OCTOBER 2024

SOPHIE DAVIS
CATRINA BOMFORD
LAURA BRITTON
ALEXANDER IOSAD

A New Approach to Serious and Organised Crime in the UK

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Contents

3 Executive Summary

8 The Rising Threat From Serious and Organised Crime

27 A New Approach to Tackling SOC

58 Conclusion

59 Methodology

Our Future of Britain initiative sets out a policy agenda for governing in the age of AI. This series focuses on how to deliver radical-yet-practical solutions for this new era of invention and innovation – concrete plans to reimagine the state for the 21st century, with technology as the driving force.

01

Executive Summary

Serious and organised crime (SOC) is now assessed by the government to affect more people, more often, than any other national-security threat.[1] While overall crime figures have fallen over the past decade, the National Crime Agency (NCA) states that the scale and harm from SOC has increased.[2] In total, SOC is estimated to cost the United Kingdom an eye-watering £47 billion every year.[3]

The threat is evolving rapidly across a range of categories. Fraud has risen at an exponential rate, and now makes up about 40 per cent of all crime.[4] Reported incidents of modern slavery and human trafficking, driven in part by an improved awareness of the threat, have seen considerable increases. Drug-related crime is rising, driven by shifts in drug-trafficking dynamics and markets. Against a backdrop of cost-of-living increases and rising geopolitical instability, organised-crime groups (OCGs) are increasingly involved in economic crime and the exploitation of migrants, including refugees. And volumes of online crime, such as cyber-crime and child sexual abuse and exploitation, are growing rapidly.[5]

Organised criminals have proven to be highly adaptable, nimbly pivoting their business models and operations when confronting new restrictions and opportunities. They are developing new technical capabilities, and exploiting global conflicts and instability as well as the UK's own vulnerabilities and lack of resilience to SOC.

Polling by Deltapoll, commissioned by the Tony Blair Institute for Global Change for this paper, shows that the public has caught on to the scale and nature of the problem, with 88 per cent of respondents considering SOC to be a serious threat to the country as a whole. More than half of residents in the most deprived neighbourhoods say it is a serious problem where they live.

The national approach to SOC is not keeping pace with the scale and nature of the threat. The UK's intelligence capabilities and understanding of the threat are not good enough. Law enforcement and other agencies are not collaborating effectively to tackle a problem that crosses the boundaries separating police forces. Traditional approaches are ineffective because they are largely focused on the pursuit of known, often lower-level offenders and enforcement through the courts, rather than by limiting OCGs' ability to operate in the UK and targeting the enablers of organised crime. And while criminals have adopted new technology, the UK's take up of novel technical capabilities, such as the ability to better trace the flow of illicit finance through behavioural biometrics, remains underwhelming.

The UK needs a different approach. First and foremost, it needs to equip police forces with powers that are commensurate with the scale of the threat. Deltapoll's research, mentioned above, shows that the public believes the police should prioritise SOC and 84 per cent believe SOC should be treated as a threat comparable to terrorism.

Yet counterterrorism powers are more extensive than those available to combat SOC. The consensus opinion, including from the Independent Reviewer of Terrorism Legislation, is that on the whole these greater powers have been applied conscientiously.[6] They have been effective in countering terrorism by giving police forces the ability to investigate and generate better intelligence, disrupt the flow of people and money for criminal purposes, and restrict the ability of offenders to participate in criminal activity from behind bars or by moving abroad.

Similar powers, with a clear overarching framework and strong oversight, including the appointment of an Independent Reviewer of Serious and Organised Crime Legislation, should be introduced to provide UK police forces with the tools they need to respond effectively to SOC's growing threat.

More funding, policing and reliance on traditional criminal-justice pathways, such as arrests and convictions, on their own are not sufficient solutions to the problem posed by SOC. Introducing a SOC framework and new counterterrorism-style powers would enable police forces to gather better intelligence, including on individuals not previously identified as participating in SOC. This approach would strengthen measures to destabilise OCGs, disrupt the flow of illicit finance and increase the deterrent effect of prisons. It would also improve the ability of law-enforcement agencies to collaborate with international counterparts and tackle online and cross-border crime.

Alongside these measures, the UK needs to disrupt the enabling environment that allows SOC to flourish in the country. OCGs currently benefit from weaknesses in the UK's response to professional enablers, corrupt insiders, online and internet-enabled crime, and illicit finance.

The UK should also review the structure of police forces, to improve regional coordination and update their capabilities; this would raise them to match the sophisticated methods used by OCGs. The current policing model is ill suited to the cross-regional nature of SOC, lacking key specialist capabilities and adequate resourcing.

Effectively and rapidly tackling the threat of SOC is key to achieving the government's mission of creating safer streets for all. This report suggests three main lines of action to achieve this objective:

1. Treat SOC as a national-security threat, and tackle it using the powers

and resources commensurate to those used in counterterrorism as well as enhanced intelligence and foresight capability.

2. Strengthen the UK's infrastructure and legislative framework to disrupt criminal enablers, resources and tools.
3. Support law enforcement's ability to respond to SOC by updating structures and capabilities to fit the modern threat.

1. Treat SOC as a national-security threat

- Enhance the UK's intelligence capability by introducing a new National SOC Lab that would report to the Labour Party's "take back our streets" mission board.
- Establish a range of new counter-terror-style powers to tackle SOC.
- Unlock the benefits of technology by creating a SOC technology strategy and an Advanced Procurement Agency.
- Adequately finance the UK's response to SOC by instituting a dedicated SOC fund, drawn from recovered assets and savings made available due to reduced demand for police services and lower socioeconomic costs associated with organised crime.

2. Disrupt criminal enablers, resources and tools

- Target the enablers of SOC by launching a package of measures to increase executive accountability, as well as a new anti-corruption strategy.
- Limit criminals' ability to operate online by introducing measures to facilitate collaboration and data sharing with the private sector, and rolling out digital ID verification more widely.
- Tackle illicit finance by simplifying anti-money-laundering supervision, closing the loopholes in the UK's offshore financial centres and empowering Companies House to detect and prevent fraud.
- Recover more of the proceeds of crime by reforming the confiscation regime and introducing a Criminal Asset Recovery Board.
- Disincentivise organised immigration crime by:
    - opening safe and legal asylum routes that allow claims to be made from abroad
    - negotiating an agreement for the safe return of rejected asylum seekers with the European Union (EU), or selected EU countries

    - speeding up asylum-claims processing
    - leveraging digital ID to reduce the attractiveness of the UK's informal labour market

3. Bolster law enforcement's ability to respond

- Create a more coordinated and coherent law-enforcement structure by introducing:
    - a new SOC minister
    - a greater focus on SOC within the Labour Party's "take back our streets" mission
    - a powerful regional tier of policing
    - a UK-wide police force to tackle cross-border threats
- Enable policing to harness the power of artificial intelligence by:
    - prioritising the interoperability of police systems through radically reform of the IT-systems procurement process
    - developing a SOC computational twin
    - gaining UK membership of Prüm II

02 The Rising Threat From Serious and Organised Crime

Serious and organised crime (SOC) is defined as “individuals planning, coordinating and committing serious offences, whether individually, in groups and/or as part of transnational networks”. It encompasses a range of disparate offences – including child sexual abuse, modern slavery and human trafficking, organised immigration crime, illegal drugs, illegal firearms, organised acquisitive crime,[7] cyber-crime, fraud, money laundering, bribery, corruption and sanction evasion[8] – but as this paper shows, the tactics of offenders in all these areas of operation have much in common.

