

The National Strategic Assessment is split into three main sections:

Overview of SOC > Summarises key issues across the SOC domains, explains how the threats have changed, and the future of SOC.

Domains > Provides more detail on each SOC domain.

Tackling the Threat > Shows how the NCA and partners responded to the SOC threat in 2025.

"As criminality becomes more interconnected, the NCA, policing, and our partners must be too."

Graeme Biggar



Welcome from the Director General

Serious and organised crime (SOC) continues to present a profound threat to the UK. Its corrosive impact is felt nationally, in our institutions and economy, and locally, in the safety, confidence, and resilience of communities across the country. To combat it, we need to understand it, and that is the point of this 2026 National Strategic Assessment.

We have changed the structure of the assessment this year from a threat focus to looking at domains: within communities, at the border, transnationally, online, and within finance. The intent is to shine a different light on familiar challenges, expose how criminals exploit vulnerabilities across multiple spheres, and thus enrich our understanding of crime and how we can tackle it.

That domain focus has helped illuminate four cross-cutting trends: the technological transformation of SOC; the convergence, diversification, and expansion of criminal activity; the increasing impact on the UK of SOC exploitation of global instability and geopolitics; and, as a result, the increasing harm posed to society. Of these trends, the most notable has been technology. This year we assess technology is no longer just an enabler of SOC; it is driving a large-scale transformation in terms of its scale, sophistication, and resilience.

The consequence is that, overall, we assess that the SOC threat has increased in 2025 and – despite the excellent work of NCA officers, policing and our partners – is likely to do so again in the coming year.

It has not done so uniformly. Of the nine specific threats we assess, drugs remains the only one where both the threat and the harm have increased, driven by increased production,

falling wholesale prices, rising consumption of a wider range of drugs, and a diversification of smuggling routes and methodologies.

The threat from organised immigration crime and illicit finance has also increased, reflecting higher demand, more organised facilitation, and rising criminal profits. Whilst the harms from cybercrime and fraud have escalated following several high-impact ransomware attacks and increasing romance investment frauds, both fuelled by online enablers and increasingly sophisticated social engineering.

The overall level of the remaining four threats - child sexual abuse, firearms, modern slavery and human trafficking, and organised acquisitive crime - has neither increased nor decreased.

Little of what is set out in this assessment applies uniquely to SOC. We see the same trends affect terrorism, state threats, violence against women and girls, and much other crime. And we see more links between these threats and SOC. This insight has informed the Government's decision to merge the NCA and Counter Terrorism Policing into a new National Police Service. As criminality becomes more interconnected, so must we. I am confident this assessment provides a foundation from which to do so, and I am grateful to all those who have contributed to it.

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 2025, rather than providing a baseline of all SOC threats.

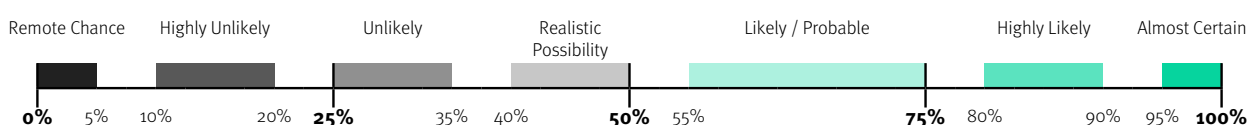
Unlike previous National Strategic Assessments, this document moves away from presenting individual sections on each SOC threat to focus on five domains where SOC operates: UK communities, the border, transnational networks, online environments, and finance. By adopting this domain-based approach, the assessment captures cross-cutting vulnerabilities, mirrors offenders' agile and threat-agnostic methods, and provides a holistic view of the overall threat to the UK.

The primary SOC threats considered in this paper are child sexual abuse, cybercrime, 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 2026 is January 2025 to December 2025; however, where available and relevant, data and intelligence up to and including March 2026 has been used.

It is not always possible to be certain of a development in the threat, so throughout the National Strategic Assessment 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, Border Force, the Crown Prosecution Service, HM Prison and Probation Service, HM Revenue and Customs, Immigration Enforcement, the National Ballistics Intelligence Service, and the Serious Fraud Office;
- UK intelligence community, including the National Cyber Security Centre;
- HM Government, including the Cabinet Office, Companies House, Foreign Commonwealth & Development Office, HM Treasury, Home Office, and the Office for National Statistics;
- Overseas law enforcement agencies and organisations;
- 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;
- Opal, the national police unit focused on the collation, coordination, and dissemination of intelligence relating to organised acquisitive crime.



Technological transformation is almost certainly reshaping serious and organised crime at scale, increasing automation, reach, and routes into offending.

Summary

The SOC Threat in 2026

SOC is one of the UK's most persistent and harmful threats. In 2025, the threat continued to become more diverse, with criminal groups exploiting fast-moving technologies, working in looser alliances, and using specialist facilitators to cause more harm at greater scale.

In 2026, four cross-cutting trends define and drive the SOC threat to the UK:

- Technological transformation is reshaping SOC, as rapid digital change increases scale, automation, and routes into offending.
- Criminal markets are converging and expanding as global criminal groups increasingly diversify and collaborate.
- Global instability is driving developments in SOC, as conflict and geopolitical pressures create new criminal opportunities.
- Harms from SOC are being felt more intensely across society, with growing impacts on individuals, communities, and national resilience.

These trends have almost certainly expanded the reach and impact of SOC, with rapid technological change acting as the primary driver of this evolution. The overall threat is highly likely to continue increasing over the next 18 months, challenging not just law enforcement but society as a whole, including government, industry, and communities.

How SOC is Evolving | Drivers and Enablers

Technological Transformation

Technological change is no longer simply an enabler of SOC; it is almost certainly reshaping it at scale. Digital tools are transforming how criminal groups operate, increasing their reach, sophistication, and resilience. For example, social media platforms allow offenders to identify and target victims, recruit technical specialists, expand their operations, and operate across jurisdictions with vastly greater scale and ease.

The increased functionality, scale, and development of artificial intelligence tools and their adoption by offenders will enhance and enable SOC activity. Increasingly accessible artificial intelligence tools and large language models are lowering barriers to entry by providing individuals with limited technical expertise with the capability or tools needed to offend. Artificial intelligence use has been most visible in the production of increasingly realistic child sexual abuse material and in improving the effectiveness of fraud activity, but is also enabling cybercrime, money laundering, and organised immigration crime activity.

Younger, digitally native offenders are the first generation to have grown up within integrated online and offline environments and are almost certainly more attuned to their exploitation for criminal gain.

Social media and communication platforms, including Discord, Facebook, Instagram, Snapchat, Telegram, TikTok, and X, are attractive due to their audience reach, interconnectivity, and the perceived anonymity they grant users.

Online spaces that offer support, community, and connection for vulnerable children are highly likely targeted by offenders. The proportion of children reporting upsetting online experiences rose to 25% in 2025, from 10% in 2024. Popular gaming platforms such as Roblox and Minecraft continue to be used to target children.

An estimated 80% of migrants facilitated to the UK via small boats used social media to locate or communicate with an agent working as part of an organised crime group at some stage in their journey, with TikTok highly likely the primary platform used to promote the services of organised immigration crime groups.

Organised crime groups are increasingly using individuals with chemical or scientific expertise to produce and extract drugs within the UK. The use of chemically concealed cocaine is becoming more sophisticated, requiring specialist knowledge to extract the drug on arrival. Illicit laboratories present significant risks, including exposure to harmful substances and the potential for explosions. Equipment and precursor materials are often sourced online, with little regard for safety standards.

Organised crime groups and prisoners are highly likely increasingly using drone experts providing services across multiple groups. Custom-built drones enable larger payloads, more frequent use, and remote 'beyond line of sight' operation. SOC use of drones is likely to expand in the next few years.

The Diversification, Expansion, and Convergence of Criminal Activity

There has been a long-term trend in SOC offenders broadening the range of criminal activities, commodities, and methodologies they engage in; however, in recent years opportunities

[Overview of SOC](#) > [Summary](#) | [How the Threats Changed in 2025](#) | [SOC Futures](#)

presented by new and evolving technologies, alongside the growing as-a-service marketplace mean that it is almost certainly easier than ever for offenders to diversify and grow their influence and profitability.

Human enablers, including complicit and unwitting professional enablers, corrupt individuals, and sometimes members of the community, play a critical role in ensuring that SOC activity remains hidden.

Online platforms make it easier for criminals to access specialist services, allowing groups to outsource key functions rather than retain them internally. This has contributed to more fragmented and networked operating models. For example, organised crime groups frequently outsource money laundering to specialist networks. Russian-speaking money laundering networks, in particular, service a wide range of clients. This includes transnational organised crime groups and, in some cases, state-linked actors, enabling the movement and concealment of criminal proceeds.

Foreign states use criminals as proxies for illegal activity in the UK, offering plausible deniability and ease of employment. In 2025, state-linked interests were connected to cybercrime, drug and firearms trafficking, fraud, money laundering, and violent crime.

Exploitation of Global Instability and Geopolitics

It is likely that most SOC impacting the UK has direct or indirect overseas links. Technology enables organised crime groups to exploit global instability, conflict, weak governance, corruption, and differences in international law and enforcement. For example, fraud compounds, first detected in South East Asia, have expanded their operations and are spreading globally, with SOC groups exploiting areas affected by conflict and weakened governance.

Powerful and accessible new technology enables offenders to bypass state infrastructure and to operate remotely, allowing criminals to target the UK from around the world. For example, the use of Starlink communications networks by fraudsters in 2025 made it possible for them to continue operating for a time when other internet services had denied them.

Transnational organised crime groups from China and the Western Balkans remain persistent threats. Organised crime groups from China are highly likely among the most significant threats to the UK, with roles in fraud compounds, drug precursor supply, synthetic opioids, and underground banking. Western Balkan organised crime groups highly likely retain the highest level of control over the end-to-end supply of cocaine into the UK.

SOC Impact on the UK

SOC remains a persistent and embedded threat to the UK's national security. Its impact undermines border security, weakens governance, and erodes public trust in institutions. The cumulative harms experienced by large numbers of individuals can create heightened public fear and community tensions.

SOC also imposes substantial economic harm. It distorts legitimate markets and undermines the confidence that underpins investment and growth. These economic impacts are compounded by links to state threats and by offenders' exploitation of global vulnerabilities, making SOC not only a law enforcement challenge but a wider threat to the UK's economic security and long-term resilience.

Impact on Communities

Illicit drug markets remain the main driver of SOC in UK communities and are continuing to grow in scale and harm. Firearms are often used to protect drug businesses; modern slavery victims are used in drug production; and the billions of pounds generated annually from the UK illegal drug trade are laundered in the UK and overseas, fuelling further criminality. Violence, including firearms offences, knife crime, kidnap, and extortion, is frequently associated with the drug trade. The threat to the UK from illicit drugs remains high and likely increased in 2025.

Levels of SOC-related violence are highly likely to have remained broadly stable, with drug supply continuing to drive most firearm use. There is unlikely to have been a significant change in criminals' overall ability to source and use firearms in 2025. However, the criminal use of counterfeit firearms is highly likely increasing, partly driven by reduced availability of original lethal-purpose and converted blank-firing weapons. Counterfeit firearms are of better quality, and can use more powerful ammunition, than the converted top-venting blank-firers most prevalent in firearms criminality in 2023 to 2024.

A small number of UK-based criminals use children and individuals outside their core networks to carry out violence-as-a-service, including firearms offences. The UK has not experienced this at the scale observed in parts of northern and nearby European countries in 2025, where organised crime groups have increasingly outsourced serious violence to third parties.

Many SOC-linked crimes within communities (including extortion, kidnap, intellectual property theft, organised prostitution, protection rackets, waste crime, and wildlife crime) are almost certainly under-reported, but generate substantial profits used to support further criminality.

Impact on Governance and the Border

Organised crime groups looking to transport illicit commodities or facilitate people into the UK must find ways to evade border controls. It is likely that the overall SOC risk to the UK posed by organised crime groups at the border has increased in 2025.

The threat from organised immigration crime likely increased in 2025, primarily driven by adaptations to small boats facilitation models, including higher numbers of migrants per vessel. These crossings continue to pose significant risks to life and safety, with fatalities and injuries occurring in dangerous maritime conditions. Beyond the immediate human harm, increased irregular arrivals add sustained operational and financial pressures to UK border and asylum systems, while the visible demonstration of criminality can amplify community tensions.

Corruption is almost certainly a key enabler of SOC. Whilst it can occur within international supply chains, it is also a domestic threat and is likely to be significantly under-reported. In the UK, local government and construction are assessed as among the sectors most exposed to bribery and corruption risks. High levels of procurement activity and subcontracting arrangements in these sectors create vulnerabilities that can be exploited.

Impact on the UK Economy

SOC imposes substantial economic costs, which can undermine growth and resilience. The Jaguar Land Rover ransomware incident was very costly, to the extent that it affected gross domestic product. In October 2025, the Cyber Monitoring Centre, a non-profit organisation, assessed this to be the most economically damaging cyber event to hit the UK, with an estimated cost to the UK economy of £1.9 billion. Fraud cost England and Wales an estimated £14 billion in 2023 to 2024 and remains the most prevalent headline crime, estimated to be 45% of all crime.

Overview of SOC > [Summary](#) | [How the Threats Changed in 2025](#) | [SOC Futures](#)

Organised acquisitive crime continues to cause losses and infrastructure disruption. Criminals are increasingly targeting valuable metals from renewable energy sites, causing substantial losses and disrupting green energy production and hindering progress towards the UK's climate goals.

SOC offenders use high street businesses, including barber shops, minimarkets, nail bars, and vape shops, to support criminality, distribute illicit goods, engage in illegal working, or launder funds. These practices undermine legitimate businesses, damage consumer confidence, and harm local investment.

Drugs, organised immigration crime, and illicit finance increased in 2025, driving disproportionate harm. While a small number of high-impact incidents increased the harm from cybercrime.

How Threats Changed in 2025

At the individual threat level, drugs, organised immigration crime, and illicit finance are all assessed to have increased in 2025. These are high-volume crimes that generate significant harm across the UK. As a result, changes within these areas have a disproportionate impact on the overall SOC landscape.

These threats also act as drivers of wider criminality: drugs underpin much serious violence, including firearms offending; organised immigration crime sustains illegal and grey economies; and illicit finance both enables and profits from other criminal activity. Harm from cybercrime has likely increased despite no overall significant change in threat: whilst the majority of ransomware attacks have been no more serious than in 2024, changes in the methods of criminals caused very serious harms in 2025.

Threat	Change in Threat in 2024*	Change in Threat in 2025**	Change in Harm in 2025**
Child Sexual Abuse	Increase	No Change	No Change
Cybercrime	No Change	No Change	Increase
Drugs	Increase	Increase	Increase
Firearms	No Change	No Change	No Change
Fraud	Increase	No Change	Increase
Illicit Finance	Increase	Increase	No Change
Modern Slavery and Human Trafficking	No Change	No Change	No Change
Organised Acquisitive Crime	No Change	No Change	No Change
Organised Immigration Crime	Increase	Increase	No Change

* From NSA 2025. ** 01 October 2024 to 30 September 2025.

