# Providing a picture of the threat to the UK from serious and organised crime

**This is a PDF version of the NSA 2025 website.**
**Click here to view website**

The National Strategic Assessment is split into three main sections:
**Overview of SOC** | Summarises the key issues across the SOC threats, including cross-cutting enablers.
**Threats** | Provides more detail on each SOC threat. See menu for links to threat pages.
**Tackling the Threat** | Shows how the NCA and partners responded to the SOC threat in 2024.


## Welcome from the NCA's Director General

Serious and organised crime (SOC) continues to cause more harm to more people than any other national security threat. It is responsible for danger in our homes and on our streets, stunting our economy, and damaging our communities.

The purpose of this assessment is to understand these threats, so that we can better address them. The National Strategic Assessment of Serious and Organised Crime 2025 builds on last year's comprehensive baseline and draws out the trends and themes of the last 12 months.

We have developed it through extensive consultation with partners across government, policing, the UK intelligence community, and the private sector, and I thank them for their contributions.

**Like those we seek to disrupt, we need to become more agile to respond to the evolving threat.**

Overall, the SOC threat to the UK increased in 2024, albeit at a slower rate than previously. We have seen a mixed picture across the different threats. There have been continued increases in child sexual abuse, drugs, and illicit finance. And last year's decreases in fraud and organised immigration crime have been reversed. More positively, the firearms threat has remained suppressed following the reduction last year. And the seemingly unstoppable growth in cybercrime was arrested, due to significant law enforcement disruptions; albeit the threat remains high, and may increase again as

criminals regroup. There has been no material change in the level of threat from modern slavery and human trafficking and organised acquisitive crime.

We said last year that the societal shift to living more of our lives online was being exploited by criminals in the form of cybercrime, fraud, and child sexual abuse. One of the most striking themes emerging this year is how the threat is diversifying between and beyond these threats, with a growing overlap with online radicalisation to serious violence and extremism. Other technological trends, such as increased adoption of artificial intelligence and easy access to communications channels with victims without content moderation or other safeguards, are allowing offenders to scale their offending more readily.

At the same time the physical harms from SOC are growing. We have seen drug supply, consumption, and deaths all increase, with new trends in drug use and smuggling. Migrant deaths in the Channel were over six times higher than in 2023. Online forums promote and lead to physical and sexual abuse.

These developments, many of which are paralleled in partner countries around the world, are challenging law enforcement's capacity and capability to respond. And we are responding. The assessment includes a section on how we are tackling the threat, along with a series of case studies from the NCA and policing. The case studies show how some of the most sophisticated and hardened criminals, be they in the UK or overseas, can be brought to justice; and how some of the most vulnerable people can be protected. I pay tribute to the brilliant officers and staff in the NCA and across policing and our partners who are behind these successes and so many others.

There is more to do. Like those we seek to disrupt, we need to become more agile to respond to the evolving threat, use the advances in technology and other capabilities to greater effect, and build new partnerships in the UK and globally, including seeking common cause with industry. This will empower us to both increase our impact on the SOC threat and to disrupt it in new ways. This assessment provides the foundation from which we can deliver an improved response. I look forward to working with all our partners across the system to meet that challenge head on.

**Graeme Biggar CBE**

## About the National Strategic Assessment

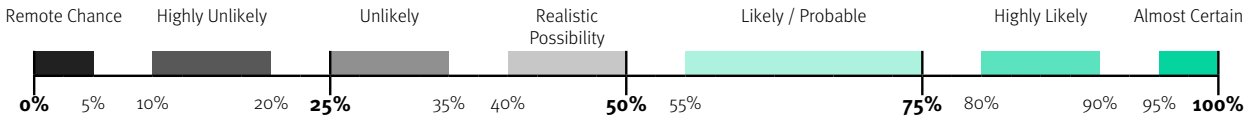
The National Strategic Assessment of Serious and Organised Crime (SOC) provides an annual assessment of the SOC threat in the UK. The emphasis in the report is on what changed in the SOC threat picture in 2024.

The main SOC threats considered in this paper are those set out in the UK Government's Serious and Organised Crime Strategy 2023-2028: child sexual abuse, cyber, drugs, firearms, fraud, modern slavery and human trafficking, money laundering, organised acquisitive crime, and organised immigration crime. Serious and organised offending is not limited to these offence types and other forms of offending are also considered in this assessment.

The intelligence collection period for the National Strategic Assessment 2025 is September 2023 to October 2024; however, where available, data and intelligence up to and including December 2024 has been used.

It is not always possible to be certain of a development in the threat, so throughout the NSA the 'probability yardstick' (as defined by the Professional Head of Intelligence Assessment) 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:




## Acknowledgements

The National Strategic Assessment is compiled by the National Assessments Centre, the NCA's centre for assessed intelligence reporting. We would like to acknowledge the support offered by many partners in the preparation of this assessment. Our partners include, but are not limited to:

- Law enforcement and criminal justice bodies, including the police forces of England and Wales, Police Scotland, Police Service of Northern Ireland, National Ballistics Intelligence Service, HM Revenue and Customs, the Serious Fraud Office, Border Force, Immigration Enforcement, HM Prison and Probation Service, and the Crown Prosecution Service;
- UK intelligence community, including the National Cyber Security Centre;
- HM Government, including the Home Office, Foreign, Commonwealth and Development Office, the Cabinet Office, and HM Treasury;
- Overseas law enforcement agencies and organisations such as Europol and Interpol;
- The academic, private and third sectors, including research from universities, charities, non-governmental organisations, banks, and other financial institutions, communication service providers and technology companies;
- Regulatory and professional bodies such as the Financial Conduct Authority and Ofcom; and,
- Opal, the national police unit focused on the collation, coordination, and dissemination of intelligence relating to organised acquisitive crime, who authored the organised acquisitive crime section of this product.

## SOC offenders are increasingly exploiting advances in technology to access victims and cause them harms on a larger scale

ADOBE STOCK

# Overview of SOC in the UK

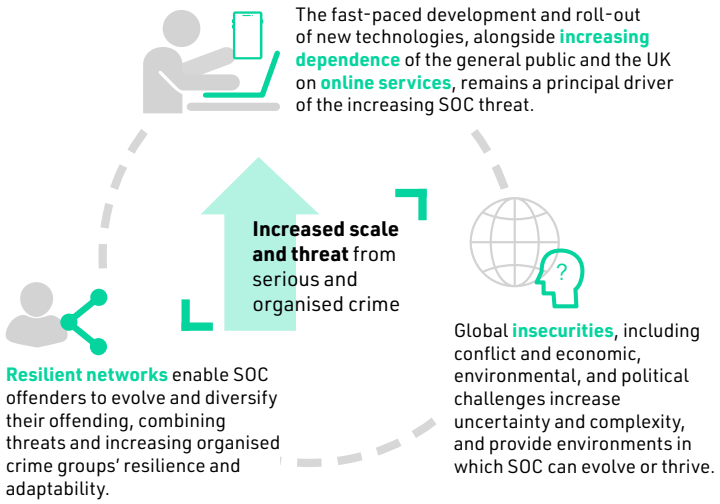
### The SOC Threat Today

SOC is a national security threat, causing significant levels of harm to individuals and communities, undermining confidence in government and law enforcement agencies, and impacting on economic prosperity and growth.

The SOC threat in the UK grew in 2024 but at a slower pace than in the previous, post-pandemic period. There was a mixed picture: some threats remained unchanged and others increased. The threat from illicit drugs continues to increase, causing harm to victims and communities, and driving many other types of criminality.

This growth in SOC is principally being driven by online connectivity and the growth of automation technology. Offenders are also taking advantage of opportunities for criminality created by global instability, including the demand from migrants to risk their lives to travel to the UK on small boats.

Online connectivity underpins a wide variety of offending including child sexual abuse, cybercrime, and fraud, and enables almost all serious and organised criminality in some form. SOC offenders are increasingly exploiting



advances in technology to access victims and cause them harm on a larger scale, connect with global networks, and enhance their adaptability and resilience to disruption.

Developments in automation technology and artificial intelligence are likely to be increasing the speed and volume of SOC offending, as well as the level of harm caused to victims.

The impact of these combined drivers is that SOC is likely becoming less hierarchical and more cellular, both within the UK and globally, with loose affiliations made and broken on a regular basis, and less obvious chains of command.

Loose networks serve to make SOC networks more resilient and agile in their response to change; however, to operate effectively, the criminal groups need to trust in each other and the professional and technological enablers that support them. This is a vulnerability which law enforcement agencies are increasingly looking to exploit.

SOC can affect anyone, but it almost certainly disproportionately impacts some of the poorest and most vulnerable communities in our society. It causes harm through the physical and psychological impact of SOC-related violence, exploitation, and abuse.

SOC erodes a community's sense of safety which contributes to a lack of trust in the police and the UK Government, and its ability to fight crime. It also has a significant impact on the capacity of local or neighbourhood policing, diverting investigative resources and limiting the gathering of community intelligence.

It is highly likely that the overall threat posed by SOC will continue to increase over the next 18 months, with the rapid evolution of the SOC threat challenging law enforcement's capacity and capability to respond.

## Key Trends in SOC in 2024

The SOC threat continued to increase in 2024, with technology both the core driver and enabler of this change. It is highly unlikely that we will see a reverse of this trend in the next 18 months.

A core characteristic of SOC in 2024 was the continued diversification of criminal activity beyond our previous understandings of the SOC threat. This is the result of the emergence of new groups of offenders with a broader range of motivations, diversification of methodologies, and more crossovers between different SOC threats.

Criminal business models continue to adapt to a more interconnected and unstable world. A key trend in 2024 was for offenders to broaden their criminal activity across multiple threat areas, enabled by online connectivity, use of new technology, and reliance on the specialist services offered by 'crime as a service' providers. It is becoming increasingly easier for SOC offenders to connect with other offenders or to enter new criminal marketplaces.

**SOC Online**

SOC offending continues to evolve most rapidly in the online world. Privacy enhancing technologies, including end-to-end encryption, continue to provide opportunities to offend undetected across a wider range of platforms, especially when implemented without sufficient consideration for public safety. This hinders law enforcement and companies' capacity to identify illegal material, gather evidence, conduct investigations, and thus protect the public.

Generative artificial intelligence technology has not yet been integrated into most SOC offending but there has been an increase in its use to generate partial and fully synthetic child sexual abuse material. Across other threat areas, generative artificial intelligence almost certainly has the potential to enhance offender capabilities and increase the speed, scale, and sophistication of attacks.

While artificial intelligence also presents opportunities for law enforcement to scale up, the quantity of material produced using this technology will challenge law enforcement's ability to keep pace with the increasing sophistication and evolution of this threat. This risk is magnified by the use of end-to-end encryption, which reduces moderation of material circulated, unless reported by recipients.

2024 saw the increased identification of 'Com' networks: networks of individuals typically operating on social media or instant messaging platforms which routinely share harmful content and extremist or misogynistic rhetoric. Extreme and illicit imagery depicting violence, gore, and child sexual abuse material is frequently shared amongst users, normalising and desensitising participants to increasingly extreme content and behaviours.

'Com' networks use extreme coercion to manipulate their victims, who are often children, into harming or abusing themselves, their siblings, or pets, and re-victimising them by doxing or appropriation by other offenders. Members of 'Com' networks are usually young men who are motivated by status, power, control, misogyny, sexual gratification, or an obsession with extreme or violent material. The emergence of these types of online platforms are almost certainly causing some individuals, especially younger people, to develop a dangerous propensity for extreme violence.

**The Impact of SOC on Communities**

Violence against women and girls continues to be a feature of many types of SOC offending, although levels of organisation vary. Overall, the harms posed to female victims of SOC are likely higher than those posed to male victims. Organised crime groups involved in child sexual abuse and modern slavery and human trafficking deliberately target women and girls to exploit vulnerabilities, including their relationship to the offender, relative deprivation, substance addiction, and a lack of support networks. Within child sexual abuse offending, males continue to commit the majority of offences (82%) while females make up the majority of victims (79%).

It is almost certain that the indirect consequences of SOC activity disproportionately impact some of the most vulnerable individuals in society, especially in relation to drug use. Heroin and crack cocaine use is strongly linked to deprivation. 56% of individuals arrested by police between March 2022 and September 2024 tested positive for cocaine, opiates, or both. The Association of Police and Crime Commissioners estimate that half of all acquisitive crimes and half of all homicides are drug-related.

It is almost certain that a range of criminal activity linked to SOC takes place within communities, and is either unreported or not recognised as SOC-related. This includes a range of activities which can cause fear and distress, such as racketeering, extortion, and kidnap.

Some SOC nominals were linked to incidents of violent disorder in July and August 2024, directed towards migrant accommodation, mosques, and police, with their level of involvement ranging from organising events to participating in acts of disorder. This involvement was unlikely to be directly related to SOC activity and was more of a reflection of the offenders' political views or their affiliations to far-right or extremist organisations.

SOC offenders are highly likely capitalising on opportunities provided by pressures within the criminal justice system and law enforcement, which include financial constraints, recruitment challenges, and technological deficits. Deterrence depends on the perception that offenders will be detected, and that

justice will be swift and proportionate to the crimes. However, short or suspended sentences, longer times between arrest and sentencing, and challenges in maintaining supervision on probation, likely reduce the level of deterrent that SOC offenders have from the criminal justice system. Furthermore, the rapid adoption of new technologies by offenders and the general public creates additional vulnerabilities that challenge the system to maintain legislation and sentencing frameworks proportionate to the harms experienced.

**SOC Overseas**

It is likely that the risk to the UK from SOC-linked to countries across South East Asia has increased and will continue to grow through 2025. This is almost certainly due to a range of different factors impacting on different parts of the region at the same time, including the legalisation of cannabis in Thailand, the evolution of the fraud threat in South East Asia (although the level of impact on the UK is not yet known), and increased irregular migration from Vietnam into the UK.

It is highly likely that, cumulatively, offenders linked to China currently pose the biggest non-British SOC threat to the UK. The SOC threat from China to the UK comes from Chinese national offenders based within China and globally, including within the UK. Chinese national offenders are linked to cyber, drugs, fraud, illicit finance, modern slavery and human trafficking, and organised immigration crime offending that impacts on the UK.

It is highly likely that some foreign states, including Iran and Russia, continue to be permissive of SOC activity which supports their objectives and is conducted from within their jurisdictions. Ransomware groups operating from countries such as Russia and Iran, which are uncooperative to Western law enforcement, make disruption more problematic.

It is highly likely that some states are able to harness SOC, especially cybercrime, international drug trafficking, and money laundering, to support their state objectives and/or evade sanctions. For example, North Korea has deliberately engaged in SOC to support its fiscal position. It is likely that several other countries possess the capability and intent to gather information and conduct activity against the UK and its allies using individual criminals.

Albanian organised crime groups continue to be linked to a range of SOC threats impacting on the UK, especially drug supply and production. Albanian organised crime groups use networks of Albanian national 'brokers' to connect individuals together in encrypted chat groups to facilitate commodity movements worldwide.

## How the Threats Changed in 2024

**Child Sexual Abuse**

The scale, severity, and complexity of child sexual abuse is increasing and continues to cause substantial long-lasting harm to victims. The hidden nature of online and offline types of child sexual abuse continue to create challenges for law enforcement, with around a quarter of all reported physical sexual abuse classed as non-recent. Online, offenders are increasingly using generative artificial intelligence to produce partial and fully synthetic child sexual abuse material, including the creation of images which are sadistic or extreme in nature.

The child sexual abuse threat continues to evolve, especially in the online space where it is almost certainly becoming more monetised. The financially motivated sexual extortion of children, more commonly known as sextortion, continues to predominantly affect young males. Financially motivated sexual extortion has

been driven in particular by West African offending methodologies capable of indiscriminately targeting large numbers of victims, including children. This trend has likely been exacerbated by accessibility to technology such as chatbots, as well as the proliferation of online guides to sextortion on the internet. Police recorded crimes of this type reduced in the first half of 2024, although it is too early to confirm if this is a lasting trend.