The scale of SOC and the issues it causes for society are colossal. The National Crime Agency (NCA)[9] estimates that there are more than 59,000 known SOC suspects in the UK. At least 6,000 offenders are estimated to be involved in the trafficking of people in the UK, while HM Prison and Probation Services (HMPPS) suggests that more than 10 per cent of the prison population and 3.9 per cent of those on probation as of December 2023 are involved in SOC.[10] Based on the latest available estimate (2020–21), there were 4,772 organised crime groups (OGCs) operating in the UK.[11]

Adjusting the latest available analysis for inflation, SOC costs the UK an eye-watering £47 billion every year.[12] The largest components of this cost are spent tackling drug supply (£26 billion), economic crime (£11 billion) and modern slavery (£3 billion).[13] The government has acknowledged that these figures are an underestimate, and yet has not produced an updated cost estimate since a 2019 publication reporting details from the 2015–16 financial year.[14] As well as the costs to society and individuals, the rise in SOC is shifting political priorities. The increase in the number of people being smuggled across borders and the impact of drug-related violence are driving illegal immigration and law and order up the agenda, with leaders of all persuasions strengthening their rhetoric in response.[15]

Criminals operating in SOC are highly adaptable; they are adept at exploiting geopolitical instability and technological advancement, as well as using insiders to facilitate and enable crime through bribery and corruption. SOC is difficult to tackle due to its inherently international nature and the regular criminal exploitation of vulnerable individuals to commit the most visible crimes, which shields those at the top of the chain from law-enforcement agencies.

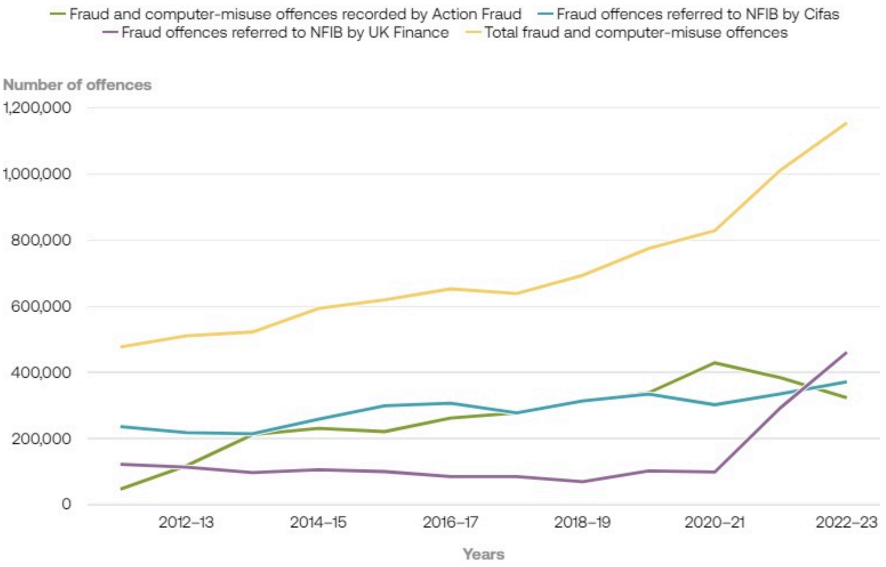
The Threat Posed by SOC Is Pervasive and Evolving

The threat from SOC is difficult to accurately measure and assess. It encompasses a multitude of offences, behaviours and criminal markets, many of which are, by their very nature, hidden. As with crime trends generally, it is often difficult to distinguish between genuine increases and the impact of greater awareness and/or improvements in recording practices. A number of these crimes are significantly underreported (for example, the Crime Survey for England and Wales suggests that only 13 per cent of frauds against individuals are reported to Action Fraud) and it can be challenging to estimate what proportion of other crimes is linked to SOC.[16] As a result, the UK's understanding of the SOC threat, and the markets that drive it, is not as comprehensive as it could be. Nevertheless, what is known points to a substantial threat that continues to grow and adapt.

Fraud has risen exponentially over the past decade and now accounts for an estimated 37 per cent of all crime in England and Wales.[17] Police-recorded fraud offences have increased by 128 per cent since 2012–13,[18] and while these figures are likely affected by changes in recording practices and fluctuations in the public's confidence when it comes to reporting incidents, the NCA estimates[19] that 86 per cent of instances of fraud currently go unreported. Estimates from the Crime Survey for England and Wales[20] found that there were 3.2 million fraud offences in the year ending September 2023,[21] with £2.46 billion lost by businesses and individuals to fraud in 2021–22, an increase of 17 per cent from the previous year. Fraud increasingly occurs online, classified as computer-misuse offences.[22] The NCA suggests that inflation and the cost-of-living crisis have increased the vulnerability of potential fraud victims and those recruited as money mules, as people attempt to save and make money.

FIGURE 1

Fraud and computer-misuse offences



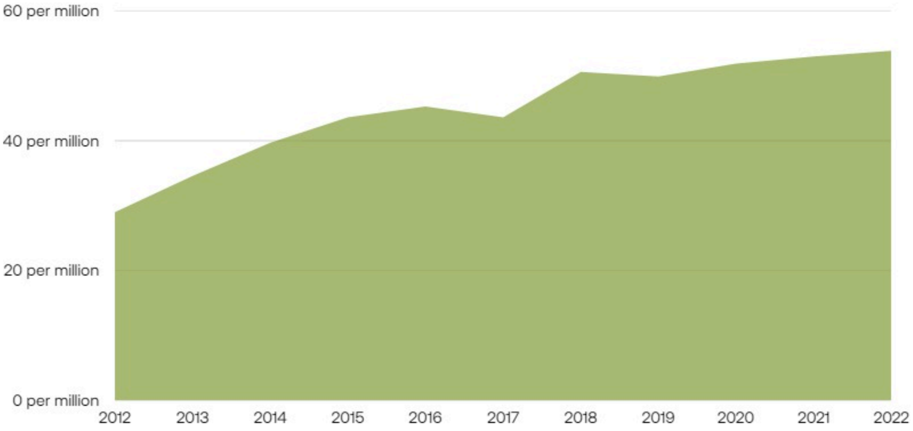
Note: Years in this chart span from April to March