The Changes by Threat

Child Sexual Abuse

There is no substantial change in the child sexual abuse threat in 2025, with trends continuing to evidence high harm offending following an increase in the threat in 2024. While the volume of offences reported to police in England and Wales continues to grow (104,266 in the year to September 2025, 3% higher than the 101,184 the previous year) it is highly likely that factors driving offending, such as sexual gratification, financial gain, and the desire to cause harm to others remains broadly unchanged.

The complexity and severity of the threat continues at high levels resulting in physical and psychological harm to victims. Offenders will continue to identify and target vulnerable individuals both offline, such as in contact group-based child sexual exploitation, and through the exploitation of online environments. Offenders continue to develop their capability to target and harm multiple victims, as well as exploiting children to produce increasingly more indecent and depraved imagery.

Cybercrime

The threat from serious and organised cybercrime to the UK did not increase in 2025, despite the increase in harm from a small number of impactful events; however, the threat remains very high. The intent of cybercriminals impacting the UK remains consistent; while there has been a small number of attacks from UK-based individuals whose motivation includes notoriety, the vast majority of attacks are conducted by criminals based in other jurisdictions, for financial gain. Some criminals had greater effect than previously seen from deploying social engineering techniques, but the overall capabilities of offenders did not increase in 2025. Data theft and/or encryption remains the most common attack methodology. The opportunity for cybercriminals to conduct malicious activity that affects the UK continues to increase, due to increasing online dependence across society.

Drugs

The drugs market continues to evolve with a diversification of products. Significant increases in the volumes of ketamine (from 769kg in the year ending March 2024 to 1,092kg in the year ending March 2025) and cannabis (from 74.2 tonnes to 127 tonnes over the same period) seized at the UK border, along with more detections of domestic drug laboratories and changes in drug distribution models, all indicate an upward trend in the threat in 2025.

The threat from cocaine remains high, with seizures in the UK having increased by more than 440% in the last ten years (from 3.4 tonnes in 2015 to 18.5 tonnes in 2025). The range of substances that are currently popular among users is increasing, creating new markets, while the harm from illicit drugs has also increased.

Drug-misuse deaths in England and Wales continued to increase in 2024, rising by 3% from 3,618 in 2023 to 3,736 in 2024, and more than doubled since 2012 (1,496). Although this was a smaller increase than the previous year when there was a 16% increase, deaths related to cocaine abuse in England and Wales increased by 14% to 1,279 in 2024, 11 times higher than in 2011 (112). Though the synthetic opioid market continues to evolve, there was a 17% decrease in the number of recorded nitazene-related deaths in the UK in 2025 to 359 deaths, a reduction from 435 in 2024,

Overview of SOC > [Summary](#) | [How the Threats Changed in 2025](#) | [SOC Futures](#)

with recorded nitazene-related deaths now close to 1,000 in total since June 2023. The figure for 2025 is expected to increase as additional test results are finalised.

The drugs threat further increased as organised crime groups, using the container shipping mode to smuggle illicit drugs, demonstrated their ability to diversify their methodology. This includes using alternative European ports, enhanced concealments, and at-sea-drop-offs, in response to high volumes of seizures in recent years.

Firearms

Firearm use in the UK remains low and offences decreased by 9% in England and Wales in the year ending September 2025 (from 5,356 to 4,851 offences). However, criminal intent and capability to source and use firearms is unlikely to have changed significantly. Discharges with converted blank-firers are decreasing due to reduced availability, following action taken by the NCA and partners. Conversely, although not available to most criminals, there has been an increase in [counterfeit firearms](#) that are of better quality and can use more powerful ammunition. Firearm ownership remains aspirational for many criminals who do not have the requisite contacts or funds, and threats to use a firearm, even where none exists, remains the most common criminal use.

Fraud

There is no evidence of a substantial change in the overall threat to the UK from fraud; however, harms have increased. The Crime Survey for England and Wales estimated fraud had risen by only 7.6% (295,000) over the year ending September 2025, compared to the same period the previous year, which was not a statistically significant increase. However, it is likely the threat from both investment and card not present fraud has continued to increase. According to UK Finance, losses from investment fraud during the first six months of 2025 rose 55% to £97.7 million (from £63.0 million) compared to the same period in 2024. Similarly, reports of card not present fraud have continued to rise, likely driven in part by a growing capability to socially engineer victims into revealing one-time passcodes.

Illicit Finance

It is likely that organised crime networks' capabilities and opportunities to conduct illicit finance impacting the UK have increased in 2025, although the overall level of harm likely remains unchanged. Professional enablers (based in the UK and overseas), in addition to technological enablers, continue to innovate to avoid detection of illicit finance activity and maximise SOC profits. The rate of growth has been limited by law enforcement action, including against some Russian-speaking money laundering networks, highly likely disrupting their criminal business infrastructure, reputation, and relationships during 2025. It is likely that opportunities, and demand, for money laundering have increased due to rising predicate threats like drugs and organised immigration crime.

Modern Slavery and Human Trafficking

There is no evidence of substantial change in the overall threat from modern slavery and human trafficking in 2025 compared to 2024, with the number of potential victims exploited in the UK broadly stable. Although the level of harm from modern slavery and human trafficking remains high, it is highly likely that offender intent, capability, and opportunity have remained largely unchanged, with factors such as profitability, consumer demand, offender organisation, and sophistication continuing to underpin offending. Modern slavery and human trafficking remains

a highly gendered crime, with women and girls accounting for the majority of victims of sexual exploitation and domestic servitude, and men and boys most often exploited for labour and in criminal activity.

Organised Acquisitive Crime

It is unlikely that the overall threat from organised acquisitive crime has substantially changed in 2025. The level of organised acquisitive crime offending has remained broadly stable, despite indications of a reduction in acquisitive crime more generally in 2025, driven by decreases in organised retail crime, personal robbery, residential burglary, and vehicle crime offences. Law enforcement activity and partnership work with industry are highly likely to have contributed to this reduction. Increased awareness of criminal organisation, improved security measures, and target hardening by businesses have also likely played a role.

Offenders continue to diversify both their methods and the enablers used to facilitate organised acquisitive crime activity. Online platforms remain a key tool for identifying victims, communicating with associates, identifying commodities in demand, and disposing of stolen goods. Targeting of renewable energy infrastructure was a notable trend in 2025, with wind turbines and electric vehicle charging cables increasingly targeted due to the high value of associated materials. Offenders have also continued to exploit a range of criminal tools and techniques, and organised crime groups remain agile in adapting their operating models to maximise opportunities across the organised acquisitive crime landscape.

Organised Immigration Crime

It is highly likely that an increase in organised crime group capability (through more organised launch tactics, such as the taxi boat method) and opportunity (through increased demand from Horn of Africa migrants) within the small boats threat drove an overall increase in the organised immigration crime threat to the UK in 2025 compared with 2024. There were 41,472 small boat arrivals to the UK in 2025, a 13% increase on 2024 (36,816). Despite a 3% decrease in UK small boat events in 2025 (672) compared with 2024 (695), organised crime groups increased the number of migrants per boat to enable more arrivals. The average number of migrants per boat arriving in the UK was 62 in 2025, a 17% increase on 53 in 2024.

2025 saw fewer migrant fatalities in the English Channel (27) than 2024 (78), highly likely due to intervention by rescue craft and fewer incidents of non-paying passengers opportunistically storming boats in the water.

Emerging technologies will redefine criminal capability enabling less-skilled offenders to operate at scale.

SOC Futures

Three cross-cutting drivers will shape the impact of SOC over the next five years: conflict and economic tensions; technology; and trust in information and institutions.

Conflict, Insecurity, and Economic Tensions

Global instability is increasing. In 2024, the number of state-based conflicts reached 61, the highest level since 1946, and new conflicts emerged across multiple regions in 2025. Conflict and insecurity are destabilising regions and nations, weakening the rule of law, and creating permissive operating environments for SOC. Conflict also drives migration increasing the number of people organised crime groups can engage with and exploit.

Rising insecurity is driving increased global military expenditure which reached \$2.7 trillion in 2024. The United Nations assesses that increased global military expenditure is likely to divert funds from social programmes. It is highly likely that in some countries this increased spending will divert resources away from policing and SOC prevention. In low-income and fragile states, it is highly likely that increased military spending will replace investment in education, health, and infrastructure, entrenching poverty and inequality and widening the pool of individuals vulnerable to involvement in SOC.

Global tariffs rose sharply in 2025. Once the effects of tariffs are felt through higher prices and disrupted supply chains, it is likely SOC groups will exploit opportunities to undercut legitimate markets. Higher prices will also expand profit margins for manufacturers and distributors of counterfeit goods, strengthening illicit trade.

Technology

Technology will continue to play a transformative role in SOC over the next five years. It is almost certain that offenders will favour technologies that reduce the perceived risk of detection,

Overview of SOC > [Summary](#) | [How the Threats Changed in 2025](#) | [SOC Futures](#)

increase profitability, lower barriers to offending, and enable offending across jurisdictions. It is highly likely that crime-as-a-service providers will increasingly allow low-skilled offenders to leverage advanced technologies such as artificial intelligence, as well as magnifying the threat from technologies such as drones and applied chemistry for the manufacture and concealment of drugs.

The Threat from Artificial Intelligence-Enabled SOC Offending

While artificial intelligence will likely provide significant capabilities to law enforcement over the next five years, it will also be used increasingly for SOC to make offending easier and more profitable:

- Large language models and sophisticated deepfakes will enhance victim engagement techniques for child sexual abuse, fraud, and modern slavery and human trafficking offences.
- Artificial intelligence-powered translation tools will allow non-English-speaking offenders to target UK victims more plausibly.
- Artificial intelligence is identifying software vulnerabilities at greater pace and will enable the automation of elements of cyber attacks, and the targeting of child sexual abuse, fraud, and modern slavery and human trafficking victims at scale.
- Generative artificial intelligence will increasingly be used to create child sexual abuse material.

It is likely that legitimate and SOC-generated companion apps will create opportunities for SOC offenders engaged in extortion and romance fraud. In a 2025 UK survey, 36% of respondents had used an artificial intelligence companion at least once, 23% were interested in doing so, and 25% believed such apps could replace human relationships. It is likely SOC groups will develop their own artificial intelligence companion apps designed to manipulate users into sharing sensitive personal data, enabling future extortion. It is likely that legitimate companion apps pose risks, as they collect and store highly personal information that is often poorly secured, leaving users vulnerable to extortion by SOC. In August 2025, 117 misconfigured artificial intelligence chatbots were identified that were exposing explicit user fantasies.

The Evolving Threat from Drones

It is likely that SOC use of drones will diversify over the next five years and will be increasingly enabled by specialist drone builders and operators. SOC offenders most commonly use drones to convey contraband into prisons and, to a lesser degree, to locate cannabis cultivations (using thermal imaging) for burglary, and to conduct counter surveillance from law enforcement or rival groups.

It is highly likely that in the next five years organised crime groups will seek opportunities to import illegal commodities into the UK using marine and aerial drones. In July 2025, the Colombian Navy intercepted a self-propelled semi-submersible vessel capable of carrying 1.5 tonnes of cocaine, which was fitted with a satellite antenna enabling it to be remotely operated. In November 2024, Spanish police dismantled an organised crime group using fixed-wing drones to transport drugs from Morocco to Spain.

The Threat from Old Technology

It is not just new technologies that provide opportunities to SOC. It is almost certain that the persistence of obsolete and unsupported technologies will provide opportunities for SOC to exploit over the next five years and it is likely that as technological change accelerates, the number of legacy systems with unpatched vulnerabilities will grow.

When free security updates for Windows 10 ended in October 2025, 31% of Windows users were still operating on this version. An estimated 25% of users did not intend to upgrade, leaving approximately 5 million devices vulnerable to emerging cyber threats.

Trust in Information and Institutions

It is highly likely that trust in information and institutions will decline between 2026 and 2031. It is highly likely that exposure to mis- and disinformation will increase, driven by shifting patterns of news consumption away from traditional news providers such as television and print towards less moderated channels such as social media, the increased use of generative artificial intelligence to create synthetic media, and the increasing amplification of false narratives by malicious actors.

It is highly likely that SOC offenders will exploit less moderated online spaces and synthetic media to market illicit goods, target child sexual abuse, fraud and modern slavery and human trafficking victims, and advertise services including people smuggling.

It is highly likely that trust in the criminal justice system will be reduced by the proliferation of deepfake media and the degrading effect it has on trust. While deepfake media detection capabilities are improving, it is almost certain they will at times lag behind improvements to generative artificial intelligence models. It is likely that SOC offenders will attempt to undermine the integrity of criminal trials by introducing deepfakes that provide false alibis or depict judges, jurors, or witnesses in ways that undermine their credibility or impartiality. It is also likely that as media generated by artificial intelligence becomes more realistic and commonplace in daily life, genuine video evidence such as CCTV footage will carry less weight with juries, potentially leading to acquittals where other sufficient corroborating evidence is lacking.

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

Illicit drugs continue to be the main driver of harm linked to serious and organised crime in our communities, with the threat likely increasing in 2025.



SOC in Communities | Harm to Individuals

A wide range of SOC threats cause harm to individuals in our communities including the supply of illicit drugs, use of weapons including guns and knives, and serious violence and coercion. SOC threats involving the use of abuse and exploitation, such as child sexual abuse and modern slavery and human trafficking, often harm some of the most vulnerable individuals in our societies.

Drugs

The overall threat to the UK from illicit drugs is likely to have increased in 2025. Several trends indicate an increase in the threat: a wider variety of substances, lower wholesale prices than in 2024, significant increases in volumes of ketamine and cannabis seized at the UK border, an increase in consumption of a range of substances, and an increase in drug-related deaths.

The threat from cocaine remains high, with seizures in the UK having increased by more than 440% in the last 10 years, from 3.4 tonnes in 2015 to 18.5 tonnes in 2025. Cocaine prices were lower in 2025 than in 2024, while wholesale purity levels remained consistent, likely reflecting robust and adaptable supply chains and high levels of production in source countries. The increase in availability is a likely cause of lower prices, with competition for market share amongst criminals also likely contributing. Deaths where cocaine use was a contributory factor increased significantly in England and Wales in 2024, rising by 14% to 1,279 deaths, 11 times higher

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

than in 2011 (112). It is highly likely that poly-drug use contributed to the registered cocaine-related deaths, although it has not been possible to determine all contributing factors.

Overall [drug-misuse deaths](#) in England and Wales have continued to increase with a 3% rise from 3,618 deaths in 2023 to 3,736 deaths in 2024, according to the Office for National Statistics. However, there has been a mixed picture across the UK, with an overall decrease in drug-related deaths in Scotland and Northern Ireland. Scotland continues to have much higher drug-related deaths per capita than all other UK regions. Overall, drug misuse deaths in Scotland decreased by 13% from 1,172 in 2023 to 1,017 in 2024. Deaths due to drug-related causes in Northern Ireland decreased by 22.5% from 218 deaths in 2020 to 169 in 2023.