**Cyber**

The cyber threat persisted in 2024 despite the splintering of the ransomware market as a result of law enforcement disruptions against LockBit and BlackCat. There is an increasing threat from younger UK-based cybercriminals, although these make up a small proportion of the overall threat picture.

**Drugs**

It is likely the threat from drugs to the UK increased in 2024. It is almost certain that drug organised crime groups are increasingly collaborating in order to traffic larger shipments into the UK; for example, sharing transportation networks and distribution enablers. Cocaine use in the UK has increased, with overseas cocaine production also seeing a potential significant upturn. Criminals continue to supply the UK heroin market despite reduced opium production in Afghanistan. Cannabis importations are rising, while large scale domestic cultivation continues. Ketamine use is increasing and causing significant physical and mental harm to individuals. Global synthetic drug markets are rapidly evolving and pose significant harm to users.

The level of harm caused to victims and communities, continued to increase in 2024. This was driven by a dangerous combination of domestic and global drivers, including increasing demand for drugs in the UK, an abundant supply in most drug producing countries, sophisticated and adaptable drug importation methods, and an expanding synthetic drug market. The fortification of heroin with nitazenes and other synthetic opioids has increased the risks of harm to users. Drug-related deaths in the UK increased by 15% in 2023, with 4,936 drug misuse deaths in England, Wales, Scotland, and Northern Ireland.

**Firearms**

There is no evidence of substantial change in the overall threat of criminal intent, capability, and opportunity to source and use firearms in 2024. The UK continues to have some of the lowest levels of firearms crime in the world. It is highly likely that this is due to the continued suppression of organised crime group access to firearms and ammunition within the UK. This is in contrast to some European countries where there was a rise in levels of SOC-related violence, especially firearms incidents, in 2024.

**Fraud**

It is likely that the fraud threat to UK individuals and businesses has increased since 2023, although estimated fraud levels are similar to those last seen in 2019. Fraud remains a significant problem for the UK and remains the most prevalent crime against individuals in England and Wales, accounting for an estimated 41% of all crime reflected in the Crime Survey for England and Wales in the year ending September 2024. The population's routine dependence on online services continues to provide opportunities for fraud offenders to target victims, sustaining the UK's vulnerability to fraud. Industry prevention measures continue to contain the threat from fraud to some extent, but some fraud types, such as card-not-present fraud, are increasing.

**Illicit Finance**

It is likely that the amount of money laundered in the UK increased in 2024 due to growth in the underlying criminal offences, including drug supply. It is a realistic possibility that the impact and harm to the UK caused by money laundering has also increased. Criminals continue to identify innovative ways to launder

the proceeds of their crimes. International money laundering networks have amplified their capabilities through the adoption of technology and broadened their client base across multiple threat areas.

It is likely that the threat relating to money laundering by Chinese-speaking organised crime groups in the UK, already one of the highest money laundering risks, has been increasing.

The scale of activity by the Russian-speaking money laundering networks investigated under NCA-led Operation DESTABILISE is highly likely greater than previously reported. These groups provide cash to cryptocurrency conversions in the UK and overseas, to launder funds for transnational organised crime groups. They have a combined global reach extending to over 30 countries and move billions of dollars. As well as laundering funds for transnational organised crime groups they have enabled Russian elites and entities to evade UK financial sanctions, and have funded Russian espionage operations.

**Modern Slavery and Human Trafficking**

There is no evidence of substantial change in the overall threat and harm from modern slavery and human trafficking in 2024. It is highly likely that factors that underpin offending, such as profitability, consumer demand, offender capability, and vulnerability to exploitation, remain largely unchanged. Most victims reported to the National Referral Mechanism are children being exploited for criminal activity.

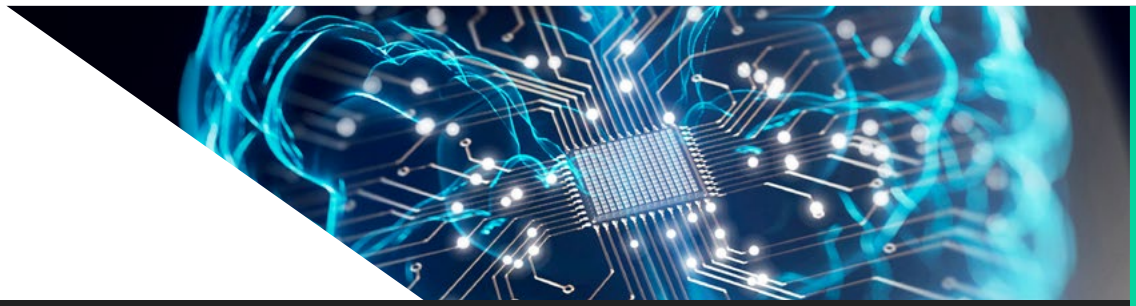
**Organised Acquisitive Crime**

It is likely there was no substantial change in the threat from organised acquisitive crime in 2024. Reported organised acquisitive crime offences were steady overall, with some degree of fluctuation across specific crime areas. High domestic and international demand for second-hand and cheaper products continues to be a key driver of organised acquisitive crime.

**Organised Immigration Crime**

The organised immigration crime threat to the UK increased in 2024, with a 25% increase in small boat arrivals from 29,437 in 2023 to 36,816 in 2024, but 19% lower than in 2022 (45,755). 2024 was the deadliest year to date for small boat migrants, with 78 fatalities. Organised immigration crime offenders are taking greater risks to service migrant demand for small boat crossings, including use of cheaper, more dangerous boats. Risks associated with other types of clandestine entry have also increased, including more use of refrigerated HGVs.

## As more people spend more time online, it is easier for offenders to target people in the UK



GETTY IMAGES

# Cross-Cutting Threat Enablers

To effectively tackle SOC in the UK it is important to target factors that can impact across a range of criminality. These cross-cutting vulnerabilities and enablers enhance organised crime groups' abilities to conduct crime. Those covered in this section include:

**The Criminal Use of Technology |** Technology and online spaces enable most SOC offending.

**The UK Border |** By exploiting vulnerabilities at the UK border, organised crime groups seek to move commodities in and out of the UK and evade detection.

**Insider Threats, Bribery and Corruption |** Insiders, bribery, and corruption enable offending and threaten the UK's national security, economic prosperity, and international reputation.

**Prisons and Probation |** The prisons estate provides opportunities for offenders to network and develop their offending, both inside and on release.

## The Criminal Use of Technology

Online, offenders are able to increasingly exploit a wide range of vulnerabilities and opportunities, taking advantage of increased connectivity and the ability to offend on a greater scale. As more people spend more time online, there is potential for a greater number of offenders, including those based overseas, to target UK victims.

The fast-paced development and roll-out of new technologies remains a principal driver behind the growth of SOC. Technologies that make it easier and more lucrative to commit offences, reduce the risk of detection, and extend the range of offending across global jurisdictions will continue to be adopted by criminals.

It is likely criminal 'as a service' providers will increasingly enable criminals to access and leverage the most cutting-edge technologies. Once a technology has been shown to benefit an organised crime group, it is likely to be integrated into wider offending models, as long as it is accessible and affordable.

Criminal uptake of new technologies generally happens faster than adoption within government and law enforcement, as a result of ethical, legislative, and procurement factors, and limited capacity to develop workforce skills; constraints which typically do not affect offenders.

Business email compromise is much more prolific and profitable to offenders than ransomware, with the FBI assessing that global business email compromise losses were on average at least $5 billion each year over the past decade, compared to ransomware payments of approximately $813.55 million in 2024. However, the significance of ransomware is in disruption to users and services, data breaches, and remediation costs. As the volume of ransomware incidents has increased, it is almost certain that the quantity of personal data available online to criminals has increased.

Although the risks around generative artificial intelligence are increasing, there has not yet been a widespread adoption of this technology by serious and organised criminals. For now, generative artificial intelligence serves to amplify existing risks, rather than creating new ones, thereby increasing the level of harm and the scope and range of offending.


of UK internet users over 16 reported **using a generative AI tool** in the past year.

Source

It is highly likely that more organised crime groups and lone offenders will use artificial intelligence technologies as they become cheaper and more accessible. This will enable them to offend on a greater scale with a higher degree of sophistication. 41% of UK internet users aged over 16 said they had used a generative artificial intelligence tool in the past year.

The use of generative artificial intelligence as an enabler of SOC will continue to increase in 2025, especially in relation to child sexual abuse, cybercrime, and fraud. Generative artificial intelligence is increasingly being used to produce large volumes of partial and fully synthetic child sexual abuse material, including sadistic or extreme imagery. This will increase the overall volume of child sexual abuse material available online and put additional pressure on law enforcement agencies.

The deliberate creation of deepfakes for malicious purposes has become easier and cheaper. It is almost certain that human detection of deepfakes will become impossible by 2029, with some industry figures predicting that by 2025 not even the best experts will be able to discern deepfakes from genuine media.

The development of privacy enhancing technologies, including end-to-end encryption, continues to provide offenders with opportunities to obscure their activity on a wide range of platforms. Meta, for example, began to roll out end-to-end encryption by default across Facebook Messenger chats for UK customers from January 2024.

The expansion of privacy enhancing technologies hinders law enforcement's efforts to identify illegal material, gather evidence, and conduct investigations. Privacy enhancing technologies will almost certainly become more sophisticated and more widely integrated into existing technologies as companies seek to innovate and as the public comes to expect greater levels of control over data and privacy.

It is likely that offenders are increasingly using social media platforms, rather than more traditional e-commerce marketplaces, to buy or sell illicit goods. Criminals often seek to use the same platforms as the general public in order to connect them to the largest marketplaces. Facebook, Instagram, TikTok, and Telegram, for example, are all platforms used by criminals involved in organised immigration crime.

Online platforms are also used by fraud criminals to deceive customers by selling counterfeit goods or not dispatching items which have been paid for. Some fraud offenders are able to use algorithms on these platforms to deliver targeted advertisements directly to potential victims.

The dark web continues to be used to commit many types of SOC, including child sexual abuse, cybercrime, fraud, and to facilitate illicit commodity supply. It is likely that some offenders are moving from the dark web onto the clear web, or encrypted apps, as privacy enhancing technologies are more widely deployed on these platforms.

It is likely that drones will become more widely integrated into SOC offending models as costs decrease and functionality improves. Serious and organised criminals are increasingly using drones for a range of activity including transporting illegal commodities and conducting reconnaissance activity.

## The UK Border

Commodity-based SOC crime in the UK, such as the supply of drugs and firearms, relies on international flows of illicit goods and the ability of organised crime groups to circumvent controls at the UK border. Albanian organised crime groups, for example, are responsible for regular multi-tonne cocaine movements out of South America, and particularly Ecuador where they have a strong presence.

Most modes of transport used by organised crime groups for smuggling commodities remained consistent in 2024 although there were significant increases in detections of illicit goods, in particular cannabis, being smuggled via international parcel operators, the postal service, and by air passengers and freight. Cannabis seizures across these modes increased significantly in 2024.

The volume of legitimate freight traffic across the UK border in roll-on/roll-off vessels provides opportunities for criminals to conceal commodities and to connect with overseas supply routes. It is almost certain that organised crime groups involved in smuggling cocaine into the UK continue to have a high level of confidence in the roll-on/roll-off method, as demonstrated by increased levels of cocaine seizures at the border from roll-on/roll-off traffic in 2023 and 2024.

Organised crime groups continue to exploit weaknesses in outbound controls at the UK border to export stolen vehicles and machinery, mobile phones, illicit cash, and to supply drugs to lucrative overseas markets. Organised crime groups can maximise profits by supplying drugs to countries where prices are higher, including Australia, New Zealand, and Japan.

It is likely that organised crime groups moving illegal commodities across the UK border will be forced to review their smuggling methodologies in response to new legislation. New requirements for safety and security declarations for imports into the UK were introduced from January 2025. The introduction of this new regulation will allow for more targeted interventions by border agencies. There is a realistic possibility this will cause organised crime group displacement to alternative modes such as the roll-on/roll-off tourist mode, which does not require the same declarations.

Incidents of Class A drugs being found washed-up on British and Irish shores continued in 2024. This is likely an indicator that the general maritime method continues to be used more frequently, to import drugs, than was observed pre-2023. Similarly, general aviation continues to be abused by criminals who have access to light aircraft and/or helicopters, which are capable of making flights to numerous airfields and suitable landing areas in the UK.

The overseas legalisation and decriminalisation of commodities which remain illegal in the UK continues to create a challenge for law enforcement. High volumes of cannabis imports from Thailand and North America

continue to impact UK law enforcement resources, with seizures in 2024 surpassing the record levels seen in 2023. While users in the UK are paying a significant premium for North American and Thai cannabis, wholesale prices have reduced to approximately 10-20% above the price of UK-grown cannabis. Cannabis from North America and Thailand remains largely indistinguishable, in terms of its chemical composition, from cannabis supplied from other sources, including cannabis produced within the UK.

The number of arrests for cannabis importation via the air passenger mode increased significantly by 456% between 2023 and 2024, from 134 to 745. This compares to a pre-pandemic baseline of 56 in 2019. Smugglers using the air passenger mode travel with wholesale quantities of cannabis, sometimes carried in multiple pieces of luggage, and averaging more than 20kg per detection.

**456%**

increase in arrests relating to **cannabis seizures** in the air passenger mode.

*i* Source

The Common Travel Area, and particularly the routes between Ireland, Northern Ireland, and Great Britain, continues to be exploited by criminals for the purposes of immigration crime, excise fraud, and for the smuggling of illicit commodities. In 2024, a trend emerged which saw foreign nationals entering the UK and then using the Common Travel Area to travel onwards to Ireland. Naturalisation in Ireland affords an individual access to both the UK and European Union, making Ireland an attractive country to migratory communities. There has also been an increase in the smuggling of raw tobacco over the Ireland-UK border bound for illicit UK factories.

It is highly likely that organised crime groups are taking advantage of additional ferry routes between mainland Europe and Ireland in order to avoid detection at the UK border. Since the beginning of 2023, there has been a notable increase in seizures of cocaine in excess of 100kg at Irish ports from ferry routes originating from within the European Union.

Technological developments such as the automation of container movement and the use of telematics continue to present a range of risks and opportunities, for both organised crime groups and law enforcement. GPS tracking devices continue to be used by criminals to remotely track the movement of commodities. Some organised crime groups have used hidden GPS trackers to track the crossing of small boats transporting irregular migrants across the English Channel.

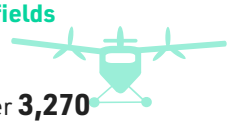
## UK Border Operating Environment

In the UK, high volumes of passenger and freight traffic move through a multitude of environments.

Criminals can exploit these routes, creating opportunities for serious and organised crime.

This makes the UK border an extremely challenging space for law enforcement to control.

**Airfields**



Over **3,270** aerodromes, small airfields, farmers' field strips, and helipads

**Airports**

**38** international airports

**Vessel Landing Sites**

Approximately **3,500** general maritime official landing sites

**International Rail**



**1** passenger terminal to/from Europe via the Eurostar

**2** main rail depots receiving freight direct from the Channel Tunnel

**Sea Ports**

**51** major freight seaports

**27** roll-on/ roll-off ports

Source: Department for Transport, Civil Aviation Authority, Home Office.

## Insider Threats, Bribery and Corruption

Corruption and the use of insiders in both the public and private sector continues to enable organised crime groups to carry out their offending. While the number of corrupt individuals actively enabling SOC is likely to be low, the impact that insiders have is disproportionately high.