Source: Home Office

Drug-related crime has also seen significant increases. The rate of deaths due to drugs[23] has risen from 29 per 1,000,000 people in 2012 to 53.9 in 2022, while homicide cases involving drugs increased by 36 per cent over the same period. Heroin[24] and crack cocaine[25] (the markets that account for most drug-related costs[26] to society) have seen a boost in production over the past decade,[27] as well as an increase in purity and falling prices;[28] this indicates that supply is plentiful. At the same time, trafficking dynamics and markets have shifted. The rise of technology has facilitated the growth of web-enabled transactions, often used in tandem with postal and parcel services to traffic drugs. In the UK, county lines (drug dealing by violent OCGs operating between large cities and smaller towns, using phones to conduct business and often involving the exploitation of children and vulnerable people) have expanded,[29] supplying towns and cities across the UK with heroin and crack cocaine. The past decade has seen an explosion in the manufacture of synthetic illegal drugs, benefiting from a cheaper and easier method of production and readily available chemicals.[30] Europol concludes that synthetic-drug production is becoming more sophisticated, distribution networks are nimbler and smarter, and the drugs themselves have become more harmful.[31]

FIGURE 2

Deaths due to drug misuse, rate per million people



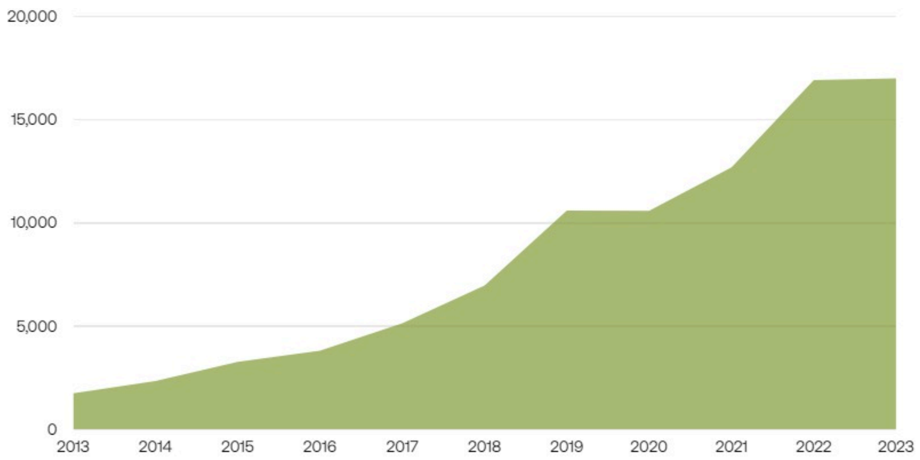
Source: Office for National Statistics

Organised immigration crime has started to rise rapidly in recent years, adding to the threat. Trends in organised immigration crime reflect rising geopolitical instability and the growing use of social media to advertise dangerous and costly border crossings. The number of people attempting to enter the UK via small boats has increased dramatically in recent years, from 299 in 2018 to 29,437 in 2023 (peaking at 45,774 in 2022).[32] The monthly average number of people per boat is also increasing: 49 per boat in 2023 compared to 13 in 2020, and only seven per boat in 2018.[33] The NCA suggests that the threat from organised acquisitive crime, including high-harm burglary, vehicle crime and robbery, is also likely to rise due to increases in the cost of living.[34] Almost half of acquisitive crimes are associated with drugs,[35] demonstrating the link between the various forms and drivers of SOC.[36]

Reported incidents of modern slavery and human trafficking have risen considerably. The National Referral Mechanism (NRM) – a framework for identifying and recording potential victims of human trafficking and modern slavery – received 17,004 referrals in 2023, compared with 1,743 in 2013, an increase of 876 per cent and the highest number since reporting began. Police-recorded modern-slavery offences have seen similar trends, increasing from 955 in 2015–16 to 9,053 in 2022–23.[37] The Modern Slavery and Exploitation Helpline[38] received a record number of calls in 2023 and its fourth consecutive annual increase. Understanding of previously hidden threats, such as modern slavery and human trafficking, has significantly improved over the past decade, which may account for some of the increase. Nevertheless, the overall numbers – and the resulting pressure on law enforcement – remain staggering.

FIGURE 3

Number of National Referral Mechanism referrals



Source: Office for National Statistics

Other SOC threats – such as child sexual exploitation and abuse (CSEA) – remain prevalent. For example, the Independent Inquiry into Child Sexual Abuse estimated that one in six girls and one in 20 boys experience CSEA.[39] While most abuse takes place within family environments, there is concern about the increasing volumes of CSEA taking place online. Online spaces such as social media and gaming platforms allow strangers to interact with children, while the use of extended reality technologies, such as deepfakes, to conduct abuse has been identified as an evolving threat. As with modern slavery, increased awareness and understanding of CSEA is also driving up reporting rates.

The SOC threat is not confined to the UK. Reports suggest that Sweden has witnessed a surge in gang violence and shootings since 2013, with firearm deaths more than doubling during this period.[40] France – the country with the highest national homicide rate in Western Europe – has also seen an increase in gang violence among young people: in December 2023, the public prosecutor of Marseille reported an all-time high of 47 deaths and 118 injuries related to drug trafficking.[41] OCGs operating in Ireland have fuelled high levels of firearms-related violence compared with the UK, as illustrated by the Dublin-based Kinahan OCG, responsible for 18 deaths between 2015 and 2021.[42] Irish OCGs have strong links to drug-distribution hubs on the European continent, and they exploit the Common Travel Area while using the UK as a waypoint for drug trafficking. Last year, the secretary-general of Interpol said that, over the past five years, drug trafficking and organised crime had increased "by an order of magnitude", with Interpol stating that "organized crime groups are increasingly posing a direct threat to state authority in many countries".[43]

Technology, International Instability and Increasing Vulnerabilities Are Fuelling Organised Crime

Technology is a key enabler of SOC in all its forms.The widespread use of the internet[44] and the sheer volume of online material presents criminals with increased opportunities and more potential victims (particularly in relation to fraud and CSEA), while the rise of cryptocurrency and the increasing ease of online financial transactions facilitates money laundering, criminal transactions and the trade in illegal commodities. Online criminal activity is also more difficult for law enforcement and intelligence agencies to detect and disrupt. Criminals use technology to anonymise and hide their communications from law enforcement, with methods including virtual private networks (VPNs) and encrypted messaging platforms.[45] Recent advances in generative AI will only exacerbate the challenge faced by law enforcement: the Virtual Global Taskforce, an international alliance of 15 dedicated law-enforcement agencies working together to tackle child sexual abuse, recently warned about the use of AI in facilitating CSE.[46]

How OCGs Use Technology

Technology has lowered the barrier to entry to perform SOC, exponentially increased the criminal opportunities open to OCGs and effectively dissolved geographical boundaries. It enables OCGs to operate easily, quickly and at scale, helping them evade law enforcement and conceal their activity.