The heroin market in the UK was stable in 2025, despite ongoing market uncertainty related to the Taliban's narcotics ban in Afghanistan since 2022. Although heroin supply into the UK has remained steady overall, in terms of seizures and purity levels, it is highly likely that UK-based drug suppliers will continue to fortify heroin, and illicit pharmaceutical drugs, with more [harmful substances](#), including synthetic opioids. This significantly increases the risk of harm with many users unaware if heroin or illicit tablets have been fortified. In addition, the practice of poly-drug use, where users consume additional drugs or alcohol, will almost certainly increase the risk of overdose.

Although the synthetic opioid market continues to evolve, there was a decrease in the number of recorded nitazene-related deaths in the UK in 2025 to 359 deaths, a reduction from 435 in 2024. However, the figure for 2025 is expected to increase as additional test results are finalised. There were some regional variations in 2025 with nitazene-related deaths increasing in Scotland compared with England, Wales, and Northern Ireland where they decreased.

Naloxone is used widely by first responders and hospitals to reverse opioid overdoses. Take-home naloxone kits are also distributed to people who use opioids, and others who may witness overdoses, by a [range of services](#). However, it is not currently possible to assess the overall impact on drug-related deaths and non-fatal overdoses due to data gaps.

It is almost certain that organised crime groups have been adapting their business models to meet persistent demand for a range of substances associated with the night-time economy and general recreational drug use. This includes drugs such as cannabis, cocaine, and ketamine.

It is likely that the threat from ketamine continued to increase in 2025. The number of ketamine users starting drug treatment in 2024 to 2025 (5,365) in England is now over 12 times higher than it was in 2014 to 2015, when the number was 426. There has been a rise in the number of children aged 17 or under entering drug treatment and reporting a problem with ketamine use, from 512 in 2021 to 2022, to 1,465 in 2024 to 2025. Long-term abuse of ketamine can commonly lead to [uropathy](#), often culminating in the need to surgically remove the bladder. Ketamine-induced uropathy has been increasing in the UK, particularly in the younger population, with some urology departments responding by setting up specialist clinics.

It is likely that the volume of ketamine entering the UK is increasing to meet higher demand. In the year ending March 2025, there was a 34% increase in the total quantity of ketamine seized by Border Force compared with the previous year, from 769kg to 1,029kg.

It is likely that drug organised crime groups are increasing their use of sophisticated chemical techniques to conceal or produce drugs. The operation of illicit laboratories poses an inherent risk to the public, both from exposure to harmful substances, the potential for explosions, and the

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

harm caused to the environment by waste products.

Drug distribution models continue to adapt to market changes. It is likely that the number of county lines was broadly stable between 2024 and 2025, with a shift towards a more localised model of drug distribution and a significant rise in social media lines.

Violence, Weapons, and Coercion

It is highly likely the threat from SOC-related violence in the UK remains broadly stable but there is a mixed picture across regions. Imitation weapons, cross-commodity criminality, and organised crime group tensions continue to generate harm to UK communities through intimidation and violence. Drug supply continues to be a significant driver of SOC-related violence, including use of firearms. These dynamics are likely to sustain public perception of an increasing threat despite a relatively stable number of incidents.

Firearm use in the UK remains low with offences decreasing by 9% (from 5,356 to 4,851 offences) in England and Wales in the year ending September 2025, according to the Office for National Statistics. This was the lowest level of offences since current police recording practices began in the year ending March 2003. There were 36 homicide offences involving a firearm in England and Wales in the year ending March 2025; this was slightly higher than the ten-year average of 31 but within the expected range. Indirect threats (for example, verbal threats where no firearm is seen, or threats made on social media) are now more common than threat incidents where an actual firearm is involved or seen.

Although criminal capability to source and use firearms is unlikely to have changed significantly, it is highly likely the use of counterfeit firearms is increasing. It is likely the number of injuries and fatalities will increase as counterfeit firearms are of better quality, and can use more powerful ammunition, than the converted top-venting blank-firers most prevalent in criminality in 2023 to 2024. Less availability of convertible blank-firers in Europe is likely causing criminals to seek alternative firearms, such as counterfeit firearms.

Trends observed in some parts of northern Europe in 2025 have seen organised crime groups increasingly outsource serious violence, including firearms offences, to third parties, often children. The UK has not seen UK-based criminals use children and individuals outside their core networks to carry out violence-as-a-service in the same volume, with only a small number of cases.

Knives continue to be used significantly more in serious violence than firearms due to their availability. Within a SOC context, criminals using only knives are likely to be lower-tier criminals involved in urban street gangs or county lines activity, typically motivated by physical protection, self-advancement, and promotion of gang identity.

It is likely that the threat from knife crime reduced overall in 2025, in part due to targeted policing efforts. Office for National Statistics figures indicate a 9% decrease (from 55,149 to 50,430 offences) in knife-enabled crime to the year ending September 2025. There was also a 10% decrease in knife-enabled robbery in force areas targeted by the UK Government's taskforce between the year ending June 2024 and the year ending August 2025.

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

SOC-related vendetta kidnaps continue to be used by criminals involved in a range of SOC including county lines, drug supply, money laundering, modern slavery and human trafficking, and organised immigration crime. Although the number of kidnaps reported to the NCA was stable in 2025, the number of incidents has steadily increased since 2018.

Most incidents of violence against women and girls do not relate to SOC. However, the attitudes and behaviours that underpin violence against women and girls can act as a driver of SOC offending, both in highly gendered forms of offending such as child sexual abuse, modern slavery and human trafficking, and organised prostitution, and in forms of offending in which women and girls are actively recruited into criminality, such as in urban street gangs involved in drug supply.

Abuse and Exploitation

SOC-related abuse and exploitation continue to harm some of the most vulnerable individuals in our communities, including children. Organised crime groups continue to exploit young people as couriers and facilitators across multiple threat areas including drug supply and fraud. Recruitment of [money mules](#) remains a persistent money laundering method with under-18s and students specifically targeted.

The scale of child sexual abuse and exploitation continues to maintain high levels, with the volume of [child sexual abuse offences reported to Police in England and Wales](#) remaining broadly consistent in 2025 (122,768, 6% more than in 2024). Children are increasingly being exploited to produce more indecent and depraved imagery, and offenders' sophistication online is increasing their capability to target and harm children. The complexity and severity of the threat continues to grow, with the levels of physical and psychological harm to victims resulting from all child sexual abuse and exploitation offending remaining high into 2026.

Offenders continue to identify and target vulnerable individuals both offline, such as in contact group-based child sexual abuse and exploitation, and through the exploitation of online environments, through the indiscriminate targeting of multiple victims.

[Contact child sexual abuse and exploitation](#) offences recorded by police in England and Wales remain consistently high: in 2024 accounting for 65% of all child sexual abuse and exploitation crimes, and more likely to involve a known perpetrator (87%) than non-contact offending. Where a relationship was recorded, a quarter of abuse occurred in the familial environment, with parents the most common perpetrators in familial contact child sexual abuse and exploitation offending, followed by siblings. However, all child sexual abuse and exploitation offending remains under-reported, which continues to impact wider understanding of the threat.

It is likely that the threat from group-based contact offending has remained stable between 2023 and 2025. Within contact child sexual abuse and exploitation, group-based offending accounted for 5.6% of all offences in 2024, according to the [Hydrant Programme](#). The complexity of group-based offending is likely a factor in the low volume of reporting to police.

The Hydrant Programme classify group-based child sexual abuse and exploitation into seven categories: Child-on-child (24%), [Child Sexual Exploitation](#) (17%), Familial (32%), Institutional (9%), Ritualistic, as well as Other (11%) and Unknown (6%). The most notable change was a 6% increase in crimes categorised as 'Familial', rising from 26% in 2023 to 32% in 2024. Offence types committed remained consistent, with rape remaining the highest recorded offence, followed by sexual assault.

Domains > SOC in Communities: Harm to Individuals & Harm to Society | SOC at the Border | Transnational SOC | SOC Online: Online Harms & Online Enablers | SOC Finance

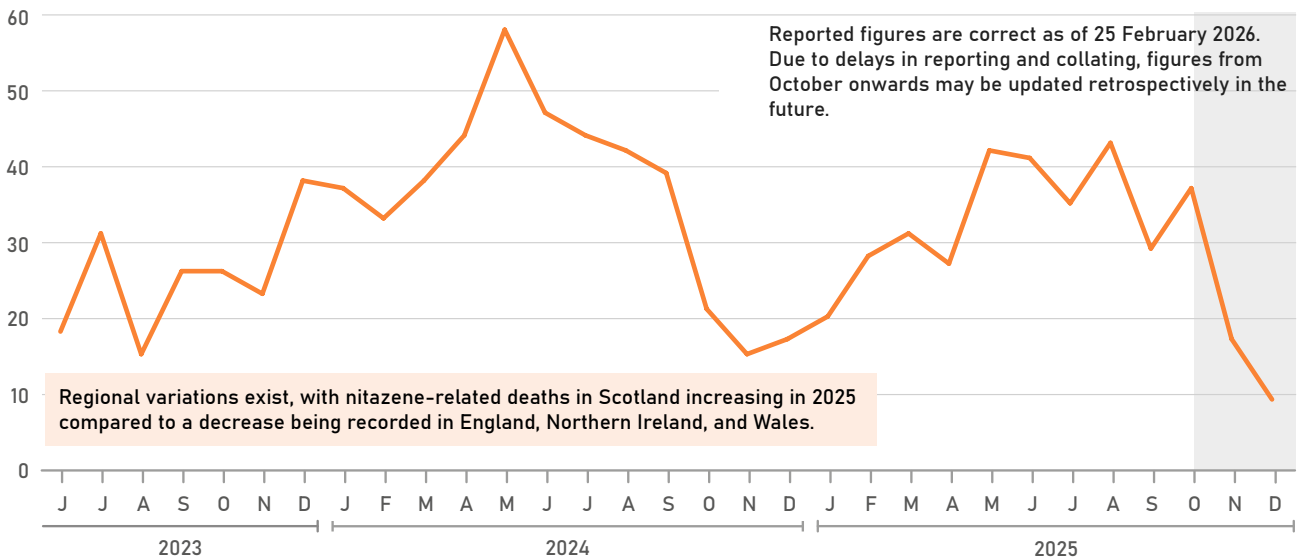
Case Study | First Cocaine Extraction Laboratory Discovered in the UK

In October 2024, two men were arrested following the search of a site in Vauxhall, London. Chemicals and equipment commonly used for cocaine extraction and conversion of cocaine base to cocaine hydrochloride were found and seized, as well as chemicals used for cocaine adulteration. Packaging and measuring equipment consistent with street-level sized deals was also found, alongside other evidence of street-level dealing.

This was a relatively small facility, with extraction yielding approximately 2.25kg of cocaine hydrochloride; however, it does represent the first discovery of an extraction laboratory in the UK. It is likely that drug organised crime groups are increasingly using chemical concealment as a method to hide drugs coming into the UK, and then using extraction facilities to produce the drugs for distribution.

Both men have pleaded guilty to conspiracy to supply Class A controlled drugs and producing a Class A controlled drug.

Drug-Related Deaths Involving Nitazenes



Source: National Crime Agency and Department of Health and Social Care. Drug-related deaths in which a nitazene was present reported to Project HOUSEBUILDER between June 2023 and December 2025; data confirmed as of 25 February 2026.

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

Serious and organised crime instils fear, undermines local businesses and services, erodes public trust, and diminishes community resilience.

SOC in Communities | Harm to Society

SOC affects communities in many ways. As well as harming individuals, it also impacts local businesses and public services, and undermines the wider economy. It damages property and infrastructure and harms the natural environment. SOC erodes public trust in institutions and government services, making communities feel less safe and less resilient.

Some SOC offenders use a wide range of businesses on the high street including barber shops, mini-markets, nail bars, and vape shops, to support their criminality. These types of businesses are used to facilitate a range of SOC-related activities including selling or otherwise distributing illicit goods, illegal working, and the laundering of funds. Many individuals are supporting and enabling SOC in communities, usually unwittingly, by supporting these high street businesses.

Fraud continues to have a substantial impact on the community, inflicting severe emotional and financial harm on victims, reducing economic output, and undermining government services. In addition to the personal harm caused, some types of fraud including online shopping fraud, ticket fraud, advance fee fraud, investment fraud, and rental frauds all have an impact on the wider community through lost economic output and reduced levels of investment.

Although individuals aged 30 to 39 years old submitted the highest number of reports, the greatest financial losses were from victims aged 50 to 59.

Some frauds involve criminals offending from within community spaces, often targeting vulnerable individuals and organisations. For instance, courier fraud involving bank cards or

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

jewellery is often enabled by urban street gangs who move these assets, in exchange for cash, to fund personal drug consumption.

Public sector fraud continues to act as a drain on additional investment in government and community services. In 2023 to 2024, the total tax gap was estimated by HM Revenue and Customs to be £46.8 billion, with the share of the gap due to criminality being 9% (£4.4 billion). Additionally, the Department for Work and Pensions reported £6.5 billion in fraud losses over the financial year ending 2025.

Organised acquisitive crime continues to undermine the safety and confidence of our communities. However, there was a 12% reduction in overall acquisitive crime offences in December 2025 (731,136) compared with 2024 (831,498), driven by decreases in organised retail crime, personal robbery, residential burglary, and vehicle crime offences. It is highly likely the response from law enforcement agencies and partners contributed to this reduction. Organised retail crime has also shown signs of stabilisation following a sharp increase in offences at the start of 2024.

The increase in renewable energy infrastructure requiring use of valuable materials, especially copper, is almost certainly driving acquisitive crime in this sector. Solar farms, wind turbines, and electric vehicle charging cables were all targeted by organised crime groups in 2025.

Organised crime groups engage in many types of waste crime, including illegal dumping, illegal waste exports, fraud, the operating of illegal waste sites, and tax-related offences. Organised crime groups involved in the waste sector are highly likely to be engaged in multiple additional crime types, including drugs and money laundering. More widely, the production, transport, disposal, and associated payments within waste management services are themselves a means for laundering the proceeds of crime.

Wildlife crime also remains a persistent threat: the UK has links to global smuggling networks associated with the illegal trade of parrots, reptiles, glass eels, birds of prey, and other CITES species.

SOC and Prisons

The imprisonment of offenders contributes to public safety by removing high-risk individuals from communities and supporting their rehabilitation. However, some SOC offenders continue influencing or directing criminal activity from within prison through illicit communications, corrupt staff, and associates operating in the community. Some offenders also likely increase their criminal capability while in prison by forming connections with more experienced individuals. These relationships provide networking opportunities and enable the exchange of knowledge and expertise.

