form of travel document. It is judged that the majority of inadequately documented arrivals (IDAs) have used some form of lost or stolen passport en route to the UK but then destroyed it or handed it over to a third person before arrival.

Trends

161. Increasing use of the hidden internet, accessed through anonymising programs, is expected, allowing criminals to hide their real identity online and in the real world. This will give criminals increased confidence in their criminal activities online as it is much harder for law enforcement to establish their identities.

162. With the introduction of major government online payment systems there is likely to be substantial interest from criminals with a shift toward more cyber–enabled fraud and more criminal use of identity.

List of Figures and Glossary

List of figures

Glossary

Boiler room fraud	This involves bogus stockbrokers, usually based overseas, cold calling people to pressure them into buying shares that promise high returns. In reality, the shares are either worthless or non-existent.
Carousel fraud	Carousel fraud involves moving goods between EU Member States, attempting to obtain a VAT repayment each time the goods are exported.
CCSA	Contact child sexual abuse: any sexual contact with a child in person. The opposite of non-contact CSEA, which includes grooming, non-contact exploitation and persuading children to perform sexual acts via the internet.
CTA	Common Travel Area denotes the minimal or non-existent border controls between the Republic of Ireland, the UK, the Isle of Man, Jersey and Guernsey.
CSEA	Child sexual exploitation and abuse (cf. CCSA, IIOC, OCSE and TCSO).
CViT robbery	Robbery of cash and valuables in transit.
Cyber-dependent	Cyber-dependent crimes are crimes such as the creation, dissemination and use of malware for financial gain, hacking to steal personal or industry data and denial of service attacks to cause reputational damage. They require the use of computers, computer networks or other forms of information communications technology (ICT).
Cyber-enabled	Crimes such as fraud, child sexual exploitation and the purchasing of illegal drugs can be conducted online or offline. Where they are conducted online they are described as cyber-enabled.
Dark web	A subset of the hidden internet comprising sites that are publically accessible but which hide their servers' IP addresses using anonymity software, such as TOR. Like the hidden internet this material is not necessarily criminal (e.g. anonymous news submissions) but criminals do take advantage of the difficulty in identifying sites' origins and the dark web is used to host illegal online marketplaces.
DDOS	Distributed denial of service attack: multiple compromised systems - usually infected with a Trojan - are used to target one system causing a denial of service attack. This generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the internet, typically on high-profile web servers, such as banks or credit card payment gateways.
E-commerce	Online business services, including online marketplaces and shopping cart software, secure online business transactions, electronic data interchange and online banking. Includes m-commerce.
EEA	European Economic Area.
FOG documents	Fraudulently-obtained genuine documents.
Freenet	The Free Network, an internet anonymisation program.
Hidden internet	The hidden internet (or deep web) is the portion of the worldwide web that is not indexed by standard search engines and constitutes approximately 96% of the entire web. In most cases, this is not for sinister reasons and is simply due to the sheer size of the internet. The dark web is a subset of the hidden internet.
HMRC	Her Majesty's Revenue and Customs.
I2P	The Invisible Internet Project, an anonymisation program.
IDA	Inadequately documented arrival. Any person who arrives in the UK, who requires leave to enter and who fails to produce the required documents. It includes passengers who arrive with no documents, those who arrive with unacceptable documents and those who arrive with 'spurious documents', i.e. which have been issued by a state or international organisation that does not exist or is not generally recognised.
IIOC	Indecent images of children: includes the possession, taking, making, distribution and sharing of indecent photographs of minors. These can include moving images and pseudo-photographs (e.g. computer generated images that look like photos).

Internet of Things	'The Internet of Things' describes the interconnection of uniquely identifiable embedded computing devices with the existing internet infrastructure. Connection to the internet is being designed into more and more devices in the home and those affecting our daily lives. Examples include microchips for animals, heart-monitoring implants and built-in sensors for cars.
IPC	Intellectual property crime.
IPv6	Internet Protocol is the system by which devices connected to the internet are allocated a unique address. IPv6 is beginning to replace IPv4, which, with a possible 4.3 billion permutations, effectively ran out of unique addresses in 2011. IPv6 will provide an exponential increase in the number of unique addresses which will meet the demand even from the proliferation of devices inherent to the so-called 'Internet of Things'.
ISIL	Islamic State of Iraq and the Levant.
Jabber	An encrypted internet communication chat service.
Juxtaposed controls	This describes an arrangement between Belgium, France and the UK whereby immigration checks on certain cross-Channel routes take place before boarding the train or ferry. It does not affect customs checks other than on the Eurotunnel route, for which all checks, both British and French, take place in Coquelles.
M-commerce	A subset of e-commerce which includes such services as mobile banking and brokerage, mobile ticketing and vouchers and mobile money transfer, and puts these services directly into the customer's hand.
MSB	Money service businesses: have specific meanings in different jurisdictions. These generally include any business that transmits money or its representatives, provides foreign currency exchange, or cashes cheques or other money-related instruments. It is usually used in the context of anti-money laundering legislation and rules.
MTIC	Missing Trader Intra-Community VAT fraud (see also Carousel fraud). MTIC fraud is the theft of VAT from a government by criminals who exploit the way VAT is treated within multi-jurisdictional trading, where the movement of goods between jurisdictions is VAT-free. The fraudster charges VAT on the sale of goods and then absconds instead of paying it to the government.
NPS	New psychoactive substances. Commonly known as legal highs, these are drugs designed to mimic the effects of illegal drugs, but are sufficiently structurally different to avoid being classified as illegal substances. This does, however, not necessarily make them safe to use.
OAC	Organised acquisitive crime: consists of commodity crime, organised vehicle crime, commercial robbery, organised metal theft and wildlife crime.
OCGM	Organised crime group mapping.
OCSE	Online child sexual exploitation: use of the internet to offer a child or an exploitative third party 'something' (e.g. money or a service) in exchange for the performance of sexual acts, either by or on the child.
P2P	Peer-to-peer file sharing network: a computer network where files are shared directly between computer systems without needing a central server. A P2P network allows every computer to exchange data and services directly with every other computer in the network. The only requirements needed to join a P2P network are an internet connection and P2P software.
PEP	Politically exposed person. There is no fixed definition, but in financial regulation a PEP describes someone who has been entrusted with a prominent public function, or an individual who is closely related to such a person. A PEP generally presents a higher risk of involvement in bribery and corruption due to their position and influence.
Ponzi fraud	Ponzi schemes are investment scams which pay returns to investors from their own money, or from money paid in by subsequent investors. There is no actual investment scheme as the fraudsters siphon off the money for themselves.

Ro-Ro	'Roll-on, roll-off' ports tend to service freight vehicles and some passengers and subject them to very limited controls.
SAR	Suspicious activity report.
TBML	Trade-based money laundering: an alternative remittance system that allows illegal organisations to earn, move and store proceeds disguised as legitimate trade. Value can be moved through this process by false invoicing, over-invoicing and under-invoicing commodities that are imported or exported around the world.
TCSO	Transnational child sex offender: a UK national committing sexual offences against children overseas.
TOR	The Onion Router is free software for enabling online anonymity and resisting censorship. It is designed to make it possible for users to surf the internet anonymously, so their activities and location cannot be discovered by government agencies, corporations, or anyone else.
Virtual currency	Virtual currencies were defined in 2012 by the European Central Bank as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community".