Technology makes it easier for criminals to identify victims. OCGs use online spaces to profile and identify victims at scale, in targeted or passive ways. Social media is used to gather information about individuals and spread messages to huge audiences, multiplying the potential victim pool for fraud or financial scams, for example. False job advertisements can lure victims into human trafficking, and posts advertising lavish lifestyles and the chance to earn money have been used to recruit children into "county lines" drug-dealing. Criminals capitalise on young children's growing use of social media to identify potential victims of child sexual abuse and exploitation. For example, in September 2022, a British man was jailed after sending sexual messages to children in multiple countries. He had used social media to communicate with 131 potential victims, some as young as 10 years old.

OCGs use technology to expand the range and reach of their criminal activities. The internet has led to the creation of entire new categories of crimes. For example, criminals used VPNLab, a virtual-private-network service on the dark web, to deploy ransomware and conduct cyber-attacks (it taken down in 2022 by an international investigation involving the NCA). In early June 2024, cyber-criminals from the Qilin group hacked NHS provider Synnovis in a ransomware attack and subsequently published almost 400GB of private patient information on the dark web; this included patient names, dates of birth, NHS numbers and descriptions of blood tests. The hack also resulted in more than 3,000 hospital and GP appointments and operations being disrupted.

Other more traditional crimes, such as drugs and firearms trafficking and fraud, are facilitated using technology. A fraud website used by criminals until 2022 was iSpoof; through the site, criminals were able to call victims, appearing as if they were legitimate employees of banks, tax offices and official bodies. This platform allowed the criminals to operate at scale; at its peak almost 20 people per minute were being contacted, and the confirmed losses to UK victims totalled £43 million.

Technology allows criminals to better hide their assets and evade law enforcement. Cryptocurrency and virtual banking services are used to facilitate money laundering and carry out criminal transactions undetected, and the dark web provides access to illegal commodities and services. The anonymity offered by online communication services and the accessibility of encrypted-communications software make it easier for criminals to evade law enforcement and conceal their activity. The online encrypted-communications platform EncroChat – taken down in 2020 in an operation involving the NCA – was used by 60,000 people worldwide to coordinate and plan the distribution of illicit commodities, launder money and plot to kill rival criminals. EncroChat provided users with handsets equipped with instant-messaging apps, the ability to make calls over the internet and a "kill code" that allowed messages and records to be remotely wiped.

Enablers – including professional services and corrupt officials – are at the heart of organised crime. Criminals exploit the specialist skills, knowledge and expertise of professionals – including lawyers, accountants, estate agents and investment advisers – to facilitate their activities. Corrupt insiders – officials working in key public services, such as the border forces or prisons – are used to “facilitate the movement of illicit commodities, divulge sensitive information and circumvent security measures, reducing the likelihood of law-enforcement detection”.[47] Europol figures suggest that 86 per cent of the most threatening criminal networks use legal business structures to enable their activities in the EU and more than 70 per cent of networks engage in corruption to facilitate criminal activity, or to obstruct law enforcement or judicial proceedings.[48] While some are criminally complicit, many individuals and firms also facilitate criminal activity through recklessness or negligence.

The international dimension of SOC is increasing, exacerbated by global instability. The sophistication of technology has opened the door to international OCGs. Most technology used by criminals (such as VPNs) is cheap and accessible, and enables criminals to operate remotely and across borders, reducing the number of people required to conduct their activities and giving them access to new markets. OCGs exploit global conflict and instability for their impact on illegal commodity supply chains or the vulnerabilities of individuals. Moreover, the NCA[49] and National Cyber Security Centre[50] (within GCHQ) point to growing concern about state-tolerated cyber-crime.

Vulnerabilities at home have weakened the UK’s resilience to SOC. Criminals rely on exploiting the vulnerabilities of individuals and communities, whether through modern slavery and trafficking, using vulnerable young people to transport drugs across the UK or preying on those facing hardship to attract so-called “money mules”. Over the past decade, the breakdown of public services, the Covid-19 pandemic and cost-of-living increases – together with the associated rises in poverty and deprivation – have created pressure on individuals and communities, rendering them more vulnerable to exploitation.[51] There have been increases in key factors associated with vulnerability: for example, the proportion of children in England who have entered care has been growing, as has the number of assessments of children at risk of serious harm and the rate of exclusion from schools.[52]

Above all, organised criminals are highly adaptable, nimbly pivoting their business models and operations to adapt to new restrictions and opportunities.

The Public Expects a Stronger Response

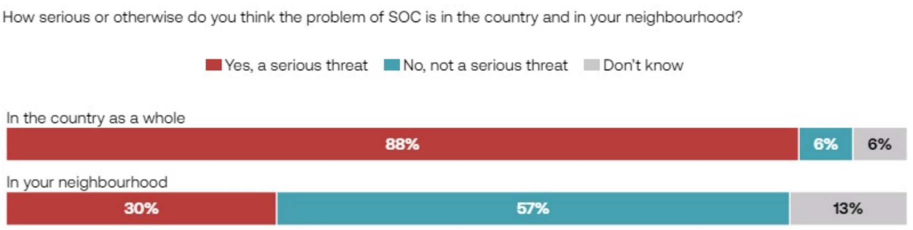
TBI commissioned Deltapoll to conduct a nationally representative survey of 1,519 adults across Great Britain to test the public's perception of SOC, how it impacts their everyday lives and how the public feels the threat should be addressed.

The conventional political narrative suggests that most people view SOC as a remote issue, with little bearing on their day-to-day lives. The funding deficit between SOC and other comparable threats is seen as a reflection of political priorities.[53] The findings, however, demonstrate the opposite: the public is alive to the evolving threat and impact of SOC and expects a stronger response.

We asked respondents how serious they believe the problem of serious and organised crime is in Britain. Our polling shows that the public is near-unanimous in seeing it as a national threat, with one in four respondents also feeling its impact in their local area.