The overall SOC threat within the prison system is likely to have remained broadly stable in 2025. However, the use of drones for smuggling contraband such as drugs, mobile phones, and weapons continues to be a growing threat to the safety and security of prison estates. Increases in reported drone incidents are likely due to cheaper and increasingly commercially available drone models, and heightened awareness of this tactic.

SOC nominals almost certainly play a role in illicit drug supply within prisons, driving addiction and sustaining a criminal economy that can lead to violence and extortion. Prisoners with a drug addiction often reoffend after leaving prison. There continues to be a significant threat from psychoactive substances, especially synthetic cannabinoid receptor agonists, entering the prison

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

establishment. Smaller quantities of these substances are required, making them easier to conceal.

Rival organised crime group members are almost certainly involved in acts of violence and retaliation within UK prisons with incidents typically originating from drug-related disputes or gang-based grievances. Disputes in the community are known to impact on the prison estate, often in relation to disputes relating to finances, drug supply, territory, or personal vendettas. Most incidents of prisoner-on-staff violence are not related to SOC activity; however, threats of violence towards prison officers or against their families is a commonly used method of corruption used by prisoners.

SOC and Social Cohesion

SOC creates fear and uncertainty in our communities which can undermine trust and confidence in UK law enforcement and other local institutions. It is likely that high-profile violent incidents and firearms threats, despite being relatively rare, attract disproportionate attention and create a heightened perception of danger within communities. The visibility of criminal activity associated with an increasing number of irregular small boat arrivals amplifies social tensions.

Domestic Bribery and Corruption

Criminal networks continue to use bribery and corruption to facilitate their activities, including the use of professional enablers in both the public and private sectors. The Home Office's Economic Crime Survey 2024 found that 1 in 35 businesses with employees in the UK (3%) had encountered a bribery incident in the previous 12 months.

It is likely that one of the areas of the public sector most at risk of corruption is local government, although this could be partly due to local councils being one of the most visible and accessible sectors for corruption to be identified by the public and/or having mechanisms in place for corruption to be identified internally. Individuals working in other public sector roles, including government, law enforcement, prisons, logistics, and at the UK border, are also vulnerable to corruption, including targeting by organised crime groups. There are indications that other business sectors also hold a particular corruption risk but further insight and analysis is needed to fully understand the threat.

Insiders in UK and international organisations continue to be sought and used by cybercriminals to gain access to organisations to deploy ransomware or to engage in other cybercrime activities.

Case Study | Operation MACHINIZE | High Street SOC

During 2025, the NCA established Operation MACHINIZE, the largest operation of its kind, focused on illicit finance and grey economy activity linked to high street businesses.

Working in partnership with the National Police Chiefs' Council across two intensifications, the operational response involved every UK police force and Regional Organised Crime Unit, Home Office Immigration

Domains > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

Enforcement, Trading Standards, HM Revenue and Customs, and Companies House.

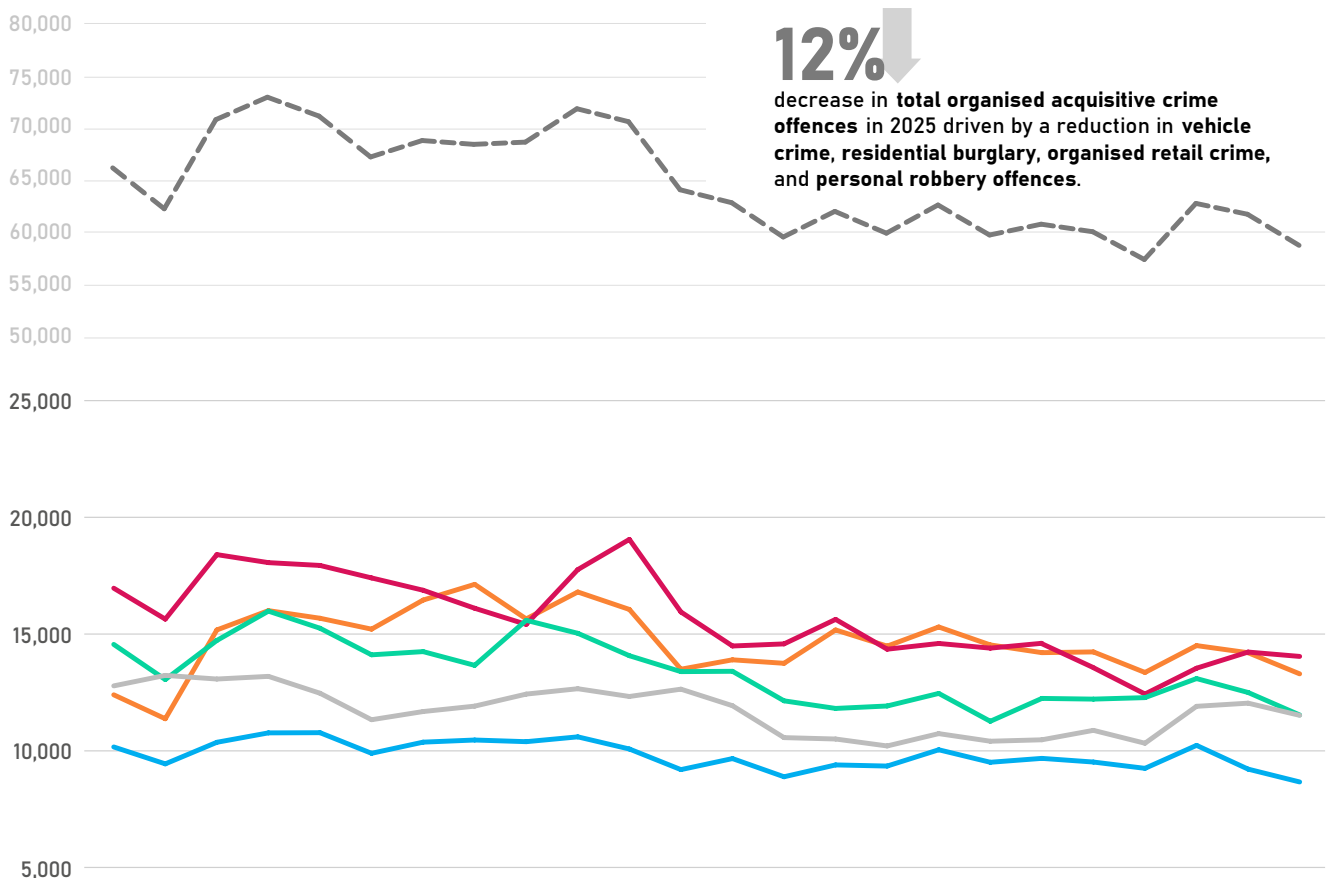
Over the two intensifications, the partnership delivered:

- 2,999 premises visited and raided
- 959 individuals arrested
- Freezing orders over bank accounts totalling more than £1 million
- 55 individuals questioned about their immigration status and 97 people safeguarded in relation to potential modern slavery
- Over £10.7 million of suspected criminal proceeds seized
- Over £2.7 million worth of illicit commodities destroyed

Organised Acquisitive Crime Offences by Crime Type

- Personal Robbery and Theft From the Person
- Theft From Motor Vehicle
- Organised Retail Crime
- Residential Burglary
- Theft of Motor Vehicle
- Total OAC Offences

Infrastructure and Metal Crime figures (Solar, Electric Vehicle, and Cable) are lower (<90) and are therefore not shown.



Domains > SOC in Communities: Harm to Individuals & Harm to Society | SOC at the Border | Transnational SOC | SOC Online: Online Harms & Online Enablers | SOC Finance

The overall risk from serious and organised crime at the border likely increased, driven by small boat activity and increased volume and sophistication of drug trafficking.



SOC at the Border

It is likely that the overall SOC threat to the UK posed by organised crime groups taking advantage of, or overcoming, border controls has increased in 2025, driven by an increase in small boats, which is the principal organised immigration crime threat to this area, and an increase in sophistication and volume of drug imports in 2025 compared with 2024.

A range of SOC offending impacting on the UK has to transit the border, and there are similarities in modes of transit used for different types of SOC, including drug trafficking, the outbound movement of cash, human trafficking, and people smuggling. However, it is highly likely that these modes of offending are distinct, involving separate organised crime groups who are not heavily interrelated.

Smuggling of criminally-generated cash and listed assets across the UK border is carried out by individuals and networks often with the aim of concealing the illicit origins of the funds and placing them in a formal financial system overseas. This ensures that organised crime groups can continue funding the predicate criminal activity and also benefit from the profits.

The Sea Border | Small Boats

41,472 migrants arrived in the UK via small boats in 2025, a 13% increase on 2024 (36,816). This increase is highly likely enabled by organised crime groups adapting to improve profits; capitalising on an increase in demand from Horn of Africa migrants, widely adopting the taxi boat method, and increasing the number of passengers per boat. Use of other methods of organised immigration crime entry almost certainly either remained stable or decreased over the same period.

The most prominent migrant nationalities arriving in small boats in 2025 were Afghan, Eritrean, Iranian, Somali, and Sudanese. An increase in demand from Horn of Africa migrants was a

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

key theme of 2025, and almost certainly driven by a combination of push factors from source countries (such as conflict and political instability) and secondary migration from mainland Europe.

In 2025, organised crime groups further evolved their launch tactics to avoid detection and capitalise on favourable crossing conditions. This included extensive use of the taxi boat method and overcrowding. The average number of passengers per boat reaching the UK was 62 in 2025, compared with 53 in 2024. This meant that the higher number of migrant arrivals was achieved with fewer small boats arriving in the UK in 2025 (672), compared with 2024 (695).

2025 saw fewer migrant fatalities in the English Channel (27) compared with 2024 (78), highly likely due to intervention by rescue craft, alongside fewer incidents of groups of non-paying passengers opportunistically storming boats in the water, causing panic and instances of crushing or drowning. In order to prevent opportunistic boarding, organised crime groups increasingly catered to lower-paying nationalities in 2025, almost certainly contributing to lower estimated average crossing prices compared with 2024.

It is highly likely that law enforcement activity has contributed towards an upwards trend in small boat equipment costs since 2023. The equipment used for small boat crossings is typically sourced from China and then assembled in Turkey, before being stored in Germany and transported to northern France. Organised crime groups almost certainly tested new supply routes in 2025 to avoid controls at the Bulgaria/Turkey border.

The Sea Border | Other Maritime SOC

While it is highly likely that maritime threats to the UK on container shipping and roll-on/roll-off modes remained stable in 2025, it is highly likely that UK organised crime groups have enhanced at-sea cocaine exchange capabilities since 2023.

A small number of organised crime groups use general maritime vessels to smuggle cocaine, firearms, and people such as organised crime group members, associates, or those willing to pay more for passage, into the UK. People and commodities are highly unlikely to be smuggled in the same vessel.

It is highly likely that organised crime groups using the container shipping mode to smuggle cocaine have diversified their methodology. This includes using alternative European ports, enhanced concealments, and at-sea-drop-offs in response to high volumes of upstream seizures in recent years.

Confirmed illegality of some top-venting blank firers, which had previously been legally sold as being UK-specification, reduced firearms availability in 2025. This has likely contributed to established organised crime groups seeking to increase importations of firearms and ammunition; it is highly likely that organised crime groups favour tried and tested routes, modes, and methodologies.

Domains > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

It is likely that the threat to the UK sea border from clandestine irregular migration via roll-on/roll-off and general maritime reduced in 2025. Detections of irregular migrants at UK ports and in country continued a multi-year decrease in 2025. During 2025, there were 1,998 recorded detections of irregular arrivals to the UK at UK ports or subsequently detected in the UK, a 36% decrease compared to 2024, which saw 3,125. While the method is covert in nature and some events will go undetected, there is no indication numbers have increased.

It is highly likely that cocaine importations to the UK via at-sea-drop-offs or coopering are mainly organised by loose consortiums of transnational organised crime groups in joint ventures with South American brokers and suppliers. A joined-up operating model for cocaine shipments presents opportunities for organised crime groups to source, and resource, large-scale importations directly from South America.

The Air Border

It is likely that the threat to the UK border from abuse of air routes, particularly from the importation of cannabis, increased in 2025. Overall seizures of cannabis in the year ending March 2025 totalled 127 tonnes, a 71% increase from the 74.2 tonnes seized the previous year, though levels of seizure stabilised through the rest of 2025. This cannabis is mainly from North America and Thailand and arrives in fast parcels and post, as well as air passenger and air freight modes.

It is likely that the overall scale of irregular migration via air in 2025 is comparable to 2024. During 2025, there were 3,027 detected irregular arrivals to the UK via inadequately documented air arrivals, a decrease of 10% compared with 3,349 during 2024.

Case Study | Disrupting Firearms Trafficking

In May 2025, Border Force located 61 counterfeit firearms concealed beneath floor panelling of a vehicle (pictured) at the Port of Dover.

The driver, a 44-year-old Polish male, received a nine-year custodial sentence for attempting to smuggle the firearms into the UK in September.

Working together, the NCA and Border Force prevented this large quantity of firearms from entering the hands of organised crime groups, which would have strengthened their capability to inflict violence, intimidate communities, and undermine local resilience.

The Threat from Non-Canalised Traffic to the UK

Canalised traffic refers to scheduled commercial and passenger services that pass through immigration on arrival.

Non-canalised traffic refers to private maritime and aviation traffic that does not pass through immigration on arrival in the UK (also known as general maritime and general aviation).

Non-canalised traffic avoids controls making it much more challenging to detect and tackle. It needs proactive resource to identify it.



Domains > SOC in Communities: Harm to Individuals & Harm to Society | SOC at the Border | Transnational SOC | SOC Online: Online Harms & Online Enablers | SOC Finance

Organised crime groups collaborate in cooperative networks to traffic larger shipments, share risk, and reduce the impact of losses.



Transnational SOC

Globally, the threat from transnational SOC continues to grow, posing a significant threat to local communities and nation states. The majority of SOC impacting on the UK likely has some direct or indirect overseas links; for example, most illicit drugs sold in the UK are imported from abroad. Trends and emerging threats which first appear overseas can often become evident in the UK as the highly interconnected nature of global SOC sees criminal methodologies and illicit commodities spread quickly throughout the world.

The globalised and interconnected nature of SOC means any changes to national policies and legislation made in one jurisdiction will have a rapid impact in other countries as transnational organised crime groups adapt and exploit new opportunities. Examples include organised crime groups responding at speed to the decriminalisation of cannabis in Thailand, and elsewhere, in order to supply the UK; the growth of opium cultivation in Pakistan following the Taliban's ban on narcotics production in Afghanistan; and the tightening of asylum policies and legislation in mainland Europe pushing larger numbers of people to attempt irregular entry to other countries including the UK.