Corrupt insiders continue to facilitate the movement of illicit commodities, divulge sensitive information, and circumvent security measures, reducing the likelihood of law enforcement detection.

Individuals working in law enforcement, the Prison Service, logistics, and at the UK border are particularly vulnerable to targeting by organised crime groups. This is typically achieved through bribery, financial incentives, or the preservation or advancement of familial, social, or romantic associations. Albanian organised crime groups, for example, use a large network of corrupt insiders at ports to evade border controls, including at UK maritime ports, airports, and postal depots.

Individuals working in sectors such as accounting, banking, and legal services are also vulnerable to targeting by organised crime groups, as these roles can provide valuable assistance in the laundering of the proceeds of crime and fraudulent activity. These professional enablers are integral to the threat from SOC.

The UK continues to face the challenge of its financial services and corporate structures being exploited to launder the proceeds of SOC, including both international and domestic bribery and corruption.

## Prisons and Probation

It is likely the SOC threat in prisons remained broadly unchanged in 2024.

Some individuals continue to offend after release from prison, even when they are subject to probation supervision, although the exact number is not known. Approximately 20-30% of offenders under NCA Serious Crime Prevention Orders are found to have breached their orders, or actively re-engaged, in SOC-related activity.

It is highly likely that imprisonment of some high-level members of organised crime groups does not significantly disrupt their ability to run criminal enterprises, particularly when they retain access to external criminal associates and funding whilst in prison.

Mobile phones are the biggest enabler of serious and organised criminality from within the prison estate although other methods of illicit communication are also used to direct criminal activity, both inside and outside of prisons. Activity also includes accessing illegal material on the internet and the dark web, and stalking, harassing, and exploiting victims.

Prison staff corruption continues to serve as a key enabler of SOC activity in prisons through the direct and indirect conveyance of illicit items such as drugs and mobile phones into the prison estate, and the overlooking of inappropriate or criminal behaviour. Indirect conveyance involves facilitation, for example, providing security information to enable others to bypass security systems and to evade searches and subsequent detection.

Criminal networking in prison almost certainly leads to the formation of new associations. The movement of prisoners around the prison estate provides networking and opportunities for criminal diversification and the sharing of skills and knowledge.

Drone incidents in prisons have almost doubled over the last two years, with drones primarily used to smuggle mobile phones and drugs into UK prisons. New air navigation regulations were introduced in January 2024 to restrict the flying of drones in the vicinity of prisons and young offender institutions in England and Wales. It is too soon to understand the full impact of this legislation but it is intended to aid police and prison collaboration and facilitate a tactical response.

# The risk to children from sexual abuse continues to increase, aggravated by evolving online environments and technology adoption


ADOBE STOCK

## Child Sexual Abuse

Child sexual abuse covers a range of offence types occurring online, offline, or moving between both, with the hidden nature of offending making it hard to detect and under-reported. Child sexual abuse disproportionately affects female victims, with four in five sexual crimes against children committed against girls, where gender is recorded. Offending by 10 to 17 year olds continued to represent around half of all police reported child sexual abuse crimes in 2024, with approximately three quarters of offending occurring outside of the family environment. We estimated in the National Strategic Assessment 2024 that 710,000 to 840,000 adults in the UK pose varying degrees of sexual risks to children.

From Q1 to Q3 2024, analysis conducted by the Vulnerability Knowledge and Practice Programme showed that 64% of child sexual abuse offences recorded by the police in England and Wales related to physical sexual abuse, with around one third committed within the family environment and around three quarters classed as recent. Analysis by the CSE Taskforce showed that group-based offending made up only 6% of the 64%, with the same proportion (around one third) committed within the family environment. However, police recorded crime does not effectively reflect the full scale of online offending, as one offence can relate to multiple instances of child sexual abuse material, and the most serious physical offence is recorded instead of any precursor online offences such as grooming.

Social media and gaming platforms encompass a wide range of communication and file sharing features, and often lack safety measures, such as robust age verification and effective moderation processes and reporting mechanisms. For example, the deployment of

**2,892**

**12% increase compared to previous year**

counselling sessions were provided by Childline to children, where their main worry was **online harm and safety**, or **online sexual abuse and exploitation**.

*i* Source

end-to-end encryption without appropriate mitigations on social media platforms can undermine Safety by Design and impairs industry ability to identify child sexual abuse content.

Online networks of offenders engaging in a range of online offences ('Com networks') have been identified grooming, blackmailing, and threatening victims into carrying out extreme acts, including sharing sexual material and self-harming. Vulnerable young victims are targeted and groomed online, and controlled through fear and manipulation to extort imagery and cause harm. These networks typically attract young males promoting nihilistic and misogynistic views, who attempt to gain status with other users by committing or encouraging harmful acts across a broad spectrum of offending.

Developments in technology continue to drive and enable more complex online child sexual abuse. This includes the manipulation of legal generative artificial intelligence tools to create child sexual abuse material which is illegal, shown with recent substantial convictions. The US National Center for Missing & Exploited Children is expected to have seen a significant rise in reports of child sexual abuse material or other sexually exploitative content related to generative artificial intelligence over the course of 2024. The use of generative artificial intelligence systems without safeguards to prevent the generation of indecent images of children will undermine law enforcement efforts to identify and safeguard victims.

The identification of indecent images of children has continued to increase, with the Internet Watch Foundation identifying 291,273 webpages confirmed as containing indecent images of children in 2024, a 6% increase since 2023. Of these, 91% were classified as self-generated indecent imagery, either shared consensually, or elicited through manipulation. Testimonies of children from UK-based reports indicate they are increasingly viewing self-generated indecent imagery as commonplace, with peer norms creating pressure on young people to create self-generated indecent imagery. The most common age of victims is 13 to 14, with a continued upward trend in reports of children aged under ten, and in particular those aged seven to ten. While dark web forums continue to be used by child sexual abuse offenders, secure clear web platforms are increasingly used for a range of child sexual abuse offence types, including those involving direct access to children online.

**91%**

of reports actioned by the IWF in 2024 were assessed as containing **self-generated indecent imagery**.

*i* Source

The financially motivated sexual extortion of children continues to predominantly affect young males, with 14 to 17-year-old males representing 90% of victims detected in National Center for Missing & Exploited Children reports. This is in contrast to sexually motivated extortion, and other types of child sexual abuse, where the majority of victims are female. While police recorded crimes of sexually motivated extortion reduced in the first half of 2024, it is too early to say if this is a firm trend.

It is highly likely that victims of financially motivated sexual extortion are most commonly engaged on the social media platforms preferred by young people. These popular platforms often have functions that create favourable conditions for offenders to easily create fake accounts, access potential victims at scale, and view their personal information and social networks in order to extort them.

## Case Study | Administrator of a Child Sexual Abuse Site

In July 2024, Colin Thackeray pleaded guilty to three counts of making indecent images of children and one count of possessing indecent images following an NCA investigation. He also pleaded guilty to a count of intentionally assisting the distribution of indecent images of children, encouraging the sexual assault of a child under 13, and inciting a child under 13 to engage in sexual activity.

Thackery was identified as a high-ranking administrator on a Tor child sexual abuse site, which had been taken down by Dutch Police. On the site he discussed and shared child sexual abuse material, while also engaging with users on dark web messaging services to provide advice on grooming children and how to start sexually abusing them.

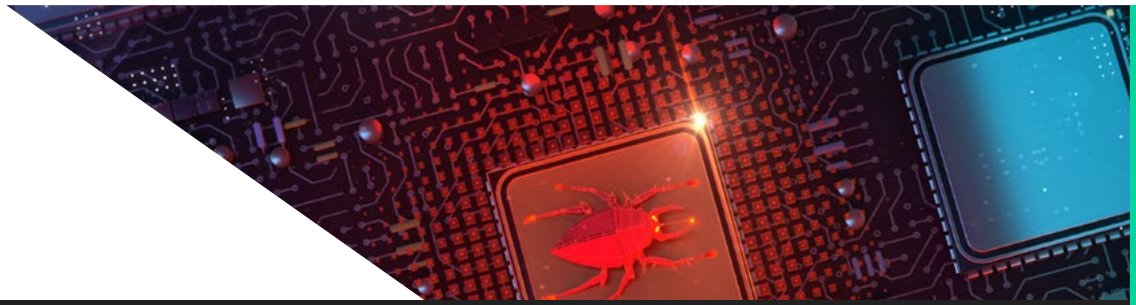
Moderators and administrators of child sexual abuse sites like Thackery pose a significant risk to children, given their capacity to influence and advise other offenders. Thackery was sentenced to 17 years, including 10 years in prison and 7 years on extended licence, and received a comprehensive Sexual Harm Prevention Order for life.

## Uses of Generative Artificial Intelligence Technologies in Offending

| Technology Definitions | | | | | |
|---|---|---|---|---|---|
| **Companion Apps** | **GenAI Models** | **Voice Cloning Software** | **Large Language Models** | **Nudifying Apps** | **Image Editing Apps** |
| Applications designed to interact with a user with personalised and humanlike responses. Some applications use avatars which can be called and messaged. | Models or machine learning software that can generate new and unique content such as text, images, sound, and videos by learning patterns from large datasets. | Technology that analyses a person's voice for tone, intonation, and speech cadence, in order to create a synthetic version. | Models trained to conduct language tasks like, generating text, language translation, or answering questions in a human manner; can freely change responses as it learns. | Image editing applications that alter photos to remove the subject's clothes. | Applications that can realistically alter photos or make edits tailored to a user's choice. |

| Uses | | Technology Used | | |
|---|---|---|---|---|
| **Grooming** | Convincing child personas can be created in order to interact with children, with voice cloning software enabling the simulation of a child's voice for authenticity. | **Voice Cloning Software** | **GenAI Models** | **Large Language Models** |
| **Concealment** | Image editing apps, GenAI models, and LLMs can be used in the creation of fake personas to conceal an offender's identity. | **Image Editing Apps** | **GenAI Models** | **Large Language Models** |
| **Extortion** | Nudifying apps, image editing apps, or GenAI models can be used to create or threaten the creation of pseudo imagery of a victim, for the purposes of sexual or financial extortion. | **Image Editing Apps** | **GenAI Models** | **Nudifying Apps** |
| **Child Sexual Abuse Material** | Partial or fully synthetic GenAI child sexual abuse material can be created at scale using nudifying apps, GenAI models like Stable Diffusion and image editing apps. | **Image Editing Apps** | **GenAI Models** | **Nudifying Apps** |
| **Pathways to Offending** | Companion apps can be used by offenders to simulate conversations with a child or can engage in sexualised interactions with a childlike character, promoting high risk sexual behaviour. | **Companion Apps** | | |

# Ransomware continues to be the major cybercrime threat to the UK and has persisted despite law enforcement's disruption of the main variants



ADOBE STOCK

## Cyber

Ransomware conducted for financial gain remains the foremost SOC cyber threat to the UK and this is highly unlikely to change over the next 12 months. A similar level of UK ransomware incidents was reported to NCA this year compared with last year (560 for 01 November 2022 to 30 October 2023, compared to 547 for 01 November 2023 to 30 October 2024). Disruption to major strains like LockBit and BlackCat has contributed to keeping the number of ransomware attacks nearly static and preventing an increase.

Ransomware causes significant financial loss to victims and can put personal data taken at further risk of exploitation. The attack on pathology service Synnovis in June 2024 caused over 10,000 postponed appointments at London hospitals. However, it is likely that for the most part ransomware is opportunistic, and unlikely that any sector is being disproportionately targeted.

**520**

**9% decrease compared to 569 incidents in 2023**

ransomware incidents in 2024 as a result of SOC activity impacting UK organisations and businesses.

*i* Source

The range of different extortion tactics in ransomware has continued to diversify in the last 12 months. In a typical ransomware attack, any of the following may occur: the encryption of data; the threat to publish that data; threatening to report victims to the authorities for a data breach following a successful attack; and alerting a business victim's customers to their compromise. Ransomware groups have also incorporated distributed denial of service attacks into their operations.

Stand-alone distributed denial of service attacks - not linked to ransomware - are likely from hacktivists or lone actors rather than organised crime groups. They have continued to increase over the last 12 months due to the increase in size and speed of the internet and attackers' attempts to overcome defences. The



Quick Links: Home | Overview of SOC | Cross-Cutting Threat Enablers | Child Sexual Abuse | Cyber | Drugs | Firearms | Fraud | Illicit Finance | Modern Slavery and Human Trafficking | Organised Acquisitive Crime | Organised Immigration Crime | Tackling the Threat

UK does not appear to be disproportionately impacted by these, nor is it one of the most targeted countries internationally.

Other cyber-dependent crime has not emerged as a replacement for ransomware attacks by organised crime groups, highly likely due to the accessibility and profitability of ransomware. The majority of theft of cryptocurrency directly from crypto exchanges ('crypto-heists' - annual global losses estimate $2.2 billion) is likely carried out by threat actors associated to the state of North Korea. Business email compromise also leads to profitable fraudulent activity following a cyber intrusion. There have been indicators of malware seen in criminal campaigns that were designed to specifically steal credentials linked to crypto coin infrastructure, such as bitcoin wallet addresses. Other forms of cryptocurrency-based crime include crypto-jacking, or using another system's processing power to mine cryptocurrencies. However, the profits from this are very small compared to those of ransomware.

Most ransomware groups continue to operate from jurisdictions that do not cooperate with Western law enforcement, However, direct disruption by the NCA and other international partners significantly reduced the threat from LockBit ransomware by closing down infrastructure and undermining the trust of other cybercriminals. This has reduced the UK and global threat from LockBit, at that point the most prolific ransomware group ever, with over 2,350 victims in 112 countries, more than double its closest competitors. Since the disruptions of LockBit and BlackCat, we have also observed an increase in the number of ransomware groups, with none having nearly the level of market share of the previous leaders.

It is almost certain that the threat from cybercriminals based in the UK and other English-speaking countries, such as the USA, has increased relative to 2023. This increase is driven by a loose association of online entities from a wider internet-based subculture nicknamed 'The Com'. To access victims they mainly use phishing, vishing, and SIM swapping. They have also deployed ransomware strains and demonstrate a diverse range of tactics.

Despite this, the number of technically capable cybercriminals in the UK highly likely remains small compared to countries such as Russia. Law enforcement action makes it highly unlikely the cyber threat from English-speaking countries will match the threat from those based in more permissive jurisdictions where criminal activity is tolerated by the state or where cyber legislation is lacking.

The vast majority of ransomware is conducted by financially motivated criminals and not directed by states, but it is likely that Russia permits cybercriminals to carry out illegal cyber activity as long as it aligns with the state's interests. Russian intelligence services have been linked to cybercriminal groups conducting activity on their behalf in the past. One such group was EvilCorp, which was sanctioned in 2019, and again in 2024, by Australian, UK, and US authorities following the use of LockBit ransomware by some of its members. The leader of the group had previously been tasked by the state to acquire confidential documents, although no tasking for the deployment of ransomware is known. There were also indications in leaked documents that the Conti ransomware group has conducted undisclosed activity on behalf of the Russian state.

Prior to 2019, the leader of EvilCorp had a family connection to a senior member of the Russian Intelligence Services; while Conti had a business structure likely making the group more widely known and accessible, including to the Russian state, than the majority of ransomware groups. It is an intelligence gap whether such state links are also found across other ransomware groups. However, the Russian state tolerates ransomware actors operating from within Russia provided domestic infrastructure is not affected.