FIGURE 4

88 per cent of the public sees SOC as a serious national threat

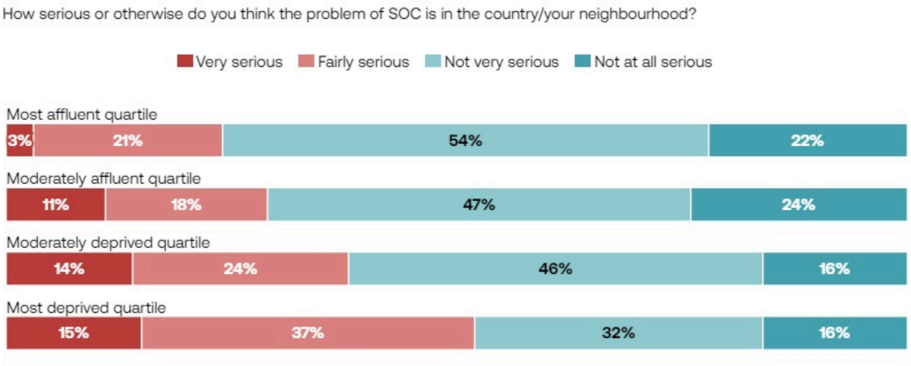


Source: Deltapoll, TBI

The day-to-day impact of serious and organised crime is felt more acutely in some communities than in others. When asked about the issue of SOC within their local area, a majority – 52 per cent of respondents – living in the most deprived areas of the country say they feel a serious impact in their neighbourhood from organised crime.

FIGURE 5

More than half of those living in the most deprived communities in Britain say SOC is a serious problem where they live


How serious or otherwise do you think the problem of SOC is in the country/your neighbourhood?

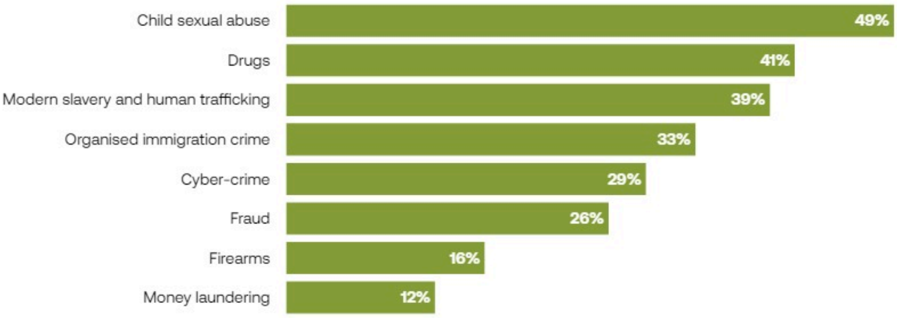
"Don't know" responses removed

Source: Deltapoll, TBI

Our survey findings also offer some insight into which SOC threats the public is most concerned about. Child sexual abuse (49 per cent), the drugs trade (41 per cent) and human trafficking (39 per cent) are the areas of greatest concern of SOC crimes, closely followed by organised immigration crime, cyber-crime and fraud.

FIGURE 6

The SOC crimes of greatest concern to the public

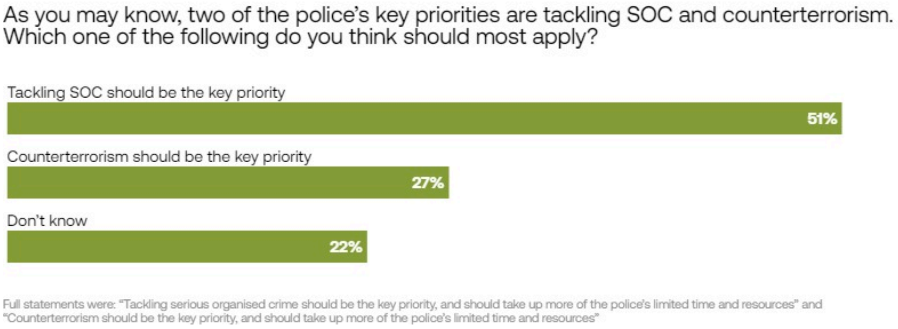


Source: Deltapoll, TBI

Our survey shows that the majority of the public thinks SOC should be a higher priority than terrorism. When asked whether organised crime or terrorism (a commensurate national-security threat) should be a key priority for the police, 51 per cent of respondents believed that tackling organised crime should be the key priority for police time and resources; 27 per cent cited counterterrorism.

FIGURE 7

SOC trumps terrorism as the public's biggest concern



As you may know, two of the police's key priorities are tackling SOC and counterterrorism. Which one of the following do you think should most apply?

Full statements were: "Tackling serious organised crime should be the key priority, and should take up more of the police's limited time and resources" and "Counterterrorism should be the key priority, and should take up more of the police's limited time and resources"

Source: Deltapoll, TBI

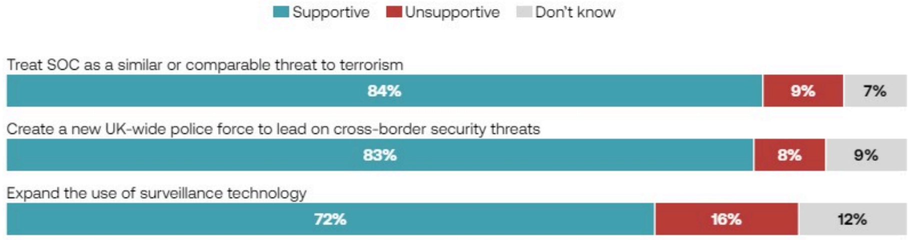
We tested several new policies with the public and our polling suggests the following would have broad support:

- **84 per cent** of respondents are in favour of SOC being treated as a comparable threat to terrorism, with similar legal powers to seize assets and stop people at the border.
- **72 per cent** are in favour of the expansion of surveillance technology, with greater use of AI-driven predictive analytics and real-time facial-recognition technology.
- **83 per cent** support the creation of a new UK-wide police force to lead on cross-border security threats, with responsibility for counterterrorism, SOC and cyber-enabled fraud.

FIGURE 8

There is broad public support for structural reforms to tackle SOC

Various ideas have been put forward to better tackle the threat from SOC. How supportive or otherwise would you be for each of the following?



Full statements were: "The creation of a new UK-wide police force to lead on cross-border security threats, eg counterterrorism, serious organised crime and cyber-enabled fraud", "Treat serious organised crime as a similar/comparable threat to terrorism, with similar legal powers to seize the assets of individuals" and "Expansion of surveillance technology, with greater use of AI-driven predictive analytics and real-time facial technology"

Source: Deltapoll, TBI

Our survey findings suggest that the public believes SOC is a serious threat, is aware of its impact on their communities – particularly for those in more deprived neighbourhoods – and would welcome a stronger response from government and law enforcement.

The National Response to SOC Is Unsuited to the Scale, Nature and Complexity of the Threat

Despite the evolving threat of SOC, and public interest in curbing it, the UK remains an attractive environment for organised criminals.