Adaptability of Commodity Flows | Cocaine Routes

In 2025, the clearest shift in global supply chains is evidenced in changes in the cocaine supply chain as organised crime groups utilise new routes and methods (such as the use of semi-submersible submarines and chemical concealment of cocaine) and exploit new opportunities presented by organised crime group collaboration and technology. Production and consumption of cocaine have never been higher, and pricing has never been lower. Cocaine trafficking drives violence, corruption, and instability along the supply routes. The number of drug-related deaths in the UK linked to cocaine use has increased for the 12th consecutive year.

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

It is highly likely organised crime groups importing cocaine are increasingly collaborating globally as a large cooperative network to traffic larger shipments of cocaine into Europe and the UK, share transportation networks and risk, and minimise the impact of losses. Multi-tonne shipments and groupage loads are increasingly common.

It is highly likely Western Balkan organised crime groups retain the highest level of control over the end-to-end supply of cocaine (importations and wholesale distribution) from source countries to the UK's streets. Their development of direct relationships with South American cartels enables them to buy cocaine at wholesale prices then resell in Europe and the UK at high profit margins.

Growing legitimate trade links between Brazil and West Africa have provided organised crime groups with greater opportunities to use commercial and container shipping modes to smuggle cocaine across the Atlantic and on to Europe and the UK. Sustained investment in maritime infrastructure in West Africa has boosted connectivity.

Western Balkan organised crime groups operate throughout West Africa, collaborating with Brazilian organised crime groups to facilitate multi-tonne cocaine shipments. They have embedded brokers in West African countries who organise logistics, establish infrastructure and liaise with local actors including corrupt law enforcement and port operators.

Exploitation of Conflict, Instability, and Weak Governance

Conflicts in the Middle East, Myanmar, Sudan, and Ukraine, as well as post-conflict transitions in countries such as Afghanistan and Syria, terrorist insurgencies across Africa, and high levels of SOC-related violence in Latin America are all contributing towards geopolitical vulnerabilities which offer new criminal opportunities to organised crime groups.

It is highly likely that opportunities for organised crime groups to innovate, network, and capitalise on global vulnerabilities are increasing. Areas of instability, weak governance, or conflict provide fertile ground for exploitation by SOC offenders. Such areas commonly lack fully functioning law enforcement to combat SOC and are instead characterised by state dysfunction, partnerships between conflict actors and criminals, high levels of corruption, and dependence on grey or illicit economies in which SOC thrives.

The spread of fraud compounds in areas of South East Asia is a recent example of how organised crime groups exploit areas affected by conflict and subsequent weak governance. Once the template is established, it can be replicated elsewhere and grow into a significant global threat largely unhindered by law enforcement. The civil war in Myanmar in particular was exploited by organised crime groups taking advantage of the corruption and lawlessness found in areas of conflict, targeting locations which are geographically remote and less likely to draw political or law enforcement attention. The phenomenon has now spread far beyond the region.

Global instability as a result of conflict, economic disparity, or natural disasters is a primary driver of transnational organised immigration crime. The resulting irregular migration drives demand for the services of organised crime groups who profit from smuggling vulnerable people across national borders. Data relating to the nationalities of irregular migrants most commonly entering the UK confirms the link between instability and organised immigration crime.

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

The Threat from State Actors Harnessing SOC Threats

It is highly likely that some foreign states, including Iran and Russia, have sought the assistance of criminals or organised criminals to pursue their state strategic objectives. These states also continue to be permissive of SOC activity which supports their objectives and is conducted from within their jurisdictions. For example, ransomware-enabling services operate from countries such as Iran and Russia, which are uncooperative to Western law enforcement, and this makes disruption more problematic.

It is highly likely that plausible deniability is the principal rationale for these states harnessing SOC to pursue their strategic objectives. The intent behind this activity varies, including using crime to support state finances, evade sanctions, intimidate dissidents, and subvert government authority domestically through hybrid threat vectors such as irregular migration and sabotage.

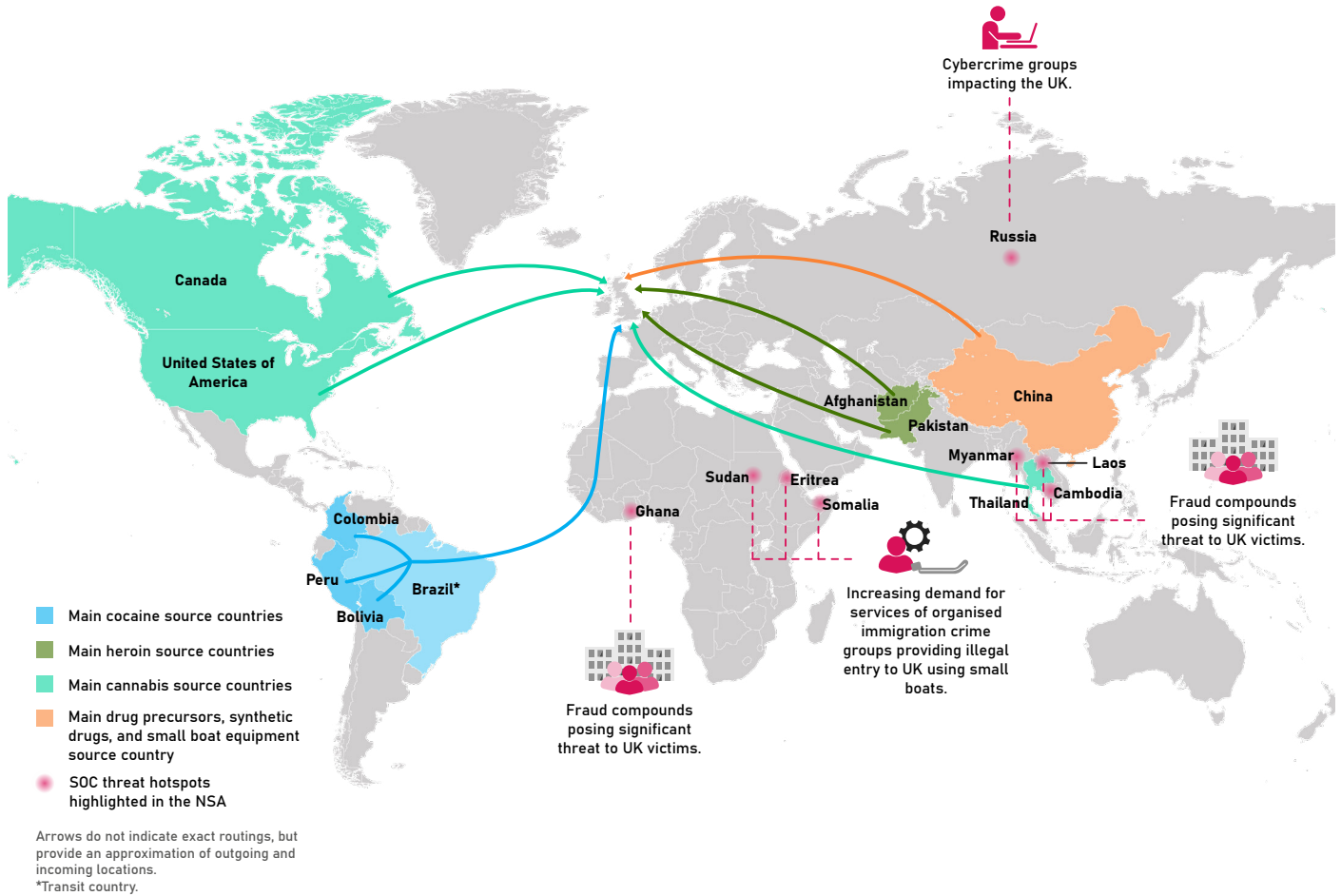
Case Study | Romance Fraud in West Africa

In 2025, a Nigerian fraud organised crime group was identified basing their criminal activities in Ghana using forced labour. One operation discovered a huge modern slavery and human trafficking ring in which over 200 people had been trafficked into a compound where they were forced to carry out romance fraud against victims worldwide.

Victims were forced to work in appalling conditions on only one meal per day. The trafficked individuals were mostly young Nigerian males who had been recruited in Nigeria with the promise of lucrative work. The leaders of the organised crime group were based in Nigeria, and money was transferred to, and laundered by, individuals in Nigeria. Whilst the use of forced or coerced labour to commit fraud has been seen sporadically, its use on this scale is more commonly linked with South East Asian or Chinese organised crime groups.

This operation was initiated in response to a referral into the 'Report Sakawa' line – an NCA fraud media campaign launched in collaboration with Ghana's Economic Organised Crime Office and the British High Commission in Accra, encouraging members of the public in Ghana to anonymously report suspicious activity. Online fraud centres using human trafficking victims are a growing trend, causing harm to victims across the world and the NCA is committed to tackling the organised crime groups responsible.

Transnational SOC Threats to the UK



Domains > SOC in Communities: Harm to Individuals & Harm to Society | SOC at the Border | Transnational SOC | SOC Online: Online Harms & Online Enablers | SOC Finance

As online dependence grows, opportunities for criminal exploitation expand, enabling higher-volume harm to people and organisations.

SOC Online | Online Harms

The increasing reliance on the internet to manage social, economic, and business operations is almost certainly expanding opportunities for the criminal exploitation and infiltration of online infrastructure. Increasing public and business resilience is crucial for mitigating SOC threats to the public.

The use of social engineering increases offenders' capability to coerce, deceive, and extort individual victims and organisations online. User-to-user networking platforms facilitate mass discoverability, allow unmoderated and/or encrypted private messaging, and use algorithms to encourage connections and to generate engagement. This enables offenders to locate, identify, and connect with victims, and exploit their online data and personal information.

Online offenders are increasingly capable of identifying and targeting victims across a range of criminal threats, with individuals and networks identified operating across child sexual abuse, cybercrime, and fraud, targeting both individuals and organisations. It is almost certain that the motivations for offending are also increasingly diverse, with factors such as notoriety and status driving the participation of young offenders in online networks where offending and harm is perpetrated. It is highly likely that the gamification of offending within such networks enables offenders to distance themselves from the harms and consequences of their actions.

Interpersonal Harms

Women and children are disproportionately impacted by sexually motivated online offending. Online-facilitated child sexual abuse now accounts for at least 42% of recorded child sexual abuse offences in England and Wales. In 2025, the Child Sexual Abuse and Exploitation Referrals Bureau received over 92,000 referrals from online platforms, representing a 31% increase on the previous two years.

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

Offenders target both children and non-consenting adults, operating as individuals, or in online networks to share and sell illegal sexual content online, and in some cases organise and coordinate sexual offending offline.

Offenders use the online environment to cause sexual, physical, and mental harm to victims remotely, which likely decreases offenders' inhibitions and increases the severity of offending. Offenders exploit poverty abroad, paying for child sexual abuse to be produced and livestreamed. Victims worldwide are also groomed, coerced, and extorted to record and share self-generated indecent imagery of sexual acts, acts of self-harm, and/or harm to others. This can often involve escalatory demands to engage in increasingly harmful activity, and offenders may also make demands to meet victims offline, placing them at risk of contact offending.

It is likely that children are increasingly being financially incentivised to produce self-generated indecent imagery, mirroring online influencers on adult sites such as OnlyFans. Whilst almost certainly less common than the scale of grooming or coercion by offenders, this is almost certainly under-identified.

Male victims are almost certainly more susceptible to, and are more commonly victims of, financially motivated sexual extortion. Offenders engage both adult and child victims in the UK. Reports of financially motivated sexual extortion impacting children under 18 increased between 2024 and 2025; it is highly likely media campaigns to raise awareness of the issue have contributed to an increase in reporting. Where financially motivated sexual extortion activities target children, it is highly unlikely that this is as result of a sexual interest in children by these offenders, but rather children's vulnerability to this model of offending.

Child sexual abuse offenders identify and target children on popular online networking and communication, livestreaming, and gaming platforms. Over the last three quarters of 2025, the Child Exploitation and Online Protection Centre received approximately 500 reports per month, a 50% increase driven primarily by increases in financially motivated sexual extortion and online grooming. Features of online platforms that increase the risk of children being targeted by offenders and exposed to harmful material, trends, and behaviours include:

- lacking effective moderation processes and/or requiring limited sign-up information;
- allowing discoverability of children via public profiles and friend suggestions;
- providing seamless movement between public and closed messaging spaces, particularly where those messaging services are end-to-end encrypted and allow private interactions between children and unknown adults;

Domains > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

- hosting unverified and/or unmoderated user-generated gaming and content; and
- featuring [algorithms](#) and/or chatbots that promote potentially harmful content, and reinforce potentially harmful user inputs and interests.

Implementation of the [Online Safety Act 2023](#) requires providers to remove **illegal content**, provide highly effective age assurance, and consider how algorithms impact children's exposure to harmful content. Online platforms' adoption of the Act's requirements are likely to embed and mature over the next 12 months, impacting offender capabilities to target children online and reducing children's exposure to harmful content. However, this is dependent on platforms successfully implementing and demonstrating safety by design at scale.

Offenders use social media platforms and classified advertising websites to offer UK employment opportunities, recruiting potential victims of modern slavery and human trafficking in source countries into sexual and labour exploitation, domestic servitude, and exploitation in criminal activity. Victims are commonly deceived about the nature of the work they will be required to undertake, and the terms and conditions under which they will be forced to work.

Financial Harm to Individuals and Organisations

The online ecosystem provides tools, products, and services that allow offenders to target victims at scale for online and offline fraudulent activity. Fraud-enabling products include compromised datasets, [phishing kits](#), malware, one-time password interception tools, [scripts](#), and tutorials for cybercrime offences.

Although incidents submitted to Report Fraud in 2025 peaked in both July and October, there is no evidence of a substantial change in the overall threat. Monthly reports later declined from October onwards and returned back to the scale identified at the beginning of 2025. However, growing levels of card-not-present and investment fraud are being facilitated by online environments. Criminals exploit online advertisements to help them target large numbers of individuals, which is likely to be a factor behind rising investment fraud losses. Additionally, compromised data purchased from online marketplaces is increasingly being monetised via card-not-present fraud, with cases rising by 22% from 1.36 to 1.66 million during the first half of 2025 compared to the first half of 2024, according to UK Finance.

Ransomware remains the highest-harm serious and organised cybercrime threat impacting the UK, and the impact on organisations has been well documented in the UK in 2025. Successful ransomware attacks impacting Collins Aerospace, Co-op, Jaguar Land Rover, and Marks & Spencer demonstrate both the financial cost to businesses of ransomware deployments, and, also, the impact on the day-to-day lives of British citizens, including customers, workers in the supply chain, and the wider economy and tax base. Reporting estimates a cost to the UK economy of £1.9 billion, including a tangible impact on UK gross domestic product from the Jaguar Land Rover attack, which is estimated to be the costliest ransomware attack ever in the UK.

Cybercriminals from English-speaking nations, including the UK, have been involved in attacks that used social engineering techniques to gain access to victims' credentials and systems, where their native use of the English language and understanding of their victims gives them an advantage. They have also made use of different forms of ransomware, demonstrating their use of tools developed by other cybercriminals.