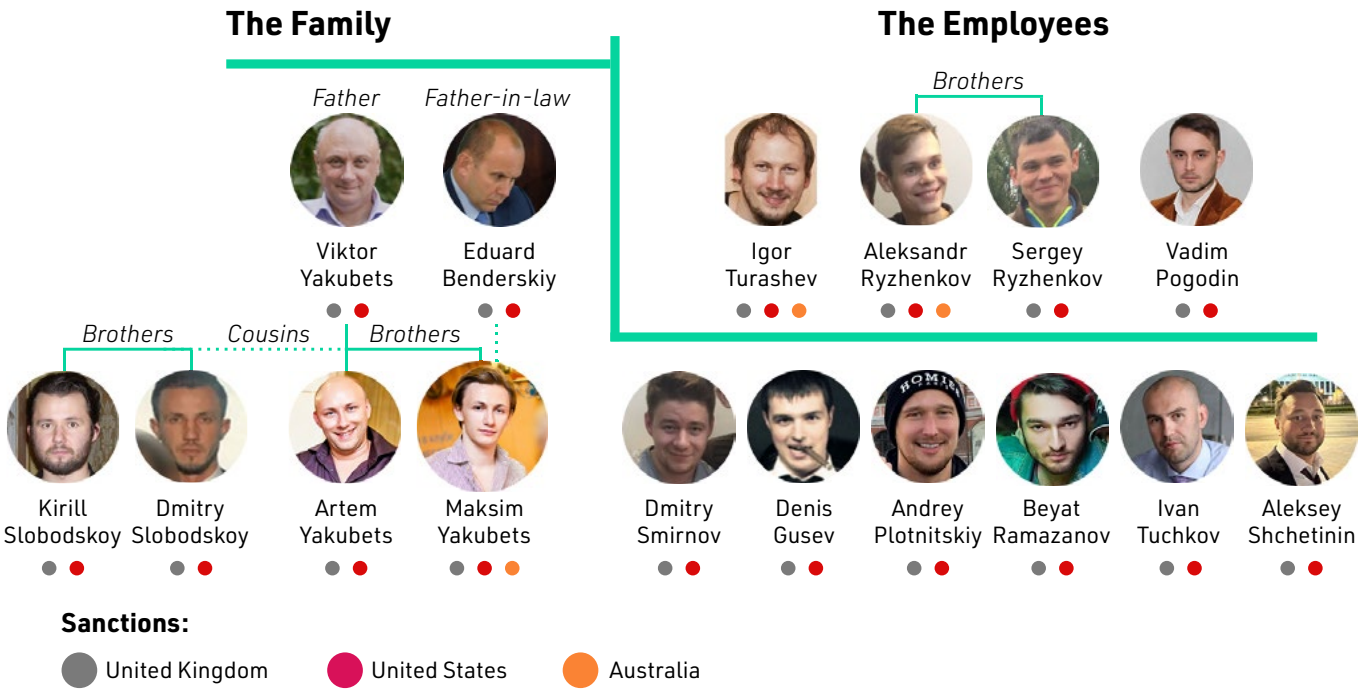
## Case Study | Takedown of Distributed Denial of Service for Hire Website

In 2024, the NCA took over a distributed denial of service for hire website, digitaldistress.su, used to commit tens of thousands of cyber attacks every week across the globe with the aim of shutting down legitimate websites and services.


Following the arrest of a 17-year-old administrator of the service by the Police Service of Northern Ireland, the NCA was able to covertly take over the site. The Agency replaced it with a 'mirror site' which criminals continued to use, unaware that the Agency was collecting their registration details to identify them and take action, both in the UK and overseas with international partners.

Booster services such as digitaldistress.su which allow individuals with limited technical ability to commit cyber offences with ease are an attractive entry-level cybercrime. This operation reflects the success the Agency and law enforcement partners have had disrupting the distributed denial of service for hire market, building on the success of other honeypot operations.

## Sanctioned Members of EvilCorp



# Consuming illegal drugs is increasingly dangerous, with a rising death toll

NATIONAL CRIME AGENCY

# Drugs

Drug use and drug-related deaths continue to impact the UK, with a total annual cost to society of over £20 billion. The harm from drugs is rising, with drug-related deaths in the UK increasing by 15% in 2023. Heroin continues to be associated with the largest number of deaths, followed by cocaine and benzodiazepines. Cocaine-related deaths increased by 30% in England and Wales (from 857 in 2022 to 1,118 in 2023), by 29% in Scotland (from 371 in 2022 to 479 in 2023) and by 6% in Northern Ireland (from 32 in 2022 to 34 in 2023).

The Home Office's Wastewater Analysis programme has estimated the change in consumption of various illicit drug types from 2023-2024. This has been done using samples covering 18% of England's population, taken between January and April 2023 and January and April 2024. These figures only represent the population and time periods captured in this sample, and do not represent England as a whole. Cocaine consumption and ketamine consumption are both estimated to have increased, by 7% and 85% respectively. However, heroin consumption is estimated to have decreased by 11%.

**15%**

increase in **drug related deaths** in the UK.

Source

There is no typical method used by organised crime groups to bring drugs into the UK. The criminal groups and individuals involved can be from any background and area/country, and can impact both their own area and other regions in the country.

Domestically-based organised crime groups have a direct impact within their region of operation through use of violence and intimidation as they seek to maintain status and market share within local drugs markets. Such organised crime groups, though regionally based, will require access to transnational crime networks to import drugs from overseas to the UK and also to launder their criminal proceeds.

Organised crime groups located, or emanating from, overseas can have a disproportionate impact on the

UK as they facilitate multi-tonne shipments of illegal drugs to the UK, establish criminal networks in the UK, and are hard to infiltrate due to high levels of sophistication. Albanian drug organised crime groups, for example, are active in almost all parts of the UK.

Transnational organised crime groups rely on expert skills to coordinate the movement of illicit commodities. They operate within global supply chains, often as part of international networks of drugs traffickers. Groupage loads of commodities (such as multiple consignments of drugs within one load) show that organised crime groups are increasingly willing to collaborate, where it is in their interest; they are constantly innovating and evolving their methodologies to evade detection, for example, diversifying importation methods through at-sea-drop-offs. More than 600kg of cocaine washed-up along the UK coast line was almost certainly due to failed at-sea-drop-off attempts, when criminals dropped loads from sea vessels for intended later collection – a method more frequently being used to attempt cocaine importations.

It is likely demand for cocaine has grown and criminal groups continue to supply at scale. There has been a 53% increase in potential cocaine production at source, along with increased seizures at the UK border, and a rise in deaths involving cocaine. Wholesale cocaine price and purity remains high, however, regional variations are evident across the UK. Cocaine use can have severe cardiovascular, neurological, and psychological effects, and likely exacerbates domestic violence.

The 2022 Taliban narcotics ban has likely contributed to a decline in heroin purity in the UK market. Despite several large-scale seizures in Afghanistan, as well as fewer seizures at the UK border, heroin remains widely available in the UK; however, the wholesale price has increased.

Global synthetic drug markets are rapidly evolving and are a growing concern in the UK. Nitazenes are a group of synthetic opioids with no approved human use. They are increasingly detected mixed with heroin, but also a range of counterfeit pills (such as benzodiazepines and painkillers) to strengthen effects, often without the knowledge of the user. Nitazene-related deaths are gradually rising: based on March 2025 data, there was a 60% increase from the period 01 July to 31 December 2023 (125) to 01 January to 30 June 2024 (200). Another 133 nitazene-related deaths were recorded from 01 July to 31 December 2024, with this number expected to grow as testing is finalised.

At least
**333**
**drug related deaths** involving the presence of **nitazenes** in the UK in 2024.

*i* Source

Xylazine, a non-opioid veterinary tranquilizer not approved for human use, is increasing in prevalence in the UK. It is often combined with other drugs, mostly heroin, to prolong effects. Xylazine has been involved in drug related deaths in the UK. Especially when used in combination with other sedatives, xylazine dangerously lowers the user's level of consciousness, and lowers their heart rate.

Fentanyl is a licensed medicine (when legitimately produced) used for anaesthesia and pain management, and like other opioids, is misused. Fentanyl has re-emerged in some regions of the UK following a dip in recent years, but the threat remains low compared to nitazenes. Since June 2023, there have been 14 deaths related to the misuse of fentanyl, including 11 where nitazenes were also present.

Ketamine is becoming more popular and is much cheaper for users than cocaine. Users frequently mistake it as safer than other drugs, however, it causes significant health harms, both mental and physical. 'Ketamine bladder' describes the severe and painful bladder damage ketamine use causes. The drug brings on a dissociative state, putting the user at risk of physical danger, and has other short- and long-term psychological effects. The number of adults presenting for medical treatment relating to ketamine during 2022-2023 was 2,211, five times greater than 426 in 2014-2015.

Cannabis remains the most widely used illegal drug in the UK, and local cannabis cultivation continues at industrial scale. Cannabis importations are growing since its decriminalisation or legalisation in other countries. Thailand has rapidly emerged as the lead source country of imported cannabis arriving by air passenger and fast parcel and post, overtaking the USA and Canada in 2024. Many air passenger couriers carrying cannabis in on commercial airlines mistakenly believe the risk is low, with 134 air passengers carrying cannabis arrested in 2023 and 745 arrested in 2024.

## Case Study | Dismantling a Large-Scale Class A Drug Conspiracy

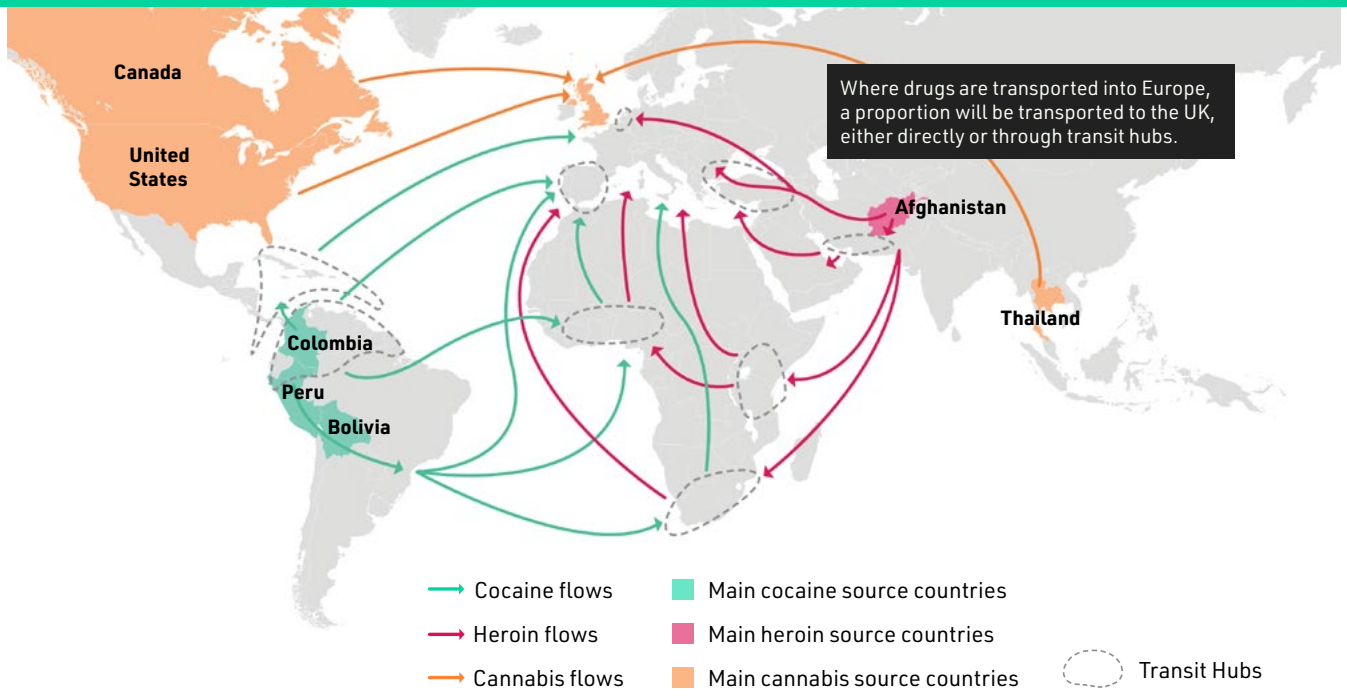
Seven men received combined prison sentences of more than 60 years for a multi-million-pound drug conspiracy, responsible for importing over two tonnes of Class A drugs into the UK with street value of more than £250 million.

The investigation, led by the North West Regional Organised Crime Unit, successfully dismantled the organised crime group which had made multiple trips to collect the drugs from mainland Europe. Using a trailer to conceal the drugs, they used the Eurotunnel to evade detection when returning the UK, before heading to a farm in Deeside, North Wales, where the drugs were split and repackaged for distribution to drugs couriers from across the UK.

However, the North West Regional Organised Crime Unit and officers from North Wales Police were targeting their group, arresting the owner of the farm as he unloaded the drugs, before they arrested his criminal associates.

The final member of the gang, who fled the UK, was subsequently arrested on his return to the UK.

## Cannabis, Cocaine, and Heroin Flows Impacting the UK




Drug flows do not indicate exact routings, but provide an approximation of outgoing and incoming locations.

# Criminals' access to original lethal purpose weapons remains suppressed due to decades of commitment to reduce the threat


NATIONAL CRIME AGENCY

# Firearms

Criminals continue to use firearms mainly to threaten or to maintain their status, rather than discharging them. Where firearms are seen during threats, they are often imitations, and where they are implied, they may not exist, especially when the threats are made on social media. The increased possession and use of imitation firearms to make threats has led to an increase in overall firearms offences, bucking the long-term trend. Most threats are linked to criminal rivalries, such as control of local drugs trades or personal feuds, but firearms are also used as threats in domestic incidents.

In 2024, discharge of firearms mostly involved rival criminal groups or individuals related to the drugs trade, territorial disputes, debt, or personal feuds, as well as in revenge for previous assaults. This results in periodic escalation of violence in local areas, although firearms crime in the UK overall remains amongst the lowest in the world.

**40%**

of firearms offences involve a firearm being **'used as a threat'** as opposed to being fired or used as a blunt instrument.

Source

Discharges involving lethal-barrelled and unknown firearms remain suppressed due to decades of commitment to reduce the threat, with 692 offences recorded by police in England and Wales in the year ending March 2024 (a 15% decrease from 814 recorded in the previous year). The number of individuals killed by firearms in England and Wales has been consistent over the last ten years, according to police recorded crime figures, with an average of 28 fatalities a year. There were 24 fatalities in 2023-2024, a slight decline on 27 in 2022-2023.

Most firearm discharges are in public spaces, such as streets and parks, which increases the risk to members of the public. People who are not connected to criminality are rarely the intended victims of



Quick Links: Home | Overview of SOC | Cross-Cutting Threat Enablers | Child Sexual Abuse | Cyber | Drugs | Firearms | Fraud | Illicit Finance | Modern Slavery and Human Trafficking | Organised Acquisitive Crime | Organised Immigration Crime | Tackling the Threat

firearm discharges, but are on occasion hit by stray bullets or in cross-fire. Isolated tragic incidents are inevitably high profile and lead to a perception of heightened firearms crime in an area.

Most criminals who want a firearm do not have the necessary criminal contacts or money to buy what they desire. This means that they often resort to blank-firing copies of well-known firearms. Although not of as good quality as original lethal purpose firearms, such weapons can be converted and become lethal. Converted blank-firers are now used more than original lethal purpose firearms and are often used with modified blank ammunition. However, the commencement of the new Firearms Act 2023, which introduces an offence to possess component parts of ammunition with intent to manufacture unauthorised complete rounds, will likely reduce criminal use of home-loaded ammunition in the next 18 months.

Criminals get firearms in a range of ways. Although in their unconverted state some blank-firing weapons can be legally bought in the UK, the majority of criminally-used firearms are smuggled in from abroad. Post and parcels remain common methods of importation, and firearms are also imported through ferry routes in small numbers. Items ordered online are sometimes legal in the country they are bought from, but illegal in the UK and are frequently detected at the border. Shotguns stolen from residential premises or private vehicles enter the criminal marketplace but thefts of legally-held firearms remain opportunistic, rather than targeted.