SOC has historically been under-prioritised. The risk it poses is chronic (as opposed to the acute threat of, say, terrorism), pervasive and not well quantified. This means that the impacts and costs of SOC can be less visible, and there is confusion over whether to classify it as a national-security threat or merely another form of crime. This is reflected in the fact that the relevant directorate within the Home Office is split between the public-safety and homeland-security groups. In addition, the current policing structure, in which accountability lies locally, cannot easily prioritise complex cross-border threats. Last, SOC has historically been seen as more of an international problem – driven by complex enablers such as the free flow of capital and lighter regulation – and as a result hasn't attracted the same level of focus or resourcing as terrorism or other comparable national-security threats.

The current understanding of the problem is incomplete. The NCA was established in 2013 and tasked with leading and coordinating the UK's response to SOC. One key role of the NCA is to develop a "single view of the threat from serious and organised crime". A 2019 report from the National Audit Office (NAO)[54] found that the government had an "incomplete" understanding of the scale of SOC, something particularly evident in relation to international illegal markets and illicit finance. The report noted that challenges centre on the "underdeveloped" intelligence and assessment capabilities of individual organisations, and inefficient data and intelligence sharing between these agencies and the NCA. The NCA has stated that it struggles to robustly compare the impact of different threats.[55] Both the NCA and the NAO have previously noted difficulties in developing an effective performance framework, limiting the ability to understand the impact and effectiveness of ongoing work.

Traditional approaches – largely focused on the pursuit of known offenders through surveillance, arrest and prosecution – are no longer sufficient to address scale or nature of the threat. Investigations can be extremely difficult, particularly when crimes involve an overseas element (as many do) or rely on encrypted technology.[56] Few cases make it to court and, when they do, trials are often lengthy and protracted. Even if more convictions could be secured, prison does not act as a sufficient disincentive to highly complex and adaptable criminal networks, whose business models often build in an expected level of imprisonment for low-level members.

Overcrowding in prisons, which means that offences are less likely to be punished by imprisonment, is also reducing the deterrent effect of prosecution. The sheer volume of crimes, particularly when compared with the resources available to law enforcement, means that while the UK must continue to pursue offenders, it cannot arrest its way out of the problem. Even when investigations can result in a charge, the complexity of these cases demand huge resources and skills that are scarce among lawyers and operational officers.

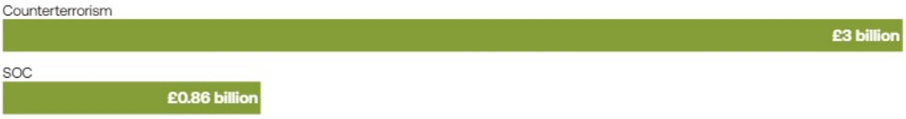
The national response to SOC is disjointed, siloed and lacks cooperation, with more than 100 organisations involved in responding to it. This looks on paper to match the scale of the SOC threat but in reality creates a complex and confused strategic and operational landscape. The latest SOC strategy paints a simplified picture of streamlined flows of influence from the Home Office and NCA, through to Regional Organised Crime Units (ROCUs) and then police forces. In this model, the NCA (answerable to the Home Secretary) provides strategic leadership of the national SOC response, directing other organisations (largely ROCUs) to act. ROCUs are defined as the operational and intelligence link between the NCA and police forces in England and Wales, leading the regional response and providing forces with specialist capabilities. In truth, the landscape is overly complex and characterised by a lack of joined-up working: individual agencies often work separately on issues which require a coordinated approach and either duplicate efforts on the development of specialist skills or compete for scarce skills. There is a lack of effective cross-organisation data or analysis sharing, which can again lead to duplicated efforts. The NCA's tasking of ROCUs and police forces has been found to be inconsistent and unclear,[57] with insufficient powers to oblige organisations to act. The Tackling Organised Exploitation (TOEX) Programme – piloted in 2022 before being rolled out nationally in 2023 – has the intention of providing a greater whole-system approach to the national exploitation response,[58] yet it also lacks the power to task police forces or other agencies.[59]

Criminals exploit known vulnerabilities in the UK's infrastructure and legislative framework. There are limited consequences for the professional services and corrupt officials who enable the OCGs' activities; the legal framework that regulates online safety (including the Online Safety Act) is far from watertight, allowing criminals to use online platforms to carry out their activities and hide behind encryption, while inefficient anti-money-laundering practices and asset-recovery laws are allowing criminals to benefit from the proceeds of their crimes. Although the past few years have seen some welcome examples of large-scale disruption – for example, Operation Venetic, which involved the dismantling of the EncroChat network – the UK's overall approach to disrupting the enablers of SOC remains reactive and disjointed.

Finally, the funding available for the SOC response is dwarfed by what the UK spends on terrorism. The UK spends more than £3 billion a year[60] on counterterrorism, compared with just £860 million on SOC[61] in 2023–24. Counterterrorism policing alone receives more than £1 billion annually.[62]

FIGURE 9

Spending on SOC and on counterterrorism, 2023–24



Source: HM Government, National Audit Office[63]

Despite this disparity in resources, SOC is an issue which dominates operational activity within policing; territorial forces shoulder a large proportion of the SOC burden, being responsible for the majority of operational activity.[64] While law-enforcement agencies can generate substantial revenue through the seizure of criminal assets and fines, too little of this is currently reinvested in fighting SOC.[65] The multiplicity and uncertainty of funding streams coming to organisations who work on SOC – characterised by yearly bidding processes and pressure to compete with other priorities – also complicates and threatens the stability of the response. Funding arrangements are not conducive to long-term planning, highlighted as a "cause of concern" by HM Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS) in 2021.[66] Further, law-enforcement capital funding (which includes investment in technology) is tiny compared to resource funding; in the year ending March 2024 policing received £17.5 billion in resource funding but only £100 million in capital funding. This hinders investment in capabilities such as data analysis, communications and technologies – all vital for an effective SOC response.

03

A New Approach to Tackling SOC

The UK's response to organised crime is out of step with the scale of the challenge and fails to reflect the public's concern, experiences and priorities. To address the rising threat and the real damage caused by SOC, the UK must become a hostile environment for organised criminals. To do so, we suggest a three-pronged approach:

- Treat SOC as a national-security threat, with powers and resources commensurate with those used in counterterrorism.
- Strengthen the UK's infrastructure and legislative framework to disrupt criminal enablers, resources and tools.
- Support law enforcement's ability to respond to SOC by updating structures and capabilities to fit the modern threat.

1. Treat SOC as a National-Security Threat

ENHANCE THE UK'S INTELLIGENCE AND FORESIGHT CAPABILITY

A full understanding of the threat posed by SOC is crucial for an effective response. While understanding is continuously improving, there are notable gaps and the overall picture remains incomplete. For example, the Royal United Services Institute recently pointed out that "the intelligence gap on the scale and nature of corruption remains concerningly large".[67] The director general of the NCA said that, while the agency has improved its ability to assess the scale of each threat, "some are better than others", highlighting their understanding of money laundering as among the weaker ones.[68] The NAO has also highlighted the government's insufficient understanding of transnational illicit markets as an area of concern. While there are good examples of collaboration and sharing of information between agencies – for example, the government's response to firearms crimes has been praised as a successful example of multi-agency working – systematic, coordinated data sharing remains a barrier to effective intelligence-gathering.