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

Artificial Intelligence

The increased functionality, scale, and development of artificial intelligence tools and their adoption by offenders continues to enhance and enable SOC. Generative artificial intelligence imagery is increasingly realistic and indistinguishable from real imagery, and is being used to produce child sexual abuse material. Artificial intelligence-generated false documentation has been identified being used to circumvent identity checks, facilitating fraud, money laundering, and organised immigration crime offending.

In 2025, the Internet Watch Foundation identified 312,030 reports where analysts confirmed the presence of child sexual abuse material. This is a 7% increase on the 291,730 reports in 2024, with increasing levels of photo-realistic artificial intelligence-generated child abuse imagery contributing to this rise. Of 3,440 artificial intelligence videos of child sexual abuse discovered by the Internet Watch Foundation in 2025, 65% (2,230) were categorised as Category A, suggesting a trend towards artificial intelligence-generated child sexual abuse material being more extreme.

The use of artificial intelligence automation and translation tools is reducing language barriers, increasing opportunities for victim targeting, and making it easier for organised crime groups to collaborate internationally. The expansion of victim pools via the use of translation tools and better-quality scripts reduces victims' ability to recognise and identify fraudulent activity, increasing the likelihood that offenders will be able to socially engineer and extract victim data and credentials. The use of artificial intelligence to automate fraudulent emails enables offenders to tailor content at scale, helping to bypass filters designed to detect malicious communications. There continue to be incremental improvements in the abilities displayed by artificial intelligence-generated malware.

Case Study | The Sanctuary | Disrupting Online Child Sexual Exploitation

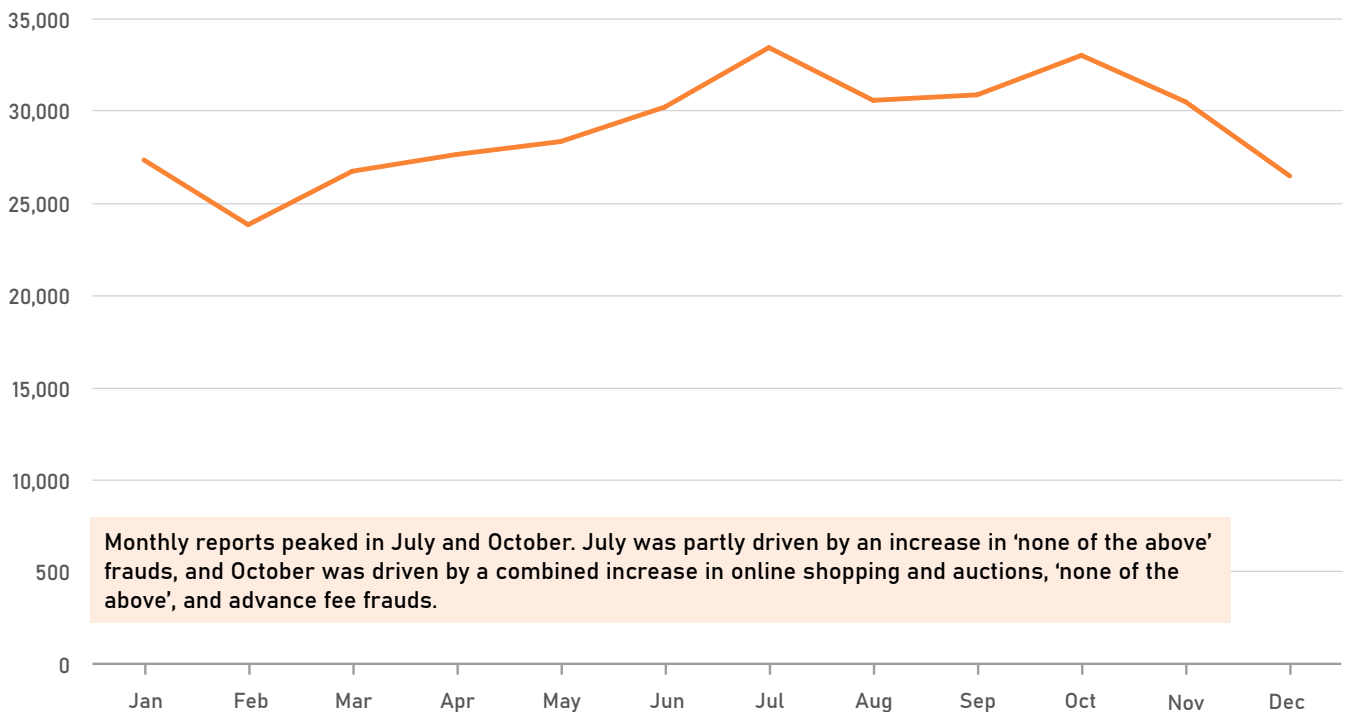
Following the launch of an investigation by the United States of America's Federal Bureau of Investigation into a private online messaging forum dedicated to the sexual exploitation of children named 'The Sanctuary', a UK-based IT worker, Robert Chown (49), was identified as a key contributor. From his home in South London, Chown masqueraded as a teenage boy online to target thousands of children worldwide, coercing them to engage in being filmed or photographed committing non-consensual sexual acts.

Girls and boys as young as six years old were groomed by Chown to livestream sexual acts at his instruction, which he would capture and share with other paedophiles on 'The Sanctuary' and the dark web. He went on to share hundreds of abuse images in the forum that he'd captured over years of sexually exploiting children online. Chown also posted an indecent photo of a 12-year-old girl that he had taken in person, who was subsequently identified and safeguarded by the NCA and child protection services. Investigators seized two mobile devices, and found over 2,000 indecent images and videos of children in categories A to C. They also discovered 204 entries into Google Translate of sexual instructions translated from English into Russian and Polish.

Domains > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

Following an NCA investigation, Chown was sentenced to 25 years, with seven to be served on licence, having pleaded guilty to 41 charges at a previous court hearing. Chown was also handed a lifetime Sexual Harm Prevention Order and will be on the sex offenders register for the rest of his life.

Fraud Incidents Submitted to Report Fraud in 2025



Source: Report Fraud. Service changed from Action Fraud to Report Fraud in December 2025.

Domains > SOC in Communities: [Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)



The same platforms that connect people also connect criminals. Online spaces enable victim targeting, illicit advertising, and offender networking.

SOC Online | Online Enablers

Shifts in the way online spaces are used and structured are influencing offender behaviour and enabling new forms of criminal activity. The increasing use of online platforms to facilitate daily living continues to expand the influence and role of online enablers in SOC. This is reducing barriers to offending and enhancing offender capabilities.

Online criminality crosses international and jurisdictional boundaries, providing offenders with access to victims on a global scale. The international nexus of online offending, combined with obfuscation and encryption in online environments, creates difficulties determining the origin and scale of SOC threats. It is increasingly difficult to determine whether offenders are operating individually, in loosely or highly organised groups, or occasionally as state-proxies.

The audience reach, accessibility, perceived anonymity, and abundance of information available online makes popular online networking and communication platforms attractive to offenders, providing an ideal medium for:

- victim identification and targeting;
- advertising illicit goods and services; and
- offender networking, research, planning, and upskilling.

Offenders demonstrate a sophisticated understanding of victim and customer targeting opportunities online. Typically, popular networking platforms act as the initial medium for identification and contact between offenders, victims, and/or customers. Further engagement often occurs via an application's private chat function, or secure messaging applications, which are often end-to-end encrypted, and perceived to offer greater privacy and security.

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

It is likely that [platform algorithms](#) play a significant and increasing role in facilitating SOC. Algorithms increase reach by connecting audiences with criminal service providers, and radicalise and connect offenders through the reinforcement, normalisation, and signposting of harmful interests and behaviours.

Offenders employ tradecraft to obscure their online activities from law enforcement, such as the use of virtual private networks and other IP obfuscation technologies. Platforms with limited controls, particularly those that do not require identifiable data to register accounts, have weak or no moderation capabilities, and platforms that are based in challenging jurisdictions are also attractive to offenders seeking to obscure their activities from law enforcement.

[Tor](#) remains the primary system used by offenders in 2025 to access the dark web, which is used to buy and sell illicit goods and services, for offender-offender networking, and viewing and exchanging child sexual abuse material. It is highly likely that Tor use by offenders has decreased in 2025, with the enhanced accessibility and functionality of clear web platforms driving a reduction in offender reliance on the dark web. Many clear web platforms now have end-to-end encryption as standard, require less technical knowledge to access and use, are more stable, and are used legitimately by millions.

Online Advertisements and Criminal Marketplaces

Illicit online marketplaces and advertisements on both the clear and dark web continue to facilitate the purchase of individual and wholesale quantities of illicit goods and services, increasing the profitability of organised crime group operations through the expansion of audience reach. Offenders demonstrate a good understanding of how to maximise platform features to increase audience engagement and sales.

It is likely that social media enabled the facilitation of at least 33,000 irregular migrants entering the UK via small boats in 2025. An estimated 80% of migrants facilitated via small boats used social media to locate an agent or communicate with an agent working as part of an organised crime group at some stage in their journey. Organised immigration crime facilitators and fraudulent document suppliers use online platforms to provide further instructions, such as tactics to avoid detection, logistics, transport details, and meeting points for migrants.

It is likely that online adverts and marketplaces facilitate the sale of a growing proportion of illicit goods and services in line with wider societal trends in online purchasing. Illicit marketplaces continue to offer child sexual abuse material, drugs, firearms, and stolen goods. Illegal substances and prescription-only medication such as benzodiazepines, cannabis, cocaine, GHB, heroin, ketamine, methamphetamine, and opioids have all been identified for sale in online drugs marketplaces.

Cybercrime and fraud-enabling tools such as ransomware and malware strains, compromised credentials, stolen datasets, and phishing kits purchased from Tor marketplaces and clear web platforms, facilitate the financial exploitation of individuals and organisations. Adverts featuring fraud-enabling products are increasingly being identified on Telegram channels.

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

Online spaces also facilitate the advertisement of services of victims of modern slavery and human trafficking, particularly adult services websites, which enable sexual exploitation.

Offender Networking and Upskilling

Online spaces encourage like-minded individuals to identify and connect with each other. This is exploited by offenders to create spaces dedicated to illegal shared interests such as child sexual abuse, which highly likely contributes to the normalisation of sexual offending against children and encourages offending.

Networking and communication platforms enhance offender capabilities through the online crowdsourcing of knowledge and tradecraft. Clear and dark web networking sites, message boards, and forums facilitate offender networking and upskilling across SOC, enabling a small number of capable and influential offenders to cause disproportionate harm. These offenders use their technical knowledge and capabilities to offend, and either share their knowledge or provide their services to other offenders. This accelerates the pace of uptake, adaptation, and innovation in SOC offending, and encourages the convergence of offending across SOC threats.

Online platforms are used by offenders to portray 'easy money' and a glamorous lifestyle to recruit others into offending. Cash and other high-value items are displayed to entice individuals to engage in criminal activity such as county lines offending, drug and illicit cash smuggling, money muling, and violence-as-a-service.

Case Study | Dark Web Vendor Account Dismantled

In November 2025, Steven Parker (52), from Norfolk, was sentenced to six-and-a-half years' imprisonment for his role as operator of the dark web illicit marketplace Dark Market Soldiers Next Day Delivery. Parker ran the marketplace from his home, using it to supply controlled drugs over a period of several years.

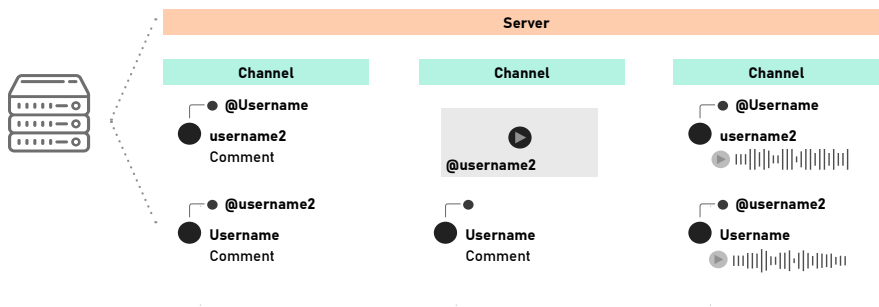
The marketplace offered drugs including heroin, ecstasy, amphetamines, diazepam, Xanax (alprazolam), and cannabis. Parker managed and controlled the operation and his then partner, Louise Daniels, provided logistical support and was later convicted of money laundering.

The investigation was led by the Eastern Regional Serious Special Operations Unit, through its specialist cyber capability, working alongside colleagues in police forces across the eastern region. This case illustrates the growing role of online marketplaces in providing offenders with direct access to customers and a scalable model for distributing illicit commodities.

Online Environment Enabling SOC Offending

Online platforms enhance the capabilities of offenders by enabling networking, recruiting, offending, and sharing of information and ideas.

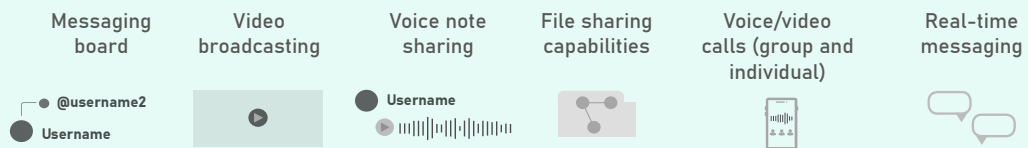
Networking platforms have attractive community building features:




Servers are virtual spaces that people can join to interact with other users with similar interests. These can be user-created.

Channels or groups can be within a server. They are virtual spaces used to discuss specific topics. They can be private and invite-only.

The combination of features within these spaces enable users to identify other offenders and share knowledge and tradecraft, and identify and interact seamlessly with victims:



Domains > SOC in Communities: [Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)



Organised crime groups often outsource money laundering to dedicated networks, taking advantage of their specialist capabilities and connections, whilst also distancing themselves from the illicit funds to spread detection risks.

SOC Finance

Most SOC is conducted for financial gain, and the UK remains an attractive location for the laundering of proceeds of crime (both those generated in the UK and overseas). Money laundering enables SOC to benefit from profits and reinvest illicit funds into criminal activity, whilst attempting to avoid law enforcement detection.

The use of technological and professional enablers has remained prominent in the facilitation of SOC finance impacting the UK during 2025.

Many organised crime groups outsource the money laundering aspect of their operating model to dedicated networks that generate profits from providing these services. Reasons for outsourcing money laundering activity include the complexities of the laundering process required, access to enabling services, and organised crime groups spreading the risk of detection by distancing themselves from the illicit funds.

Methods

Criminals continue to use UK corporate structures in a variety of ways to conduct fraud and illicit finance activity. Legislative changes, in particular Companies House reforms as a result of the [Economic Crime and Corporate Transparency Act 2023](#), aim to reduce the accessibility of some well-established illicit finance methods, which rely on abuse of the UK register of companies. Companies House reforms during 2025 and 2026 include the introduction of [mandatory ID verification](#), [authorised corporate service providers](#), and an increase in [filing fees](#). The full impact of these changes on the illicit finance threat has not yet been assessed.