Legally-held firearms are rarely used criminally by the lawful owner. However, in 2024, around one quarter of criminal firearm discharges remained unrelated to criminal rivalries and were predominantly associated with illegal hunting/poaching, the unlawful destruction of pets and other animals, as well as domestic violence incidents, including murder and murder-suicides. Firearms are also used by individuals suffering from mental ill-health episodes both for suicide and to harm others.


Firearms certificate holders and registered firearms dealers are highly unlikely to be involved in SOC, and legally-held firearms and ammunition are not often diverted to the criminal market by complicit certificate holders or dealers. Forged firearms certificates are on rare occasions used to obtain a firearm to inflict serious harm.

Although rarely used in criminal discharges, criminals resort to using privately-manufactured firearms, such as slam-guns or zip-guns, when they cannot source real or converted blank firearms. 3D-printed firearms (or components) are not sought-after weapons by criminals, as they are often perceived as being of poor quality or because they have lower status in comparison to other firearms. In 2024, there were a small number of discharges using improvised slam/zip-guns, and almost certainly none using 3D-printed firearms. It is a realistic possibility that 3D-printed firearms will become more popular as technology improves. Some criminals use stun devices and noxious sprays for protection and intimidation; these are illegal in the UK but freely available in many countries, including those in Europe.

Despite an amnesty relating to four Turkish brands of top-venting-blank-firers in February 2025, and wholesalers' commitment to cease importation, which will reduce the availability of new stock, converted blank-firing weapons will remain prevalent in UK criminality in the next 18 months. Any changes in respect of other currently legal blank-firers is likely to have a delayed impact on their use, due to existing criminal stock levels and patterns of criminal use.

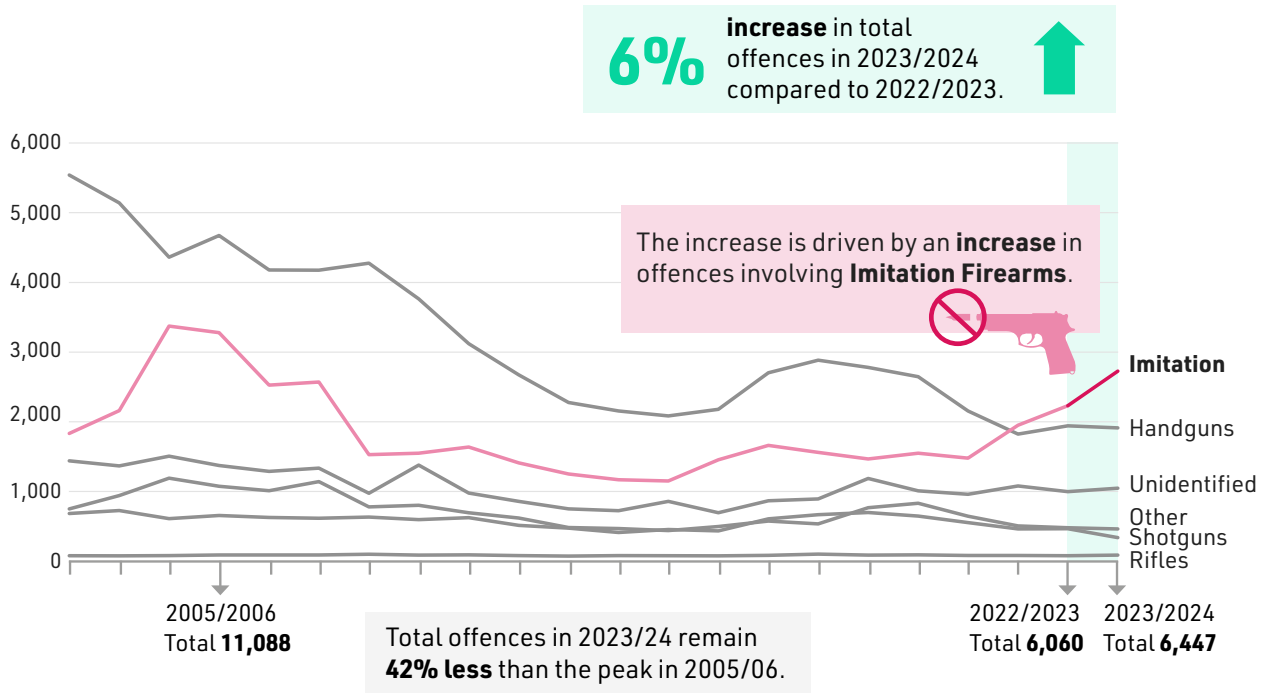
## Case Study | Stopping the Conversion of Blank Firearms

In March 2024, the NCA arrested five people for firearms and other offences following an investigation into the conversion of blank-firing pistols to carry live ammunition, and recovered ten firearms in the process.

The arrests were part of an NCA-led multi-agency response under which UK law enforcement have seized 63 of these firearms. By building a detailed understanding of the legitimate market and supply chain for these weapons, the NCA and UK police forces have arrested and prosecuted several criminals involved in illegally converting and supplying them, and identified the brands of pistol that can be readily converted, to ensure that they are banned from sale to the UK public, significantly reducing their availability to criminals.

Blank-firing weapons are the most common type of firearm seized by law enforcement over the last two years. An amnesty, held in England and Wales throughout February 2025, has enabled members of the public in possession of these devices to dispose of them safely via their local police force to further reduce the risk to the public.

## Increase in Police Recorded Firearm Offences

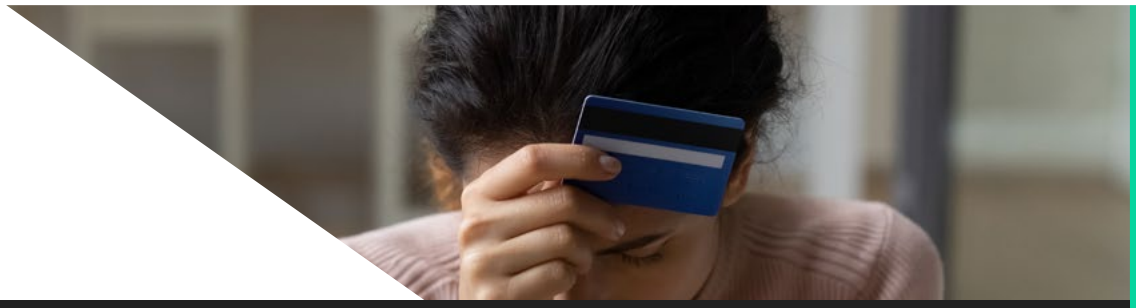



Source: Office for National Statistics, x-axis markers are financial years.



Quick Links: Home | Overview of SOC | Cross-Cutting Threat Enablers | Child Sexual Abuse | Cyber | Drugs | Firearms | Fraud | Illicit Finance | Modern Slavery and Human Trafficking | Organised Acquisitive Crime | Organised Immigration Crime | Tackling the Threat

# It is likely that the fraud threat to UK individuals and businesses increased from 2023, although estimated fraud levels are similar to those last seen in 2019



ADOBE STOCK

# Fraud

It is likely that the fraud threat to UK individuals and businesses has increased from 2023, with estimated fraud levels returning to those last seen in 2019. Fraud remains a significant problem for the UK, and is still the most prevalent crime against individuals in England and Wales, accounting for an estimated 41% of crime reflected in the Crime Survey for England and Wales for the year ending September 2024. There are no official estimates at present for fraud against businesses.

Public sector fraud is also committed by serious and organised criminals, with the UK's tax system in particular a target for fraud offenders. About £3.5 billion of the estimated total tax gap figure of £39.8 billion for the UK during the 2022-2023 period is attributed solely to criminal attacks, down from £4.1 billion and £3.7 billion in 2020-2021 and 2021-2022 respectively.

**Fraud is the most common crime type in England and Wales.**

**41%**

of **all crime in England and Wales** is estimated to be Fraud.

*i* Source

Only an estimated 14% of frauds against individuals are reported to Action Fraud or the police. The majority of unreported frauds are likely high in volume but low in value; it is likely under-reporting happens for a variety of reasons. In cases where frauds were attempted but victims have not suffered a financial loss, they are less likely to report. In cases where victims have suffered a financial loss, these reasons include: victims receiving full refunds from their banks and therefore considering it unnecessary to report the incident through the law enforcement mechanism, victim perception that Action Fraud or police could not do anything, and victims having limited awareness of the reporting mechanism.

The range of fraud datasets indicate an overall increase in reporting this year, and estimates of fraud incidents recorded by the Crime Survey for England and Wales show an increase of 19% to 3.9 million

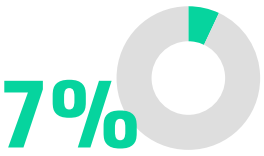
incidents in the year ending September 2024. The priority frauds impacting the UK remain on the same long-term trajectories in Action Fraud reporting. Investment fraud and romance fraud reports are at the high levels seen during the pandemic, with courier fraud and payment diversion fraud still below pre-pandemic levels, although victim harm from both remains high.

Many frauds impacting UK victims have an overseas element. The cyber-enabled nature of many frauds and the methods used to launder the criminal proceeds often involve multiple jurisdictions. In the majority of cases, adult victims of fraud have no knowledge of those who target them: in year ending March 2023 only 9% of adult victims were able to say something about the offenders.

Criminals continue to search for innovative ways to reduce the effectiveness of countermeasures, including fraudulent schemes designed to add stolen card details to digital wallets on criminally-controlled mobile phones through intercepting one-time passcodes, either via social engineering or malware. Criminals are then able to make multiple transactions rather than single transactions, which may not have been the case previously. This is likely to be one of the main factors in the rise of card-not-present frauds this year.

It is highly likely that continued cost of living pressures has led to increases in fraud against businesses by individual customers, such as first party fraud including return and refund frauds. Criminals offer 'refunds as a service', where consumers hire them to claim fraudulent refunds on their behalf in exchange for a share of the returns.

It is estimated that 67% of fraud reported in the UK is cyber-enabled, with authorised push payment frauds continuing to be driven by the abuse of online platforms. Social media platforms are a key facilitator of authorised push payments frauds, particularly in online shopping, ticket, and investment frauds, where initial contact is enabled through adverts posted on social media. A rising threat this year has been the use of social media hacking to enable ticket fraud, which has contributed to the continuing rise of ticket fraud in the UK.



**7%**

**This is approximately 3.2 million people.**

of **people aged 16 and over** in England and Wales are estimated to have been a **victim of fraud**.

*i* Source

Criminals continue to adopt generative artificial intelligence to enhance the sophistication of fraud attacks against individuals and businesses, although they are currently used to enhance existing threats rather than create entirely new ones. The use of deepfake videos and voice cloning has been used to enable CEO frauds against large businesses. In February 2024, generative artificial intelligence was used in a CEO fraud to create deepfake recreations of company employees at a virtual meeting to trick a finance worker to transfer £20 million into a criminally-controlled account.

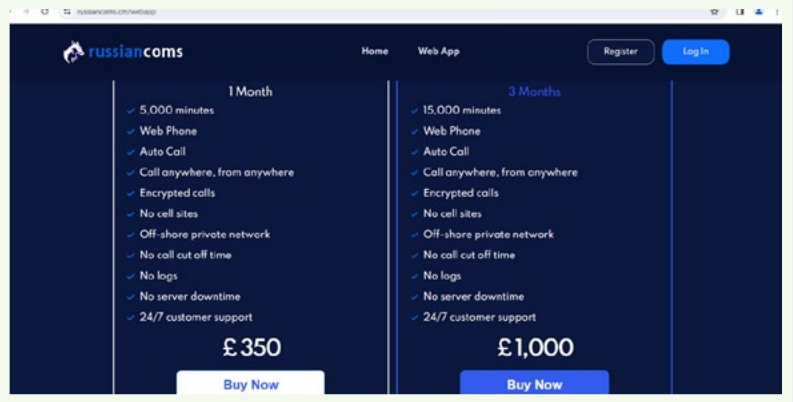
Phishing attacks remain prevalent, with criminals still using this method and compromised data to take control of accounts directly or to use in other frauds. Phishing tools are being developed with more sophisticated technical features to bypass security measures and counter the increased public awareness and understanding of fraud risk. These include using encrypted messaging protocols such as iMessage and Rich Communication Services instead of SMS to avoid anti-phishing systems.

Fraud enabling products are also used by criminals in an attempt to mitigate the effectiveness of security measures implemented by banks and online platforms, increasing the accessibility of fraud. Products and tools available include ID generation kits, phishing kits, spoofing software, and tutorials and guides. In 2024, the NCA shut down a fraud enabling platform used by criminals to defraud victims both in the UK and overseas. The calling line identification spoofing service 'Russian Coms' allowed criminals to hide their identity by appearing to call from pre-selected numbers, most commonly of financial institutions and telecommunications companies. This enabled them to gain the trust of victims before stealing their money

and personal details. Between 2021 and 2024, over 1.3 million calls were made by Russian Coms users to 500,000 unique UK phone numbers.

## Case Study | Takedown of a Major Fraud Platform

In March 2024, the NCA shut down the 'Russian Coms' platform responsible for over 1.3 million scam calls to 500,000 UK phone numbers, and thought to be behind tens of millions of pounds in financial losses worldwide.

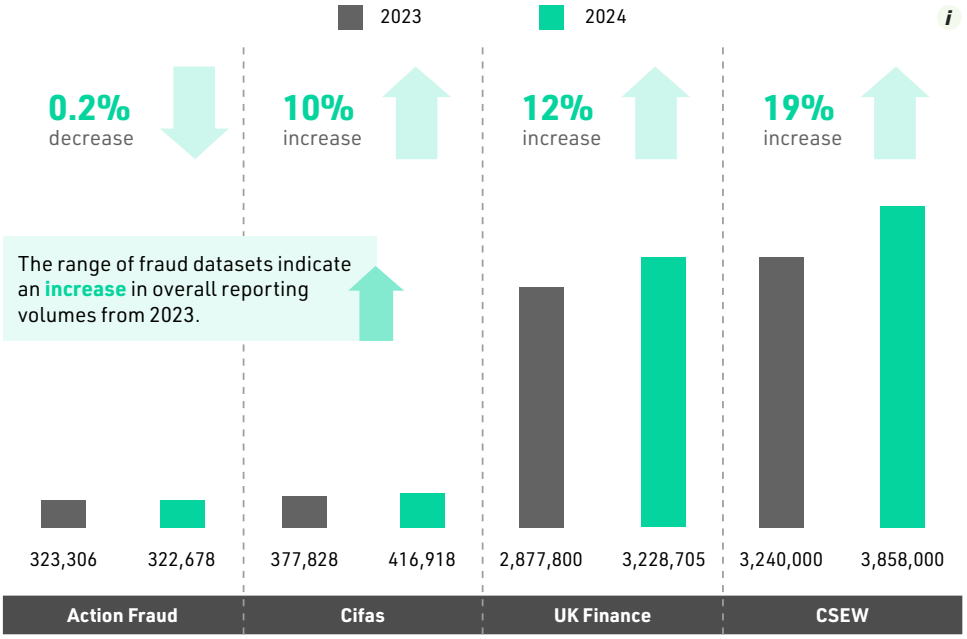


NATIONAL CRIME AGENCY

The platform provided a criminal service which allowed fraudsters to hide their identities when contacting victims. By appearing to be calling from pre-selected numbers, most commonly financial institutions, telecommunications companies, and law enforcement agencies they could gain the trust of victims before stealing their personal details and their money.

In March 2024, following months of intelligence gathering and painstaking investigative work, the NCA took down the platform and arrested two men in London, believed to be the platform's developers and administrators. A further collaborator in the fraud was later arrested in April 2024.