Beyond a full picture of the threat, the government and law-enforcement agencies lack a clear understanding of the impact of measures to tackle SOC. The NAO previously found that "performance measurement is immature and does not yet support effective decision-making". The NCA also recently highlighted the difficulty in assessing the cumulative impact of disruption measures on the overall threat and pointed out the lack of an "indicative metric of our collective ability to bear down on the threat from serious and organised crime".[69]

The lack of a complete picture not only affects the effectiveness of the response but also the priority it is accorded by policymakers and law enforcement. SOC is an ongoing threat rather than an acute one and, unlike terrorism, its impacts are not always visible. Having a better understanding of the links between SOC and other crimes (including terrorism and serious violence), and its cost to society, could help drive it up the political agenda.

In the Labour Party's election manifesto, little mention was made of serious and organised crime; but as the analysis in this paper shows, tackling it should be a top priority to achieve the objectives of the "take back our streets" mission. As it sets up the relevant mission board, the government should ensure that it is provided with a much deeper understanding of the scope, scale and impact of serious and organised crime in the UK.

Recommendation
Create a National SOC Lab. The lab would bring together experts from across law enforcement, government, academia and the private sector and would perform several functions related to SOC including:

- *producing regular analysis detailing its impact, including its economic costs and the proportion of various threats (such as irregular migration, serious violence and drug dealing) that are attributable to it*
- *developing improved metrics to understand the ongoing threat it poses and the impact of counter-SOC measures*
- *acting as a UK SOC "what works" centre, assessing the impact of interventions, including international best practice, and commissioning work to address evidence gaps*

- *forecasting and anticipating the impact of new and emerging technologies*
- *housing a review team and secretariat to enable a strategic cross-government review that could determine the roles, capabilities and reforms required to meet the challenges of international and tech-enabled SOC*

The National SOC Lab should be independent from the NCA, including its National Assessment Centre,[70] *and the Home Office but collaborate closely with them. It should report to the "take back our streets" mission board on an ongoing basis. The mission board should ensure that the findings of the Lab are routinely reflected in the NCA's annual National Strategic Assessment and the development of a broader SOC strategy.*

INTRODUCE COUNTERTERRORISM-STYLE POWERS TO TACKLE SOC

The scale and complexity of SOC is increasing, and OCGs are constantly adapting to take advantage of new opportunities. Providing law enforcement with the necessary tools to combat SOC is crucial to improve the UK's ability to disrupt OCG activity and its enablers, resources and tools. Yet the legal framework has failed to keep pace as the threat has evolved.

Counterterrorism is a useful parallel, as terrorism is a threat commensurate to SOC and shares many similarities. Terrorists and OCGs engage in similar activities, such as people and weapons trafficking. Their recruitment tactics are also similar, as they both often prey on vulnerable individuals and communities. Flows of illicit finance are key enablers for terrorist groups and OCGs, as they both rely on money laundering to facilitate their activities. New technologies such as digital currencies are used to facilitate activities at scale and make detection more difficult. Much like terrorism, SOC is a global challenge that requires an international response.

In the UK, terrorism legislation provides law enforcement with a wide range of tools. These include investigatory powers that help forces and agencies gather intelligence and identify and monitor suspects, disruptive powers that aim to stop terrorists from operating by restricting their ability to carry out criminal acts, and enforcement powers that aim to take known criminals out of action and make convictions a suitable deterrent.

Together, they act as a comprehensive framework that is widely considered to be effective in preventing and deterring terrorist attacks. In 2018, the report of the National Security Capability Review found CONTEST, the UK's counterrorism strategy, to be "a well-organised and comprehensive response to terrorism, with strengths in terms of powers, resources, reach and resilience".[71] Reports by the Independent Reviewer of Terrorism Legislation overall describe the UK's framework as resilient and able to meet the evolving threat. An example is the Schedule 7 powers, under Schedule 7 of the Terrorism Act 2000, which enable law enforcement to detain and question individuals travelling across borders even if they are not suspected of a terrorism-related offence. Those powers have been called "valuable and justified"[72] and assessed to be exercised "conscientiously and effectively"[73] as a highly valued source of intelligence and evidence.[74] The UK's approach to counterterrorism has been described as ahead of its partners[757677] and has informed other countries' approaches,[78] including those of Australia and Canada.

There is no comparable "counter-SOC" framework. Many of the powers available to tackle terrorism are not available for SOC offences. For example, there is no equivalent to Schedule 7 powers nor is there a SOC-specific sanctions regime, despite the NCA previously calling for the latter. Unlike those convicted of terrorism, SOC offenders are not subject to additional restrictions in prison, nor are they routinely separated from other offenders.[79] Although the UK has extra-territorial jurisdiction over terrorism offences, it doesn't in relation to many crimes that fall under the SOC umbrella. Where comparable disruptive powers do exist, their application has often been found to be ineffective, hindered by intelligence gaps and a lack of available resources. For example, Serious Crime Prevention Orders,[80] an equivalent to the Terrorism Prevention and Investigation Measures, are under-used, in part because the police lack the funds to adequately enforce them. Overall, the powers available to investigate, disrupt and enforce SOC vary greatly between each type of crime contained under the SOC umbrella. Responses lack an overarching legislative framework to bring these various elements together.

FIGURE 10

A comparison of counterterrorism and SOC powers

This table illustrates some of the gaps between the powers available to deal with terrorism and those available to deal with SOC. It is intended to be illustrative, not exhaustive.