It is highly likely that action by the UK and other cooperative jurisdictions to disrupt illicit finance and sanctions evasion activity on some crypto exchanges and currencies has led to displacement of this activity to other platforms in Russia or Russia-aligned nations. The UK and

Domains > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

United States of America have sanctioned a number of Russia-linked cryptocurrency exchanges including Garantex and Grinex. Tether has also frozen millions of US dollars worth of [stablecoin](#) cryptocurrency USDT, held in Garantex-linked cryptocurrency wallets.

Cryptoassets have maintained their reputation for price volatility, but between March and October 2025 leading cryptocurrencies reported all-time high values, which likely increased public willingness to invest. It is highly likely the public perception of there being profits to be made from investing in cryptocurrency is a key factor driving losses associated with investment fraud. UK Finance data shows that losses during the first half of 2025 increased by 55% to £97.7 million compared to the same period in 2024 (£63.0 million).

The purchasing of UK-based property remains an attractive investment for criminals involved in a wide range of SOC activities partly due to the large amounts of money that can be moved and the stability of property as an asset.

UK property and related services firms have almost certainly acted as professional enablers for individuals designated under UK sanctions ([designated persons](#)), thus facilitating sanctions breaches. It is highly likely that designated persons, particularly Russian, have used intricate layers of ownership to distribute their wealth by placing property and related assets under the ownership and control of their family members.

It is highly likely that the significant increase in the price of gold, particularly from August 2025 and continuing into early 2026, has increased the attractiveness of this commodity for a variety of criminal activities impacting the UK, such as money laundering and courier fraud. The UK remains vulnerable to the use of its gold market for illicit purposes for reasons including the significant volume of international trade in precious metals through London, the universal acceptance of gold as a global currency, and the lack of regulation and supervision of the recycled market.

Networks

Chinese-speaking money laundering networks continue to offer a service to UK-based criminals. It is almost certain that Western Balkan organised crime groups use Chinese-speaking money laundering networks, as well as [international controller networks](#), to transfer funds to South America, including to pay for drugs at source. Cash can be collected in the UK and the value paid out in Europe and South America.

[Operation DESTABILISE](#) continues to build understanding of Russian-speaking money laundering networks. Russian-speaking money laundering networks service a broad range of clients, creating a mutually beneficial service for transnational organised crime groups involved in a range of predicate crimes, Russian elites, and hostile state-linked entities to bypass the traditional financial sector to move illicit funds and evade sanctions. They broker transactions overseas, instructing coordinators to collect, consolidate, and convert criminal cash into cryptocurrency, facilitated by their access to sanctioned cryptocurrency exchanges and high-impact Russian cybercrime groups. Demand for Russian-speaking money laundering network

[Domains](#) > [SOC in Communities: Harm to Individuals & Harm to Society](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online: Online Harms & Online Enablers](#) | [SOC Finance](#)

services has almost certainly been accelerated by the increased use of cryptocurrency in SOC, the war in Ukraine, and subsequent sanctions against Russian entities, creating a market for the obfuscation of Russian-origin funds and their integration into Western financial systems and assets.

Despite some networks and enablers still using a variety of methods to launder Russian-linked funds, it is likely that sanctions, legislative reforms, and reduced access to investment opportunities and professional enabler services continue to make the UK a challenging environment for Russian elites.

High-impact criminal daigou networks highly likely use corrupt and/or negligent insiders within regulated professional services and high-end retailers. Although daigou activity has previously been characterised as frequently cash-intensive, it is likely that non-cash methods are now more frequently used than cash. These include goods being purchased in-store or online in pounds sterling using payment cards and gift cards (including e-gift cards), as well as using money held in Chinese accounts and accessed by shoppers instore using Chinese-registered mobile phones.

Market Abuse

It is highly likely that the threat to the UK financial system presented by market abuse increased in 2025. Whilst insider trading conducted by organised crime groups has persisted throughout the year, the threat in the form of 'pump and dump' trading of company stocks and shares has notably increased. Individuals based outside of the UK operating organised trading groups use social media and articles on bogus financial news websites to spread disinformation, impacting the share price of a chosen product. This activity has a significant negative impact on the integrity of the UK financial market, where confidence and trust in the UK economy is weakened. The threat presented by pump and dump schemes will almost certainly increase in the next year or two due to the increasing use of artificial intelligence.

Throughout 2025, the Financial Conduct Authority observed insider dealing organised crime groups, who are involved in SOC, trading on the UK financial market. Insider dealing organised crime groups have continued to favour the financial products offered by the UK market such as equity spread bets and contracts for difference. This, combined with the leveraged access to world markets, makes the UK a hub for global insider dealing.

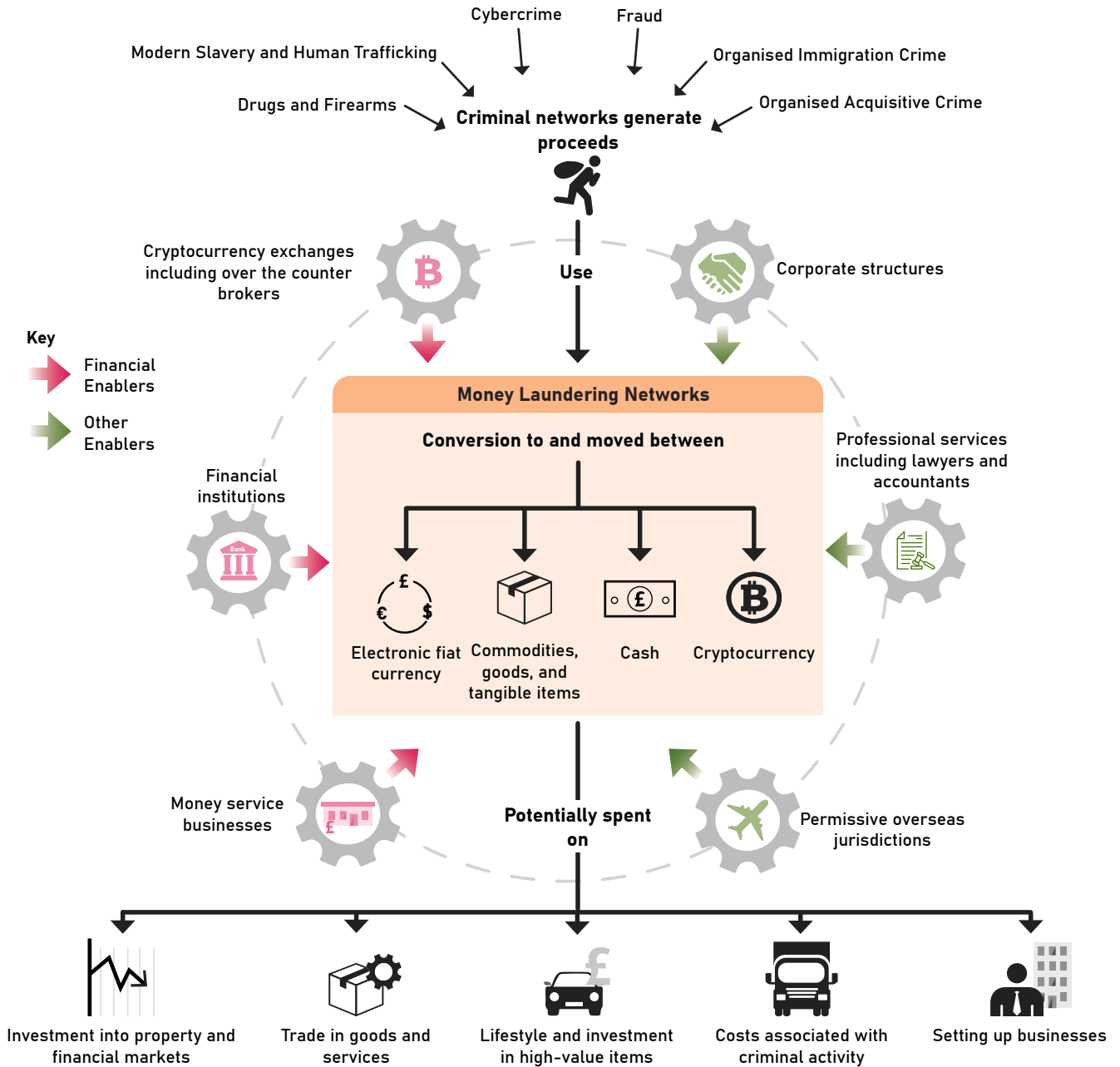
Case Study | Investigating Russian-Speaking Money Launderers

Since 2022, the NCA has led Operation DESTABILISE, an investigation targeting Russian-speaking professional money laundering networks impacting on the UK. These networks are responsible for laundering tens of billions of dollars globally to service a variety of SOC groups and upstream threat actors. This activity led to 129 arrests and over £25 million seized in cash and cryptocurrency in the UK (plus additional overseas seizures).

The operation has exposed the connection between money laundering on UK streets and the Russian state. Individuals associated with the Russian intelligence services attempted to use one UK-linked network to fund individuals including the leader of a Bulgarian network convicted of running a spying operation across Europe for Russia. Another UK-linked network purchased a Kyrgyzstan bank to facilitate sanctions evasion and payments supporting Russian military efforts.

Domains > SOC in Communities: Harm to Individuals & Harm to Society | SOC at the Border | Transnational SOC | SOC Online: Online Harms & Online Enablers | SOC Finance

Use of Global Money Laundering Networks in SOC



Tackling the Threat >

[SOC in Communities](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online](#) | [SOC Finance](#)

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



Tackling the Threat

SOC continues to pose a persistent and damaging threat to the UK. Criminal networks have further diversified their activity, expanded their reach, and increased their use of technology to enable offending. These developments have widened the impact of SOC on communities, public services, businesses, and the UK economy.

The NCA leads the national response, working with law enforcement, government, international partners, and the private sector to reduce harm and target those offenders who pose the greatest risk. This response is delivered through the UK's SOC system, a network of more than 75 organisations across law enforcement, government, the intelligence community, regulatory bodies, local authorities, and international agencies, supported by academic and private sector partners. Together, this system provides the reach, capability, and coordination required to protect the public from serious and organised crime.

In 2025 and into 2026, we continued to prioritise the most serious offenders across child sexual abuse, cybercrime, drug supply, firearms, fraud, illicit finance, and organised immigration crime. Joint operations delivered significant disruptions, removing dangerous individuals from the UK's communities, protecting vulnerable people, and degrading the capabilities of organised crime groups operating within the UK and overseas.

Technology continues to reshape SOC. Criminal groups are increasingly using online platforms, encrypted communication, and artificial intelligence-enabled tools to identify victims, outsource capability, and scale their activity. The NCA has strengthened its technical and analytical capabilities to identify offenders earlier, exploit digital evidence more effectively, and support policing with specialist expertise. We have expanded partnership working with technology companies to improve safety, reduce illegal content, and increase the UK's ability to counter online harm.

Tackling the Threat >

[SOC in Communities](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online](#) | [SOC Finance](#)

We have also focused on enhancing the UK's defences against illicit finance. Criminals are exploiting global financial systems, professional enablers, and specialist money laundering networks to conceal proceeds of crime. The NCA continues to work with domestic and international partners to identify, trace, freeze, and seize criminal assets, and to target those who provide money laundering services to high-harm networks. Implementation of Companies House reforms and increased use of financial disruption tools have strengthened our response.

At the border, the NCA has targeted organised immigration crime groups facilitating dangerous small boat crossings, alongside offenders moving drugs, firearms, and cash into and out of the UK. Our international network continues to work with partners upstream to prevent harmful commodities reaching the UK and to identify emerging trafficking routes.

Our activity also focused on protecting communities from harm caused by drug supply, violence, and exploitation. We continued to support policing to tackle high-harm gangs, safeguard vulnerable children exploited in online environments and criminal networks, and address threats associated with synthetic opioids, ketamine, and other substances.

SOC continues to evolve, driven by technology, global instability, and interconnected criminal markets. The NCA will continue to lead the national effort to identify and assess these changes, coordinate the response across the system, and deliver sustained disruption against those offenders who cause the greatest harm to the UK.

Our Response to the Threat

SOC in Communities



Drones | Digital Forensics Links Multiple Prison Flights to a Single Operator

In September 2024, Greater Manchester Police recovered a drone and a package containing drugs and other contraband in woodland near HMP Manchester. Digital examination linked the drone to multiple flights into HMP Feltham, HMP High Down, and HMP Manchester in the preceding months. Further enquiries led to the arrest of Mohammed Sharif (22) at a Birmingham address, where a second drone was seized.

The investigation began with Greater Manchester Police before being passed to the North West Regional Organised Crime Unit for further enquiries and additional charges. Sharif was convicted of possession of cannabis and multiple counts of conveying illicit articles into prisons, and was sentenced on 05 November 2025 to six years' imprisonment.

This case highlights the growing role of commercially accessible drone technology in enabling prison contraband supply and increasing risk to prison safety and control.

Tackling the Threat >

[SOC in Communities](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online](#) | [SOC Finance](#)

Operation ALLIANCES 2 | National Vehicle Crime Week Delivers Mass Disruption

In October 2025, policing partners across England and Wales ran Operation ALLIANCES 2, a Home Office-funded intensification week targeting vehicle crime and associated organised criminality. Activity across 37 forces focused on offenders linked to theft, dismantling networks and 'chop shops', reflecting the multi-agency response required where acquisitive crime intersects with wider SOC.

The operation delivered the following outcomes:

- More than 350 arrests (many assessed as linked to SOC)
- More than 400 stolen vehicles recovered (estimated value £3 million)
- More than 1,000 vehicle parts recovered (valued in excess of £13 million)
- More than 20 chop shops closed, including the largest ever identified in the UK
- Seizures included over £150,000 in cash and plant machinery worth more than £800,000

The operation demonstrates that organised acquisitive crime is rarely isolated from wider offending. At one chop shop, officers uncovered a cannabis factory, weapons, controlled drugs, and approximately 60 vehicle number plates suspected to have been used to evade law enforcement detection. Arrests have also covered potential modern slavery and immigration crime offences.

Blank-Firers to Firearms | Conversion Kit Seizure Leads to Eight-Year Sentence

An investigation began after information indicated specialist equipment used to manufacture ammunition had been ordered and delivered to an address in Birmingham. On 28 January 2025, officers arrested Banaras Malang (33) and searched his home address, recovering nine Turkish-manufactured top-venting blank-firers alongside equipment consistent with converting them into live-firing weapons, plus parts and ammunition-making equipment. The orders had been made using the bank card and address of a vulnerable man who Malang had taken advantage of.

Although the weapons were sold as blank-firers, the case proceeded on the basis that the models were readily convertible. Malang was convicted at Birmingham Crown Court and was sentenced on 04 December 2025 to eight years' imprisonment for possession of those firearms.