## Increase in Overall Fraud Reporting Volumes




Source: Action Fraud, Cifas, Crime Survey for England and Wales (CSEW), and UK Finance. 01 October 2022 to 30 September 2023 (2023) and 01 October 2023 to 30 September 2024 (2024). Percentages greater than 1% are rounded to the nearest whole number.

# The UK remains vulnerable to money laundering, in particular from illicit proceeds generated overseas


ADOBE STOCK

# Illicit Finance

Most SOC in the UK is conducted to generate profit. Crimes such as illicit drug trafficking and fraud generate funds which can be moved, hidden, and used to fund further crime. Money laundering amplifies the harm from these crimes by funding further criminality and undermining confidence in our financial and professional services sectors.

Money laundering networks use a combination of methods to move criminal proceeds and conceal the source of funds. Networks will make use of cash, cryptocurrencies, banks and non-bank payment service providers, along with corporate structures and professional enablers, in the UK and overseas, so they can offer their services to a range of customers.

It is highly likely that over £12 billion of criminal cash is generated each year in the UK. It is a realistic possibility that over £100 billion is laundered through and within the UK or UK-registered corporate structures each year.

UK corporate structures continue to enable money laundering due to vulnerabilities in their creation and oversight. Potential indicators of money laundering via corporate structure misuse include multiple companies being registered at the same residential address and the creation of large numbers of dormant companies. While it is too early to see impact from the phasing in of new powers for Companies House, the introduction of ID Verification to register UK corporate structures from autumn 2025 will likely displace some criminals from using UK corporate structures. After ID Verification was introduced in Ireland in June 2023, there was an increase in the amount of Northern Irish companies being registered with suspicious characteristics.

**84** **arrests**

**£20 Million** in **cash and crypto seized**

in Operation DESTABILISE between November 2021 and December 2024.

*i* Source



Quick Links: Home | Overview of SOC | Cross-Cutting Threat Enablers | Child Sexual Abuse | Cyber | Drugs | Firearms | Fraud | Illicit Finance | Modern Slavery and Human Trafficking | Organised Acquisitive Crime | Organised Immigration Crime | Tackling the Threat

It is likely that over £10 billion a year is moved through trade based money laundering schemes impacting on the UK each year. Research by Europol found that 86% of the European Union's most threatening criminal networks exploit legal business structures to disguise their activities, facilitate money laundering, and expand their operations while evading law enforcement.

Accounts at UK banks and non-bank payment service providers continue to be exploited by money laundering networks, including for 'money mule' activity. Cash intensive businesses, such as car washes, nail bars, and barber shops are used to introduce criminal cash into the financial sector often via the everyday banking facility at the Post Office. Money service businesses also continue to feature in investigations.

Professional enablers continue to be used to conceal and move criminal assets. They have mainly been associated with banking, payment service providers, accountancy services, estate agents, legal services, wealth management, and trust and company service providers. Some professional enablers specialise in moving value through cryptocurrencies, such as the networks investigated under NCA Operation DESTABILISE, as well as over-the-counter brokers who facilitate high volumes of cryptocurrency trades.

The use of cryptocurrencies to launder money is widely established. Cryptocurrencies are used to launder the proceeds of fraud and cybercrime as well as to pay for drug importations. The most commonly seen cryptocurrencies in laundering are Bitcoin and Tether. Decentralised financial platforms and privacy coins such as Monero are being used in money laundering, but the scale of their use is likely significantly less than through traditional financial systems, or commonly used cryptocurrencies.

**88%**

of cryptoasset firms who **applied to the FCA for registration in 2024 were unsuccessful** due to not meeting the standard.

*i* Source

High-value goods also feature in investigations and are used to transfer value, for example, through diamonds and also for lifestyle purchases or conspicuous designer goods.

Money mules continue to be used to introduce the proceeds of crime into the financial system and most proceeds of organised fraud activity use mule accounts to extract and launder funds. Money mules are often identified and recruited by mule recruiters, who also manage the mules and direct their activities.

Money laundering through the capital markets, such as buying and selling of bonds, currencies, stocks, and other financial assets continues to evolve. It offers a route for criminals to move and disguise the audit trail of money through the use of complex financial transactions.

Money laundering networks operating in the UK are usually controlled from overseas. International controller networks work together using informal value transfer systems. International controller networks are now known to offer a parallel banking facility for SOC, rather than just transferring value, providing regular account balances and monthly statements.

International controller networks use a variety of methods to provide a professional money laundering service to criminals. This includes exchanging cash for cryptocurrencies on behalf of global criminal networks. This practice links UK generated proceeds of crime to transnational cybercriminals who have access to large amounts of cryptocurrencies.

It is likely that the already high threat from Chinese-speaking money laundering networks in the UK continues to grow. As well as moving cash for UK criminals they help UK-based Chinese nationals to evade Chinese currency controls which enables them to invest in the UK. This increase has also been seen in countries in Europe and other countries in the West. This threat has historically been driven by the demand

for British pounds in the UK from Chinese students and investors, and the competitive and rapid service the networks are able to offer.

The scale of activity by the Russian-speaking money laundering networks investigated under Operation DESTABILISE is highly likely greater than previously reported. They provide cash to cryptocurrency conversions in the UK and overseas with their combined global reach extending to over 30 countries. As well as laundering funds for transnational organised crime groups they have enabled Russian elites and entities to evade UK financial sanctions, and have funded Russian espionage operations. The NCA-led international investigation has exposed and disrupted their activity through arrests, convictions and seizures of criminal cash and cryptocurrency. The US Office of Foreign Asset Control has also issued sanctions against key members of these networks and businesses that are linked to them.

It is highly likely that sanctions, legislative reforms, and reduced access to investment opportunities and professional enabler services have made the UK a more challenging environment for those individuals involved in Russian illicit finance, in particular elites. Some assets and enablers have been relocated away from the UK. Some individuals designated under UK Russian sanctions have likely developed their methods to move and access funds and circumvent sanctions. These include using countries that have not adopted sanctions against Russia and non-sanctioned family members and staff to control their assets and move funds on their behalf.

The energy, extractives, construction, refined precious metals, defence, public procurement (including transport), aviation, and finance sectors are highly likely to be most at risk from international bribery and corruption. The main method used to launder the proceeds of corruption continues to be through offshore corporate entities and trusts. Professional enablers providing company formation, accounting, legal, and real estate advisory services facilitate money laundering on behalf of corrupt politically exposed persons. 2024 saw the NCA International Corruption Unit's first foreign bribery conviction involving the former Chief of Staff to the President of Madagascar and her associate who sought bribes from a UK-based supplier of gemstones.

Producers of counterfeit currency continue to attempt to improve the quality of counterfeit notes, with incremental improvements since 2021. Social media platforms are now one of the key methods used to sell counterfeit currency.

Market abuse damages the integrity of the UK financial markets. It is likely that the most serious market abuse harm is from insider trading organised crime groups who recruit information sources employed across the financial services sector. Misconduct in the markets presents a threat to the integrity of the UK financial system as it erodes trust and confidence. Confidence in the UK financial markets is essential to maintaining growth and the UK's competitive position in global financial markets.

## Case Study | Combatting the Threat from Money Muling

The National Economic Crime Centre, working alongside City of London Police, led the UK response to a cross-Europe campaign to combat the threat from money muling.

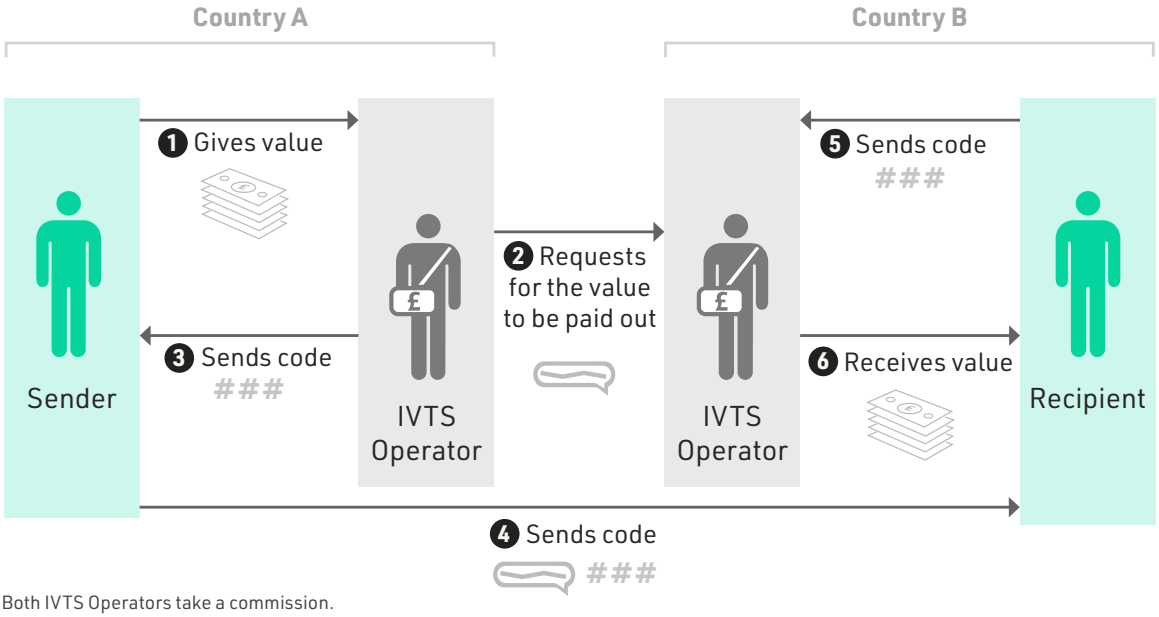
Money mules act on behalf of criminals to move the proceeds of crime, hiding their illicit funds and helping them to realise the benefits of their criminal activity.

Through November 2024, 13 partners from the police and Trading Standards participated in an intensification, securing 76 arrests, £818,000 in cash and cryptocurrency, and issuing 153 cease and desist notices to those at risk of offending.

These results were possible thanks to substantial support from the Cyber Defence Alliance, and the tireless work of hundreds of officers across the country. They also represent a significant increase on our previous intensification, removing significant criminal funds from money mule networks.

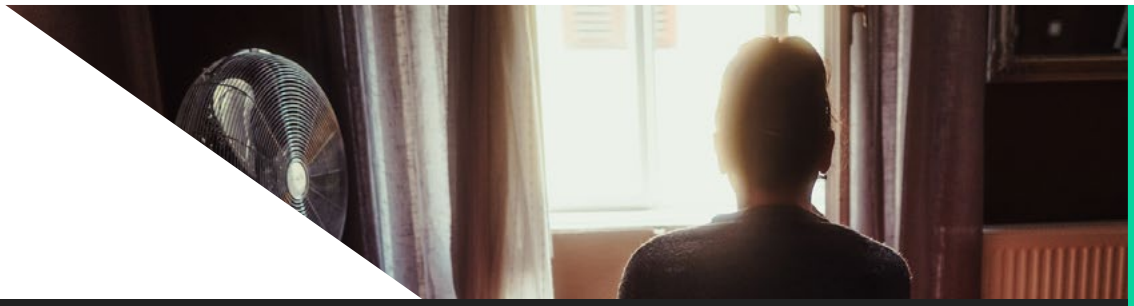
## Informal Value Transfer System | A Simplified Transaction

Informal value transfer system (IVTS) is a mechanism that facilitates the transfer of the value of money from one location to another, without the need to physically transfer the money itself.




Both IVTS Operators take a commission.

## Modern slavery and human trafficking is primarily motivated by profit, with consumer demand for the services provided by victims creating opportunities for exploitation



GETTY IMAGES

# Modern Slavery and Human Trafficking

Modern slavery relates to exploitation of children and adults in slavery, servitude, or forced or compulsory labour. Human trafficking is the recruitment, movement, harbouring, or receiving of children, and of adults through coercion, deception, or force, for the purposes of exploitation.

The National Referral Mechanism is a framework to identify potential victims of modern slavery and human trafficking and ensure they receive the appropriate support. The National Referral Mechanism provides a snapshot of modern slavery and human trafficking, but as it is dependent on the identification of a potential victim by a suitable authority or support service, and, for adult potential victims, consent to referral, it does not provide a full or accurate representation of the threat. The total number of referrals is a subset of potential victims, rather than confirmed cases of modern slavery and human trafficking.

**54%**

of referrals for exploitation wholly in the UK were for **UK nationals**; 78.5% of which involved exploitation in criminal activity.

*i* Source

A total of 8,156 referrals were made to the National Referral Mechanism reporting exploitation entirely within the UK between October 2023 and September 2024. A total of 4,415 referrals (54%) were for UK nationals, and in 58% (4,697 of 8,156) of referrals, the potential victim reported exploitation as a child.

While there is no evidence of substantial change in the overall nature and scale of modern slavery and human trafficking in the UK in 2024, it is almost certain that there has been demographic change within the threat, with shifts in migration patterns a key factor driving change. Although it is almost certain that the vast majority of migrants entering the UK to work having been recruited overseas are aware of the nature of the work in which they will be employed, with terms and conditions (including costs and debts associated

to travel and facilitation) agreed before travel, migrants with no or limited right to work in the UK are vulnerable to their status being used as a means of recruitment into or control within exploitation.

Adult victims of modern slavery and human trafficking are typically vulnerable due to economic factors, such as debt and unemployment. In some cases, victims are also vulnerable through factors such as homelessness, learning difficulties or disabilities, mental ill-health, or substance dependency or misuse. These vulnerabilities can also apply to child victims of modern slavery and human trafficking, who are also often vulnerable through their age, and factors such as family breakdown, persistent absence from school, and social isolation from peers.

Modern slavery and human trafficking manifests in four key types of exploitation in the UK: domestic servitude; exploitation in criminal activity; labour exploitation; and sexual exploitation. Although victims of modern slavery and human trafficking are of both sexes, it is a highly gendered crime, with male victims most often exploited for their labour and in criminal activity, and female victims the majority in both sexual exploitation and domestic servitude.

Exploitation in criminal activity is the form of modern slavery and human trafficking most commonly reported to the National Referral Mechanism. Exploitation in criminal activity occurs when victims are coerced, forced, or otherwise compelled to commit crime, often in drug offences such as cannabis cultivation or distribution via county lines. Although adults are exploited in criminal activity, organised crime groups engaged in drug distribution often recruit children to move and sell drugs, often due to perceptions that they are less likely to be arrested or are easier to control and manipulate. Victims of exploitation in criminal activity are often at risk of violence from both their exploiters and rival criminal groups and gangs.

Labour exploitation occurs when a person is made to work for little or no pay, or has access to their wages controlled or limited by another person. Sectors in which work is often informal or short-term, such as agriculture, beauty services, construction, food processing and preparation, and hand car washes, are particularly vulnerable to labour exploitation. Other criminal and regulatory offences, such as environmental offences and health and safety violations, are common in businesses that deliberately exploit people for their labour.

**79%**

of referrals of **UK nationals** involve the potential victim reporting having been exploited when **under 18**.

*i* Source

Sexual exploitation takes place both within the commercial sexual services marketplace, and within organised crime groups and gangs engaged in other criminal activity, particularly county lines drug supply. Victims of sexual exploitation are typically women and girls, many of whom endure long-term psychological distress as a result of their exploitation, in addition to the physical harms from sexual and sometimes physical abuse.

Domestic servitude is typically committed by individuals or family units, rather than organised crime groups, and overwhelmingly takes place in private households, making it challenging to prevent and detect. Victims can be exploited by employers, for whom they often work both in the UK and overseas, or by their own partners or family members. Offenders typically exert high levels of control over victims' movement and finances, sometimes confining them to the home entirely, and in some cases use physical and sexual violence against victims.

## Case Study | Multi-Agency Activity Targeting the Adult Social Care Sector

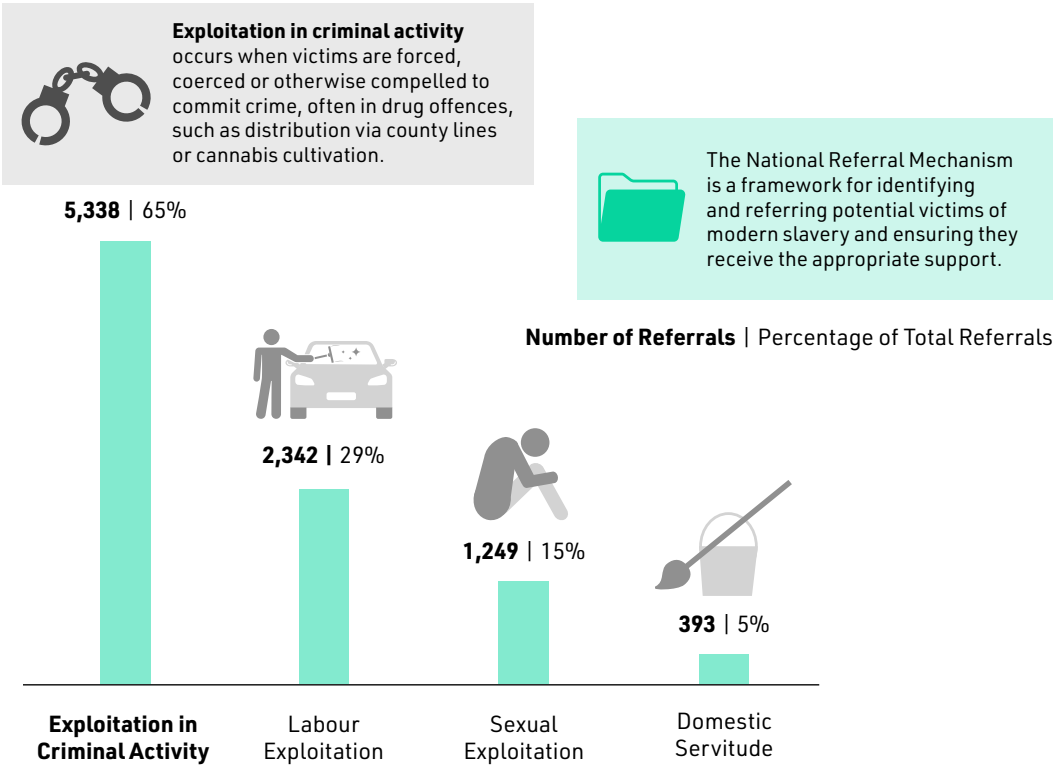
In March 2024, the NCA led multi-agency activity across the UK targeting modern slavery and human trafficking in the adult social care sector, following an increase in the number of allegations of modern slavery and human trafficking and other offences in the sector.

Thirty-five police forces across England and Wales participated, along with labour market enforcement bodies, care inspectorates, immigration authorities, and local authorities. Between them they visited over 320 premises leading to at least 23 new investigations into complex criminality.

Despite the increase in allegations, labour exploitation was found to be less common in the care sector than expected; helping to improve our understanding of the threat and the consistency of safeguarding responses across the UK.

This collaborative project has strengthened how the UK responds to modern slavery and human trafficking: driving policy reform and operational responses across government; improving information sharing between law enforcement and labour market enforcement bodies; and ensuring the effective use of resources, powers, and tools against the modern slavery and human trafficking, labour market abuses, and illegal migration threats.

## Types of Exploitation Reported in the UK




Source: National Referral Mechanism. Percentages rounded to the nearest whole number.
Percentages add up to more than 100 as one referral can involve multiple exploitation types.

# High levels of domestic and international demand for second-hand and cheaper products continues to be a key driver

ADOBE STOCK

# Organised Acquisitive Crime

*All content for this threat is provided by Opal, who are the national intelligence unit for organised acquisitive crime.*

Organised acquisitive crime focuses on high-harm and cross-border burglary, metal and infrastructure crime, plant and agricultural thefts, retail crime, robbery, and vehicle crime amongst other crime types. Offenders involved in organised acquisitive crime often have links to wider SOC networks.

It is likely there was no substantial change in the threat from organised acquisitive crime in 2024. Reported organised acquisitive crime offences were steady overall, with some degree of fluctuation across specific crime areas.

**19%**

of police reported retail crime offences had recorded **elements of organisation**.

Source

High domestic and international demand for second-hand and cheaper products continues to be a key driver of organised acquisitive crime. It is likely that elevated international supply chain pressures continue to drive organised acquisitive crime offending, particularly vehicle, and agricultural and construction equipment thefts; however, there has been no substantial change to key organised acquisitive crime drivers, namely commodity prices, economic and geopolitical instability, and increased cost of living.

International demand for vehicles and parts remains high and is likely to be driving an increase in stolen vehicles. Theft of motor vehicle offences increased by 6% in the period from October 2023 to September 2024, in comparison to October 2022 to September 2023. It is highly likely that international export will continue to be used by organised crime groups as a primary method of disposal for stolen vehicles.

Luxury and high-performance vehicles continue to be key targets for organised acquisitive crime offenders, although increased security measures and target hardening by manufacturers has made it more difficult to exploit vulnerabilities in keyless access and ignition systems. Offenders are likely to evolve their tactics to overcome these limitations.

Offenders are highly likely to be engaging in polycriminality using organised acquisitive crime as a method to generate funds or to enable wider organised crime, for example, stolen vehicles used to traffic illicit commodities such as drugs.

Domestic organised crime groups continue to target solar farms, primarily for earthing cable, which accounted for 43% of all solar farm thefts between January 2022 and September 2024. It is likely that earthing cable is stolen for its scrap value. Theft from solar farms caused an estimated total loss of £7.1 million in this period.

It is likely that international and UK-based organised crime groups continue to work together to steal and export agricultural and construction machinery from the UK to Eastern Europe and Cyprus. Recoveries of stolen plant and agricultural equipment have occurred in multiple locations across the UK and Europe, including Romania and Poland. It is highly likely that stolen property will continue to be exported to Eastern Europe over the next 12 months.

Although overall personal robbery offences have declined, it is highly likely that mobile phone thefts continue to be a key threat, particularly due to the significant availability of devices, including new models following release. Between January and August 2024, robbery of mobile phones accounted for 37% of personal robbery offences. It is likely that devices are disposed of overseas to China, Dubai, Algeria, Morocco, Romania, and Bulgaria. An emerging tactic in some areas of the UK is for offenders to access data contained within apps on stolen mobile phones in order to commit additional offences, such as theft from bank accounts.

**37%**

of personal robbery offences involved the **targeting of mobile phones**.

*i* Source

Family gold burglary incidents increased by 30% between October 2023 and September 2024 compared to the same period in the previous year. Previously, the volume of burglaries has had a strong correlation to the market value for gold which is at the highest recorded level for five years; however, there was no correlation between the monthly volume of offences and gold value.

It is likely that organised retail crime levels stabilised, even though overall retail crime continued to increase, driven mainly by an upturn in shop theft. There has been an increase in the proportion of retail crime offences provided by industry partners in which there was an element of organisation (12% of all offences between October 2023 and September 2024, compared to 9% in January to December 2023). Of offences recorded by police between October 2023 and September 2024, 19% included an element of organisation.

The stabilisation of organised retail crime is likely due to law enforcement prioritisation and operational activity, and greater partnership working. In 2024, operational activity conducted by Opal resulted in the disruption of 27 organised crime groups and one high-harm individual. This overall offending caused over £4 million worth of loss, demonstrating the scale and impact of this activity.

A significant proportion (41%) of organised retail crime groups and high-harm individuals identified by Opal have targeted supermarkets in order to commit organised shop theft offences. Health and beauty products, alcohol, and mobile phones are key items targeted by these groups.

## Case Study | Police Crackdown on Organised Vehicle Crime

A nationwide, policing-led operation against organised vehicle crime resulted in 190 arrests and the recovery of more than 300 stolen vehicles with an estimated total value of more than £4 million, including high-end luxury cars, lorries, and motorcycles.

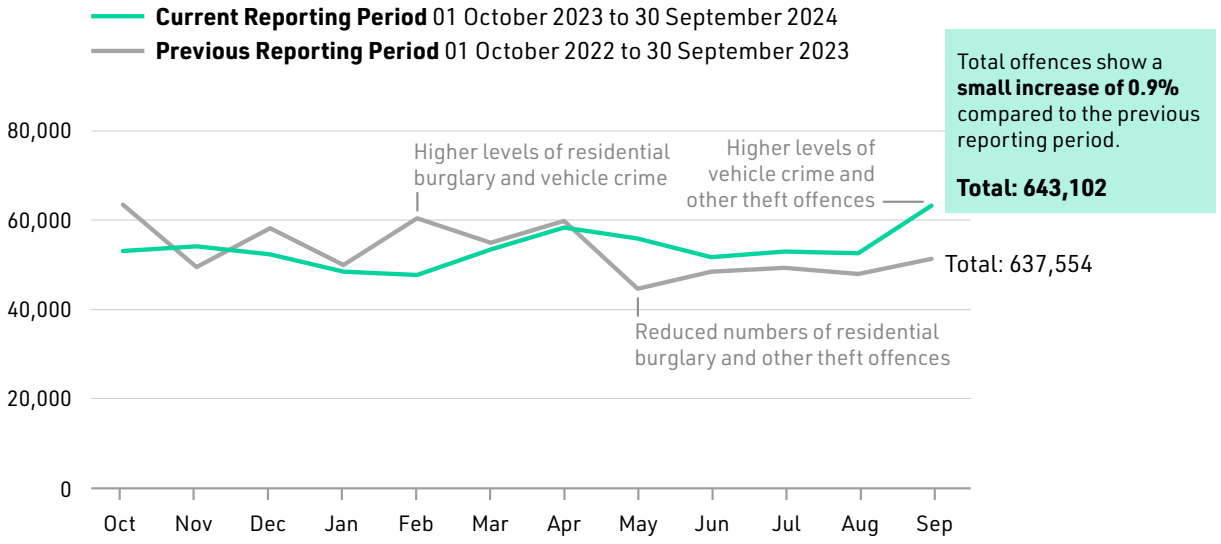
The operation lasted from 16 to 22 September 2024 and was coordinated by Opal, the national intelligence unit for organised acquisitive crime. It included activity at nine ports to locate vehicles and vehicle parts stolen in the UK, destined for overseas markets.

Across the country, police forces conducted multiple search warrants, locating and closing down a number of 'chop shops', which break stolen vehicles into parts which are more easily sold and moved, as well as visiting scrap metal and motor salvage businesses to offer relevant guidance.

Police forces also engaged with local communities to offer crime prevention advice to the public on keeping their vehicles safe.

## Total Offences Remain Relatively Stable

Whilst monthly totals fluctuate, these fluctuations resulted in a minimal change between the annual totals for the two reporting periods.




Source: Police National Database. Metropolitan Police Service data excluded, due to a pause on Metropolitan Police Service uploading data to PND until May 2025. Therefore, 2023 data in this graphic differs to that reported previously.

## There has been a significant increase in migrant fatalities as organised criminals seek to maximise profits from small boat crossings

GETTY IMAGES

# Organised Immigration Crime

Small boats continue to be the most detected method of irregular entry into the UK, with 36,816 arrivals in 2024, an increase of 25% in comparison to 2023 (29,437), but 19% lower than 2022 (45,755). This increase in migrant arrivals has highly likely been driven by increased opportunity (in particular migrant demand), enabled by more favourable crossing conditions in the latter part of the year and elevated organised crime group intent. The latter is evidenced by organised crime groups increasingly using more dangerous tactics in both the small boat and clandestine methods of entry; it is likely that this in part as a response law enforcement disruption to supply chains and a desire to optimise profits.

Afghan (5,919), Syrian (4,630), and Iranian (4,158) nationals were the most common nationalities arriving on small boats in 2024, with substantial increases in the number of Vietnamese (3,602, up from 1,306), Eritrean (3,380, up from 2,666), and Sudanese (2,695, up from 1,658) arrivals compared with 2023.

It is highly likely that the increase in migrant fatalities from 12 in 2023 to 78 in 2024 has been primarily driven by storming of boats and overcrowding, which has exacerbated the impact of unsafe small boats and equipment, reflecting an overall increase in the level of harm caused by the organised immigration crime threat in 2024 compared to 2023.

**1.6%**

**increase** in detections of migrants in the UK who have entered irregularly **via clandestine entry methods**.

*i* Source

It is highly likely that organised crime groups have increased the number of migrants on each boat, in part to maintain profit margins in the face of higher costs for purchasing and transporting small boat equipment in 2024. The average number of migrants per boat has increased from 49 in 2023, to 53 in 2024. On 30 October 2024, a

small boat carrying 98 migrants reached the UK, the highest number recorded as having successfully made the crossing. Costs incurred by organised crime groups for delivery of boats and engines to northern France have risen substantially, likely in part as a result of law enforcement seizures. Organised crime groups are also likely to be choosing to reduce costs by providing increasingly poor quality safety equipment, if any.

Small boats remain, on average, the least expensive form of facilitated irregular entry into the UK by a considerable margin. Costs paid by migrants differ significantly by nationality, but many paying migrants are unlikely to be able to pay more, so organised crime groups are likely judging that they can optimise profits by keeping small boat crossing prices stable. Some migrants secure free passage by piloting the boat and there are increasing reports of migrants storming boats, contributing to overcrowding.

Small boat equipment is typically transported to the French coast by vans or cars from Germany, Belgium, and the Netherlands. Germany is an important transit point for storage. Small boat equipment moved from Turkey, including material manufactured in China, is transported onwards into Europe.

In 2024, there was an overall 1.6% increase in detections of irregular migrants arriving clandestinely. For example, in the back of lorries, at UK ports (326), or in country, where they are believed to have entered the UK clandestinely 72 hours prior to detection (3,138), totalling 3,464 (up from 3,408 in 2023). Despite this increase, clandestine detections have been in year-on-year decline since 2019 (9,201), reflecting the shift towards small boats. The most commonly detected nationalities entering clandestinely in 2024 were Sudanese (758), Eritreans (509), and Iranians (413). These figures do not include detections at juxtaposed controls in Europe.

It is likely that some organised crime groups involved in the clandestine entry method of organised immigration crime conduct both inbound and outbound facilitation. It is likely that increased opportunity for revenue is a motive, and it is highly likely that the contacts (such as HGV drivers), and concealment techniques useful in inbound facilitation are also useful for outbound facilitation.

It is almost certain that the true scale of organised immigration crime is higher than detection figures indicate for entry methods other than small boats. The scale of difference varies by method, depending on factors such as limited law enforcement resource to cover the entirety of the organised immigration crime threat, limitations in passenger data on certain routes, and, in some modes, the use of false documentation to bypass security measures.

It is highly likely that efforts to tighten student and skilled worker visa routes has led to increased intention to abuse visitor and transit visas by both organised crime groups offering end-to-end services and migrants self-facilitating.

It is likely that organised immigration crime groups have improved their knowledge of the UK visa system to support migrants, from initial application to settlement within the UK. This is evidenced by increasing numbers of sponsorship licenses enabling fraudulent sponsorship for migrants.

**94%**

of the advertising for OIC-related services on online platforms was on **Facebook, TikTok, Instagram, and Telegram**.

*i* Source

Opportunities offered by social media and end-to-end encrypted platforms continue to be exploited at all stages of organised immigration crime. Organised crime groups use social media platforms, such as Facebook, TikTok, and Instagram, to advertise smuggling services, false documents, and assistance with fraudulent visa applications. Once contact is established, migrants are often quickly directed to end-to-end encrypted or private messaging platforms, such as WhatsApp and Telegram, whilst

end-to-end encrypted platforms are also used to enable communication between organised crime group members.