This case underlines how enforcement pressure and availability shifts can influence firearms sourcing, and how offenders may exploit vulnerabilities to procure specialist equipment.

Shatter Supply Chain Targeted | £120,000 Extractor Kits Seized with Illicit Vapes

On 13 October 2025, officers and partners visited premises suspected of supplying industrial equipment linked to a cannabis shatter laboratory discovered in the north east of England. Working with Trading Standards, teams entered and inspected the premises and seized significant quantities of apparatus, including extractor kits commonly used in shatter production.

Tackling the Threat >

[SOC in Communities](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online](#) | [SOC Finance](#)

The seized equipment was assessed to have been imported from China and to be non-compliant with UK safety standards. Two vans of items were seized, with an estimated £120,000 placed on the sale value of the extractor kits. Officers also seized more than 5,000 illicit vapes stored at the address, valued at around £40,000.

Shatter is a highly concentrated cannabis extract. Illicit drugs laboratories pose an inherent risk to the public, both from exposure to harmful substances, the potential for explosions, and the harm caused to the environment by waste products. In October 2024, an explosion at a house in Newcastle, which led to two deaths, was linked to an explosion of gas canisters used in cannabis extraction.

This case illustrates how domestic drug production can be enabled by specialist equipment and supply chains, increasing safety risks and co-locating wider illicit commodities in community settings.

SOC at the Border



£42 Million Cocaine Seizure in East Yorkshire

NCA officers disrupted an organised crime group attempting to import 524kg of cocaine (valued at £42 million) using a rigid-hulled inflatable boat. The group, which included Colombian national Didier Tordecilla Reyes, used a boat launched to collect the consignment and land it on a beach in the UK, before transferring multiple bags into a hire van.

Coordinated activity by the NCA, supported by Humberside Police and Border Force, enabled officers to intercept the group, recover the drugs, and evidence Reyes' role as a facilitator linked to Colombian cartel contacts. Reyes was jailed in September 2025.

This disruption highlights the continuing diversification in cocaine importation routes and methodologies, including small boat maritime tactics.

Tackling the Threat >

[SOC in Communities](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online](#) | [SOC Finance](#)

English Channel Smuggling Supply Chain Disruption: Boat and Engine Supplier Jailed in Belgium

A joint operation between the NCA and Belgian authorities led to the conviction of Adem Savaş, identified as a key supplier of boats and outboard engines to people smuggling networks operating in the English Channel. Operating under the cover of a legitimate maritime supply business, he sourced engines from China and moved boats and equipment via Turkey, Bulgaria, and Germany before supplying networks in Belgium and France.

Savaş was detained at Schiphol Airport, Netherlands, in November 2024 and extradited to Belgium. In December 2025, he admitted offences relating to people smuggling and membership of an organised crime group and was sentenced to 11 years' imprisonment and fined €400,000. Three co-defendants received sentences totalling 38 years.

The NCA identified Savaş during its investigation into Hewa Rahimpur, the head of a major Europe-wide smuggling network responsible for moving more than 10,000 migrants in small boat crossings to the UK. The case reinforces the impact of targeting enabling infrastructure (boats, engines, and logistics) internationally to degrade organised immigration crime capability.

Project HIDE | Strengthening the UK's Capability to Detect Criminal Concealments

In 2025, Project HIDE expanded the UK's understanding of concealment techniques used by organised crime groups, assessing around 100 new examples and contributing to a national dataset of 874 cases shared across law enforcement. The intelligence enabled the development of specialist training delivered to more than 3,200 officers in the UK and overseas, directly contributing to multiple seizures, arrests, and prosecutions linked to improved detection of hidden illicit goods.

Project HIDE's data has also been used to identify operational barriers, including the previous inability to seize vehicles containing empty concealments. Evidence presented by the project supported a major legislative change in the Border Security, Asylum and Immigration Act 2025, which now criminalises concealments in vehicles, vessels, and aircraft.

The project continues to track emerging concealment trends. In 2025, two heavy goods vehicles were intercepted at the UK border with fuel tank concealments containing significant quantities of cocaine, indicating the resurgence of a historic smuggling technique.

Tackling the Threat >

[SOC in Communities](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online](#) | [SOC Finance](#)

Transnational SOC



EncroChat Firearms Brokerage | International Coordination Dismantles Cross-Border Supply

An NCA investigation disrupted a high-harm firearms supply network run by an offender using the EncroChat handle 'Aceprespect', who advertised a catalogue of automatic and semi-automatic weapons to UK organised crime groups. Working from abroad, he marketed weapons including AK-47s, Skorpion, and Uzi machine guns, pistols, and ammunition, arranging for firearms to be smuggled into the UK and transferred via a Warrington-based associate.

NCA officers deployed with the Spanish National Police to arrest him in Malaga, leading to extradition. In 2025, the offenders admitted firearms offences and a conspiracy to inflict grievous bodily harm after plotting an acid attack, receiving custodial sentences of 26 years 8 months, and 11 years 4 months respectively.

This investigation shows how secure communications and cross-border logistics enable firearms brokerage at scale, and why international cooperation is central to disruption.

Livestreaming Child Sexual Abuse | UK Offender Jailed for Commissioning Overseas Abuse

An NCA investigation found that Patrick Howlett (58), from Kent, sent almost £56,000 to known child-abuse facilitators in the Philippines to commission livestreamed child sexual abuse over several years. Intelligence showed he maintained regular contact with a woman who abused her own children at his direction, producing and sending him images and videos in exchange for payment. Investigators recovered 14,311 illegal images, including more than 5,000 created specifically for him; the offending spanned from 2003 until his arrest in 2021.

Working with law enforcement partners in the Philippines, the NCA identified 19 child victims who were safeguarded. Howlett pleaded guilty in January 2025 and was sentenced on 18 July 2025 at Canterbury Crown Court to 26 years' imprisonment.

This case illustrates the transnational nature of online-enabled child sexual abuse, where communications and payments allow offenders to generate direct harm remotely while increasing safeguarding demands.

Tackling the Threat >

[SOC in Communities](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online](#) | [SOC Finance](#)

International Collaboration to Disrupt Organised Fraud

In 2025 and 2026, activity to disrupt organised fraud demonstrated the value of cross-border intelligence sharing and operational coordination.

In July 2025, the India Central Bureau of Investigation raided a fraudulent call centre in Uttar Pradesh, resulting in multiple arrests. This followed collaboration and intelligence sharing between the Central Bureau of Investigation, the NCA, the United States of America's Federal Bureau of Investigation, and Microsoft to identify the organised crime group, build a case, and target the complex IT infrastructure used by the criminals. Over 100 UK victims had been contacted, with total losses over £390,000.

In January 2026, the NCA supported the Nigerian Police Force to take down a fraud centre. Using intelligence from Meta, an address was identified and raided within days, resulting in several arrests. Police enquiries found the centre was conducting a range of operations including investment fraud, romance fraud, and financially motivated sexual extortion targeting the UK and United States of America.

Wider, multi-country disruption activity was also delivered through Operation SERENGETI 2.0, a UK-supported, Interpol-coordinated operation. This resulted in the arrest of over 1,200 criminals across Africa, targeting nearly 88,000 victims and the recovery of \$97.4 million. Investigators from the UK and 18 African countries worked together to tackle high-harm, high-impact crimes including investment fraud, business email compromise, and ransomware. Private sector partners strengthened the operation by providing intelligence, guidance, and training to help investigators act on intelligence and effectively identify offenders.

SOC Online



Telegram Com Forum Disrupted Following NCA Investigation into Large-Scale Online Coercion

Offenders exploit encrypted and anonymised platforms to mobilise Com networks that crowdsource coercion, blackmail, and distribution of abuse at scale. In one NCA case, Bradley Talbot (29), from Portsmouth, acted as a moderator within one such group of around 6,000 members on Telegram that targeted children, made demands for indecent images, and weaponised threats of exposure to force further compliance. The investigation identified more than 100 child victims, with at least a quarter believed to be UK-based.

Talbot pleaded guilty on 29 April 2025 to offences including participating in the criminal activities of an organised crime group, arranging or facilitating the sexual exploitation of a child under 13, and distributing an indecent image. He was sentenced to seven years and six months' imprisonment and received a lifetime Sexual Harm Prevention Order.

This case demonstrates how networked online ecosystems can scale harm rapidly, requiring fused intelligence and safeguarding responses across jurisdictions.

Tackling the Threat >

[SOC in Communities](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online](#) | [SOC Finance](#)

Joint Intelligence Cell Tackles Harms Associated with Online Forums Through Early Intervention and Safeguarding

In 2025, the NCA and partners created a joint intelligence cell to counter the global threat posed by individuals using online forums to share extreme material designed to cause harm and distress to young female victims. These forums are used to coerce victims into serious abuse, self-harm, and other harmful acts, including, in some cases, taking their own lives. Often adolescent boys, this subculture also engages in cybercrime and the sharing of extreme terrorist, racist, and nihilistic ideologies, often with a fascination with violence.

The cell has brought together the NCA, police, and Counter Terrorism Policing in the UK, alongside international partners amongst the Five Eyes community and Europol to deliver a worldwide coherent law enforcement response. Between establishment in October 2025 and March 2026, the cell received 540 referrals from industry, and international and domestic policing partners. To date, 14 arrests have resulted in the UK, 21 vulnerable individuals have been safeguarded, and 337 investigations have been instigated both in the UK and overseas supported by the cell.

In many cases, parents were unaware of the harmful online activity affecting their children at home, and some children indicated an intention to continue offending or to continue participating in coerced harms despite interventions, reinforcing the need for a broader public health approach to the threat.

Cyber Prevent | Early Support Linked to Lower Reoffending

The National Cyber Prevent Referral Mechanism provides a UK-wide process to assess and manage people at risk of engaging in cybercrime offending.

An evaluation of 1,041 referrals, made between December 2017 and April 2025, found that, although some people did go on to reoffend, reoffending rates (for cyber offences and for all crime) were around half those seen in comparable groups who did not go through the programme. Wider research suggests youth diversion schemes typically deliver more modest reductions in reoffending, making these findings comparatively strong. The results support the NCA's wider prevention offer, including Cyber Choices, which helps young people understand the law and use their digital skills safely, reducing the future supply of cyber offenders alongside operational disruption.

The UK's cybercrime threat landscape continues to evolve, requiring a coordinated system response that not only disrupts offenders but also prevents individuals from entering or escalating within cyber-dependent criminality. Cyber Prevent plays a central role in this preventative effort, aiming to intervene early and divert individuals away from a cybercriminal pathway through targeted, risk-based engagement.

Tackling the Threat >

[SOC in Communities](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online](#) | [SOC Finance](#)

'Logged Out' | Record Takedowns of Organised Immigration Crime-Linked Social Media Accounts in 2025

During 2025, the NCA led a record year of takedowns of social media accounts linked to people smuggling, with 10,700 accounts closed. Since late 2021, more than 27,000 accounts have been taken down; over 2024 and 2025 more than 90% of accounts referred by the NCA were removed by platforms.

The activity included proactive scanning and referral of potentially criminal content, while also generating crucial investigative leads. In one case, a man was detained by NCA investigators on suspicion of offering crossings from Libya to Italy on Facebook, and three individuals were arrested for offering fraudulent visas and illegal entry into the UK in posts on TikTok.

This activity demonstrates the scale at which online platforms can be used to market organised immigration crime services and how account disruption can be paired with intelligence development to support investigations.

SOC Finance



Prince Group Sanctions | Coordinated Designations and Asset Freezes Target Overseas-Linked Harm

In October 2025, the UK announced designations under the Global Human Rights Regulations against the Prince Group founder and network, after government research triggered by media allegations linking them to fraud compounds, trafficking, fraud, and money laundering.

The Prince Group is one of Cambodia's largest conglomerates, running a multi-billion pound business across real estate, construction, banking, and retail. Media reporting has alleged criminal involvement by the Prince Group and its founder, Chen Zhi, in scam compounds, including human trafficking, fraud, money laundering, and human rights abuses.

The UK designations were announced in October 2025, alongside similar sanctions by the United States of America, with parallel action being taken by UK and United States law enforcement on the same day. The NCA and Isle of Man Constabulary froze £100 million in assets and executed search warrants at UK and Isle of Man properties, including a 70-room mansion in Regent's Park, London. The United States Department of Justice also unsealed an indictment against Chen Zhi, in which prosecutors seized \$15 billion in Bitcoin.

This activity highlights how illicit finance linked to overseas harms can involve UK-based assets, and the value of coordinated international disruption using sanctions and enforcement tools.

Tackling the Threat >

[SOC in Communities](#) | [SOC at the Border](#) | [Transnational SOC](#) | [SOC Online](#) | [SOC Finance](#)

Pay As You Go SIM Diversion | Cross-Sector Data Sharing Disrupts One-Time Password-Enabled Fraud Pathways

Pay As You Go SIM cards are increasingly being taken in bulk from UK retail supply chains and used to support large-scale fraud. Instead of being used for normal calls, they are used to receive one-time passwords. Criminals use these to set up social media or messaging accounts that appear to be based in the UK. Even when telecoms companies disconnect the SIM numbers for breaking their terms of service, the online accounts that were set up using those SIMs often stay live and are then reused for harmful activity.

Stop Scams UK has been bringing together companies in affected sectors so they can work on this problem jointly. By sharing data on blocked SIMs through Stop Scams UK, members can spot and take down fraudulent accounts, because a SIM being blocked for breaking terms is a strong indicator of fraud risk. This illustrates how tackling a technical enabler through cross-sector collaboration can reduce fraud at scale, and underpins the announcement of a new multi-agency Online Crime Centre in March 2026.

International law enforcement, industry, and regulators have brought their expertise together through Stop Scams UK and the National Economic Crime Centre to understand how widespread this weakness is. The focus is on matching data to support account takedowns and collecting feedback. As the work develops, it will bring in more industry partners and continue a whole-system approach, mapping the networks involved and making policy changes that make SIM activation harder to abuse, closing the gaps criminals use to defraud UK consumers.

Aviation Parts Fraud: Forged Airworthiness Documentation Exposes Supply Chain Assurance Risks

In December 2025, the Serious Fraud Office secured the conviction of Jose Alejandro Zamora Yrala, director of UK-based aircraft parts trader AOG Technics, following a global fraud involving the sale of aircraft engine parts with forged Authorised Release Certificates. The business, operated from a home office in Surrey, sold more than 60,000 parts accompanied by forged documentation that purported to guarantee airworthiness leading to an estimated £39.3 million in losses.

The fraud came to light in 2023 when a routine authenticity check with manufacturer Safran identified a forged certificate, triggering safety alerts across the UK, United States of America, and European Union, and grounding aircraft worldwide. Zamora generated £7.7 million in revenue between 2019 and 2023. Zamora pleaded guilty to fraudulent trading and was sentenced to four years eight months' imprisonment.

This prosecution highlights how sophisticated fraud can damage safety-critical supply chains and impose high economic and institutional harms beyond direct financial loss.