It remains challenging to accurately identify the true scale of online organised immigration crime related content; however, online enablers remain central to the organised immigration crime business model and it is highly unlikely that organised crime groups' ability to use online enablers has significantly changed over the last year. Organised crime groups continue to exploit platform embedded features to reach wider audiences and avoid moderation.

## Case Study | Targeting Organised Crime Groups at Every Step

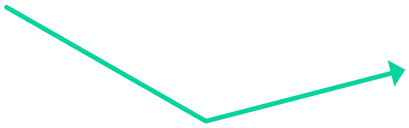
The NCA targets and disrupts organised crime groups at every step of the smuggling route, in source countries, in transit countries, near the UK border in France and Belgium, and those operating inside the UK itself.

This includes the conviction of an Iranian national, known to be responsible for three crossings of Kurdish migrants in November and December 2023, and likely many more. He was sentenced to 17 years imprisonment following the NCA's investigation.

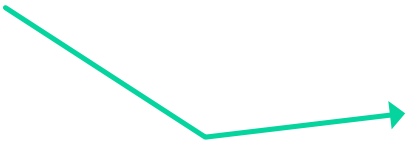
The use of social media to advertise his services was key to their success. Using multiple social media accounts, he posted phone numbers and videos of migrants he had successfully smuggled thanking him for his help as endorsements. One such video showed a group of men on a boat to Italy praising him. Whilst another, filmed in Iraq in 2021, showed him at a party with musicians singing a song celebrating him as 'the best smuggler', while he threw cash at them and fired a gun in the air in celebration.

But back in the UK, NCA officers were able to record his conversations with other smugglers where he discussed the movement of migrants, locations and successful crossings. This was key evidence that led to his arrest, and ultimately his conviction.

# Increasing Harm within the Small Boats Method of Entry



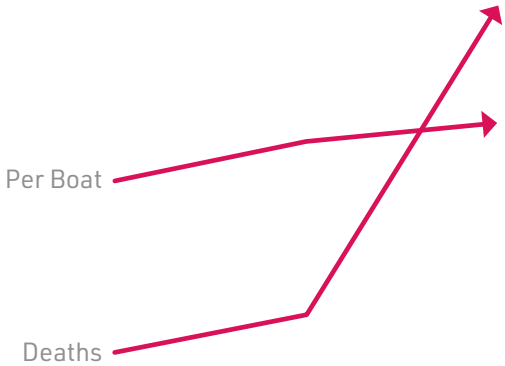
| Arrivals | | |
|---|---|---|
| 2022 | 2023 | 2024 |
| 45,755 | 29,437 | 36,816 |



| Events | | |
|---|---|---|
| 2022 | 2023 | 2024 |
| 1,110 | 602 | 695 |

An event refers to a small boat crossing that has entered UK waters.

Harm is increasing over time, as evidenced by the **rising use of dangerous tactics** resulting in increased migrant fatalities.




| Migrants Per Small Boat | | |
|---|---|---|
| 2022 | 2023 | 2024 |
| 41 | 49 | 53 |

| Migrant Deaths from Small Boats* | | |
|---|---|---|
| 2022 | 2023 | 2024 |
| 4 | 12 | 78 |

**Scale** | **Harm**

*Attributing an exact figure to small boats fatalities is challenging due to incomplete information, particularly in relation to investigations where bodies are discovered a period time after events have occurred and retrospectively attributed to specific events. As a result, these figures may be subject to retrospective change.

Source: Home Office.

## The NCA leads the UK's fight to cut serious and organised crime, protecting the public by targeting and pursuing those criminals who pose the greatest risk to the UK


NATIONAL CRIME AGENCY

# Tackling the Threat

Every day the NCA, policing, and other law enforcement agencies work to protect the public from the SOC threats set out in the National Strategic Assessment.

We do this through pursuing offenders, disrupting their criminal activities, and bringing them to justice; acting to prevent and divert would-be offenders from engaging in SOC; protecting individuals, organisations and systems so that they are less likely to become victims; and preparing for when crime occurs to minimise its impact and reduce the likelihood of further crime.

The 2024 case studies below highlight a small number of operational successes from across the UK. There are many others. And they could not be achieved without the collaborative work of the wider system of partners who work together, dedicated to tackling SOC.

**The SOC System**

Protecting the public from SOC relies on a system of organisations - the SOC System. It is made up of over 75 organisations including law enforcement and criminal justice bodies, the UK intelligence community, HM Government departments, local authorities, regulatory and professional bodies, and overseas law enforcement agencies; working in partnership with both the academic, private, and third sectors.

## Our Response to the Threat

### Protecting the Public at Home

**Disrupting the Importation of Heroin into the UK**

Under Operation SOLON, the Tarian Regional Organised Crime Unit, made up of officers from South Wales, Gwent and Dyfed-Powys Police, led the disruption of a UK-wide organised crime group responsible for trafficking more than 60kg of heroin, with an approximate street value of £6 million, around the UK.

The two-and-a-half-year investigation uncovered a Cardiff-based professional courier engaged by the heads of a Liverpool-based organised crime group to collect wholesale amounts of heroin in Liverpool before distributing them to other organised crime group members in Scotland and Northumberland.

The head of the organised crime group would then launder the proceeds through his partner's bank account in order to disguise his criminality.

In late 2022, Tarian officers coordinated action across the UK in Anstruther, Blyth, Cardiff, Liverpool, and Lochgelly to dismantle the group, executing warrants against five suspects with the assistance of local police forces, totally dismantling the group.

The evidence put forward was so compelling that all five defendants pleaded guilty prior to trial and were sentenced to 57 years and 9 months imprisonment, with credit for their early pleas.

---

**Dismantling an Organised Crime Group Responsible for Distributing Drugs Across the UK**

Twelve members of an organised crime group that smuggled several billion pounds worth of cannabis, cocaine, and heroin, into the UK were sentenced to 246 years imprisonment following a record setting 23-month trial in England and Wales after an investigation by the NCA.

NATIONAL CRIME AGENCY

The organised crime group responsible imported more than 50 tonnes of illegal drugs, the equivalent of around 30 family sized cars, through over 240 importations by hiding deliveries in strong-smelling foodstuff such as garlic, ginger, and onions to avoid detection.

The group operated across the UK and the Netherlands, renting property and setting up front companies across the UK, and developing smuggling routes from Spain and the Netherlands to supply a network of crime groups from the south east of England to Scotland, with the drugs sold across UK communities.

This highly complex investigation demonstrated the scale and reach of criminal enterprises responsible for the supply of illegal drugs to the UK's streets, and the NCA's corresponding reach to stop them.

**Disrupting the Importation of Firearms into the UK**

Following an operation led by the Eastern Region Special Operations Unit, three men from Hertfordshire and Cambridgeshire were sentenced in January 2025 to a total of 68 years and 9 months for their roles in a complex network converting and selling blank-firing weapons and ammunition.

The investigation identified dealings across multiple criminal groups, with a further five members of an associated gang also sentenced in February 2025 for their roles in selling and moving the guns.

The group had purchased over 130 blank-firing weapons which they intended to convert to use hundreds of rounds of live ammunition they had purchased, and then supply these lethal firearms to crime groups across the UK, posing a grave threat to the safety of the public.

The group were also involved in the production of 'zombie dust', a highly dangerous mix of heroin and other substances, including nitazenes, which was being sold to other criminal groups across the country, with more than 60kg of Class A drugs found at the address of one suspect.

This operation and others like it demonstrate the continued success of UK law enforcement in suppressing the firearms threat in the UK.

---

**Tackling Organised Exploitation Programme**

In July 2024, the Yorkshire and Humber Regional Organised Crime Unit concluded support for a local safeguarding unit investigation concerning the historic and potentially ongoing abuse of children at multiple unconnected locations.

The Regional Organised Crime Unit provided advanced intelligence development, deconfliction, and analysis which identified a total of 47 victims and suspects, 37 of which were overseas.

The Tackling Organised Exploitation Programme, a key capability which provides dedicated intelligence and analytical expertise in support of police forces undertaking investigations into complex organised exploitation investigations, identified a further 50 individuals.

In total, support by the Yorkshire and Humber Regional Organised Crime Unit led to over 70 intelligence disseminations which helped identify and safeguard children, removing them from harm, also identifying suspects for intervention and enforcement action across the UK and internationally.

---

**Targeting Organised Shop Theft Offenders**

In 2024, Opal, the national intelligence unit for organised acquisitive crime, coordinated the disruption of a group of offenders committing organised shop thefts. The group was operating on a national scale and was suspected of committed at least 162 offences across 40 police force areas. It was specifically targeting health and beauty products, and pet products, from four supermarket chains.

Through intelligence development, Opal was able to alert relevant police forces when the priority nominals were travelling into their areas to commit offences. Working closely with a reactive police unit, a vehicle was located within a supermarket car park, leading to arrests of two key individuals in August 2024, and a seizure of £2,000 worth of stolen goods. The offenders, who were responsible for a combined theft loss of £68,000, were convicted of 58 offences across 11 force areas. Upon sentencing, one offender received a 16-month custodial sentence and the other, 10 months. One of the offenders is scheduled for deportation once their sentence has been served.

Opal continued to act as a national point of co-ordination between impacted forces, impacted retailers, and wider criminal justice partner agencies and international partners.

## Protecting the Public Online

### Financially Motivated Sexual Extortion Alert

The NCA coordinates the UK policing response to financially motivated sexual extortion through a wide-ranging Action Plan covering guidance for front line officers, support on live investigations and ensuing that the most appropriate pathways for data collection are being created and utilised.

A key part of the Action Plan was an alert issued to education settings in April 2024 covering how to deliver effective prevention education, support victims, and communicate with parents and carers about the financially motivated sexual extortion threat.

The alert was sent to over 80,000 education professionals directly, and downloaded over 22,500 times in the first four weeks, to reach between 320,000 and 360,000 education professionals, over half the total workforce. The alert also received significant press interest which helped it to gain even further reach.

The alert improved awareness of financially motivated sexual extortion across the sector with over 65% of schools having made, or intending to make changes to their teaching practices as a result of receiving it. It also significantly increased professional's confidence in recognising financially motivated sexual extortion cases, and supporting victims in their setting, enabling them to better support young victims and deliver preventative education.

### Targeting the Ransomware as a Service Model

Ransomware as a service model, costs billions of pounds, considering both ransom payments and the costs of recovery and remediation. By February 2023, LockBit had named on their leak site more than 2,350 victims in 112 countries, over twice the all-time number of their closest competitors. That was until February 2024, when the NCA infiltrated the group's network and sized control of LockBit's services, compromising their entire criminal enterprise.

Working closely with international law enforcement partners as part of a dedicated taskforce (Operation CRONOS), the NCA shared over 1,000 decryption keys with LockBit victims and arrested and/or sanctioned various key players including the main administrator.

The NCA and Operation CRONOS partners continue to analyse the seized data working cooperatively to identify and pursue real world identities suspected of being associated with LockBit.

The activity has undoubtedly degraded the group's capability and most notably, their credibility.

### Recovering the Criminal Proceeds of Fraud

Under Operation CORNFLOUR, a South East Regional Organised Crime Unit investigation into investment fraud in Birmingham and London, 12 members of an organised crime group have been sentenced to

between two-and-a-half and nine years imprisonment for conspiracy to commit fraud and money laundering offences.

Following sentencing, the Regional Organised Crime Unit continued to pursue the group, and their criminal proceeds, recovering £167,175 from one individual which will be returned to victims, along with the value of other assets recovered through the investigation. With almost £600,000 available for recovery, and work to confiscate more ongoing, this represents one of the largest confiscation orders so far and shows how we can ensure that crime does not pay.

## Ahead of the Threat

### Russian-Speaking Global Money Laundering Networks

NCA Operation DESTABILISE targeted two Russian-speaking criminal networks responsible for laundering billions of dollars on behalf of drugs gangs, corrupt elites, and sanctions evaders operating around the world. From late 2022 to summer 2023, one of the networks was used to fund Russian espionage operations.

The networks involved used a sophisticated process of exchanging cash for cryptocurrency to move the proceeds of crime around the world, from the streets of the UK and countries across the West, to the Middle East, Russia, and South America.

This process allowed criminal gangs to reinvest in their illicit activities, including buying more drugs and guns.

The NCA, alongside national and international partners, made 84 arrests, seized over £20 million in cash and cryptocurrency, and supported US sanctions against those at the top of criminal chain harming the UK from overseas. This has severely damaged their criminal operation, strengthening the integrity of the UK economy and our financial systems.

### Joint Investigation into Suspected Small Boat Supplier

In November 2024, a man suspected of being a significant supplier of small boat equipment to people smugglers was arrested in the Netherlands, as part of an NCA operation with Dutch and Belgian partners.

The individual is suspected of being a major supplier of boats and engines to the smugglers operating in Belgium and northern France, shipping them from Turkey and storing them in Germany before they are brought forward to northern France when needed.

The types of vessels and engines used in cross-Channel crossings are completely unfit for open water and highly dangerous. There were 78 small boat fatalities in 2024.

The individual is thought to be a key member of the organised crime group and his arrest has severely disrupted their ability to facilitate illegal crossing. He now faces extradition to Belgium to face charges of human smuggling.

### Dismantling International People Smuggling Networks


NATIONAL CRIME AGENCY

The NCA is targeting every element of the criminal business model responsible for the small-boat methodology of illegal migration, and restricting the supply of key equipment.

This has meant working closely with international partners, including in Bulgaria, a key transit point for migrants and small boat equipment destined for the English Channel. Here, the NCA worked closely with Bulgarian authorities to support new legislation that enables them to seize undeclared small boat equipment, sanction those transporting it, and return misdeclared equipment at the border to its place of origin.

The NCA has also coordinated action across Europe, deploying officers overseas to work with partners conducting intelligence-led searches, and seizures of small boat equipment, at border controls on the Bulgarian and Greek land borders with Turkey.

In one case, examination of small boat equipment in the UK enabled partners overseas to identify and target the crime groups responsible. Together, this has resulted in disruption of the supply chain and a significant increase in the costs of small boat equipment; making it more difficult to secure small boats, and reducing the criminal profits of smuggling gangs.

---

### The Use of Drones to Supply Illegal and Prohibited Items to Prisoners

Officers from the South East Regional Organised Crime Unit undertook an operation against a prolific drone pilot who had targeted multiple prison establishments in 2024, as part of the Regional Organised Crime Unit network's innovative work focussed on the use of drones to supply illegal and prohibited items to inmates in prison.

The suspect had targeted 78 prisons in a six-month period, making multiple deliveries at a time, and charging thousands of pounds to provide contraband to inmates. Following their identification, the South East Regional Organised Crime Unit officers executed a warrant at their home address, discovering a 'drone style' workshop, and drug packages and knifes, believed to be destined for a prison establishment.

The suspect was later sentenced to three-and-a-half years in prison. The seizure of weapons undoubtedly prevented attacks in the prison and injury to prison officers and inmates.

This operation demonstrates both the resilience of criminal groups, and the tenacity of law enforcement to continually disrupt their operations.

---

### Building Capability to Tackle Criminal Concealments

Criminal concealments are essential to criminal efforts to evade law enforcement when bringing drugs, firearms and people into the UK illegally.

During 2024, the NCA delivered continual personal development events to almost 800 officers from law enforcement and military partners across England, Wales, Northern Ireland and internationally, and issued

five alerts covering new trends or risks in criminal concealments to improve their capability to locate them.

This has had an immediate impact, with approximately 172 sophisticated concealments discovered between in 2024, an increase of 59 on the previous year.

The work to disrupt the people who make them, and the groups that use them continues. This includes strengthening legislation through the Border Security, Asylum and Immigration Bill, which will simplify UK legislation so that law enforcement can take the same action in the UK and at the border to seize empty concealments when they are discovered.