	Examples of current counterterrorism application	**Examples of gaps in SOC response**	**Potential impact of strengthened SOC powers**
Investigatory powers help law-enforcement agencies gather intelligence and evidence, identify and monitor suspects, and uncover crimes.	The Terrorism Act 2000 gives law enforcement the power to detain and question individuals travelling across borders even if they are not suspected of a terrorism-related offence (Schedule 7) or to stop and search individuals suspected of being involved in terrorist activity (Section 43) for the purpose of gathering intelligence and identifying suspects.	No power equivalent to Schedule 7 stops exists for SOC. The police have the power to stop and search individuals or vehicles with reasonable cause to suspect they are carrying drugs or firearms. However, these powers depend on prior intelligence or evidence, and tend to target those at the low end of the OCG network.	Greater investigatory powers – for example, an equivalent of Schedule 7 stops – would enable law enforcement to gather greater intelligence about criminals and their methods. This change would fill current intelligence gaps, and in turn allow better disruption and enforcement to take place, ultimately acting as a greater deterrent to OCGs.
Disruptive powers aim to stop known criminals from operating by restricting their ability to carry out criminal acts.	Terrorism Prevention and Investigation Measures (TPIMs) can include bans on holding travel documents, specific residency restrictions, requirements to wear an electronic tag, and limits on the use of financial services, telephones and computers. In extreme circumstances, the home secretary can withdraw individuals' passports or exclude people from the UK through an exclusion order.	The closest equivalent to TPIMS are Serious Crime Prevention Orders (SCPOs). Although they can also place a range restrictions on individuals convicted of SOC offences, these are less stringent than the powers available under TPIMs. Similar sanctions can be imposed using Slavery and Trafficking Prevention Orders, Financial Reporting Orders and Travel Restriction Orders.	Enhanced disruptive powers would strengthen efforts to destabilise OCGs and frustrate their activities, reducing the burden on law enforcement.
	A range of financial sanctions can be used to freeze funds or economic resources held or used by designated people.	There is no specific financial-sanctions regime for SOC and the current sanctions regime is not applicable to SOC. Unexplained Wealth Orders can be imposed on those suspected of SOC offences, but they have also been vastly underused.	
Enforcement powers aim to take known criminals out of action and make convictions a suitable deterrent to criminal activity.	The Counter-Terrorism and Sentencing Act 2021 introduced a new "serious terrorism" offence, which requires a jail term of at least 14 years and stipulates the whole term must be spent in jail.	SOC offences attract a wide range of sentences. However, involvement in organised crime is not an aggravating factor in itself. The new offence of "participating in the activities of an organised crime group" has a maximum sentence of five years of imprisonment.	Harsher sentences that disrupt the ability of offenders to commit crimes for longer will make prison a greater deterrent.
	Terrorist offenders are subject to additional restrictions in prison, including in relation to communication. Since 2017, terrorist offenders most likely to radicalise others have been housed in separation centres away from the main prison population.	SOC offenders are not subject to additional restrictions in prison. Separation centres have thus far not been used to house SOC offenders, though there are grounds to use this power in the interests of national security.	
	The UK has extra-territorial jurisdiction across a number of terrorism offences, meaning that even foreign nationals may be prosecuted in the UK for conduct that took place outside the country.	Although the UK has extra-territorial jurisdiction over some SOC crimes, many that fall under the SOC umbrella are not covered.	

Source: TBI, Ministry of Justice,[81][82] HM Chief Inspectorate of Prisons[83]

Recommendation

The government should introduce a Countering SOC Bill that extends *relevant counterterrorism powers to SOC. It should include greater investigatory powers, a SOC-specific financial-sanctions regime and extra-territorial jurisdiction across a greater range of SOC offences. It could also create a SOC register to allow for closer monitoring of known offenders. The introduction of counterterrorism-style powers for SOC would capitalise on law enforcement's familiarity with the existing counterterrorism regime; they could become familiar with these new powers and practices more quickly than they might for others, and the new powers would consequently provide immediate returns.*

This bill should be accompanied by the elaboration of clear guidelines and principles for the use of such powers. A strong oversight regime, including the appointment of an Independent Reviewer of SOC Legislation modelled on the Independent Reviewer of Terrorism Legislation to scrutinise the use of such powers would ensure they are applied proportionately and effectively.

UNLOCK THE POTENTIAL OF TECHNOLOGY

Technology is a key enabler in SOC. Criminals continually adapt to and take advantage of technological developments and changes in user behaviour. Law enforcement's response needs to adapt, yet policing currently trails the criminals when it comes to harnessing the power of technology. While some forces are seeking to make use of new technologies, their application at the national level lacks strategic input, coordination and oversight. This has hindered forces' ability to benefit from joined-up, interoperable systems, and instead led to the development of a siloed and fragmented array of approaches towards harnessing new tech.

The ability to leverage innovation in the public sector requires a fit-for-purpose procurement system that enables the government to buy, build and deploy new software at pace and scale. It also requires a rethink of risk and a specialised environment to test and experiment with new technologies. In practice, this means a system that is flexible and agile, continuously learning and adapting with the rate of exponential technological change. The introduction of the SOC legislative framework proposed in this paper would further enable effective industry partnerships and improve technology use.

To achieve a fit-for-purpose 21st-century procurement model, the UK government should rethink its relationship with industry, particularly new startups and innovators who are leading the development of today's cutting-edge technologies. The government should also examine its relationship with users, be they recipients of government services or back-office civil servants, and its overarching approach toward innovation and next-generation technologies for government use. This must be built on three core foundational principles:

- A partnership with industry, where industry and government build, learn and deploy together.
- A direct connection with users, with all procurement processes centred on building for the user, with the user.
- A streamlined path to production, shipping fast and often, so users can interact with, test and validate solutions early and throughout the development process.

Delivering on these core foundations demands a redesign of the procurement institutions themselves.

Recommendation
The NCA should produce a five-year SOC technology strategy that sets out the priority capabilities needed to fight SOC. This should be accompanied by a gap analysis that would be updated on a yearly basis. The strategy should be informed by the National SOC Lab, which should work with industry experts to develop SOC threat models and test the safety of foundational models against misuse.

As recommended by TBI in our paper Reimagining Procurement for the AI Era*, the government should establish an Advanced Procurement Agency (APA) that would stimulate demand for innovative products and services and create lead markets for emerging technologies. This agency should have a mandate to identify and support strategic priorities, and to work with industry, the NCA and ROCUs to co-design and co-fund challenge-led procurement programmes. It should also have the flexibility to use a range of procurement methods, including pre-commercial procurement, innovation partnerships and outcome-based contracts, to support different stages of* *the innovation process. The APA should operate under a procurement-as-a-service model across ROCUs, not only to advise and support teams on procurement but also to serve as a catalyst for innovation in technology-procurement innovation across police forces.*

Case Study: Border security

Technological innovation is improving border security. The EU roadmap to fight drug trafficking and organised crime has committed more than €200 million to fund equipment to help customs authorities scan containers and goods.[84] Other initiatives include the rollout of 5G at UK ports to improve data transfer and communications,[85] and the automation of goods-monitoring processes. It is estimated that there will be 8.7 million smart containers in operation globally by 2026.[86] Smart containers are fitted with electronic devices that enable their identification, location and environmental-condition monitoring.[87] The EU roadmap has considered launching digital investigations to facilitate the detection of possible abuses of the software used in ports.

Fund the SOC Response to Match the Scale of the Threat

As previously set out, the funding available for the SOC response is dwarfed by what the UK spends on terrorism. It spends more than £3 billion a year[88] on counterterrorism, compared with just £860 million on SOC[89] in 2023–24, despite these threats costing roughly the same to society. The NCA has regularly called for its budget to be significantly increased, pointing out in 2022 that the FBI, for example, received three times as much funding per officer. The NCA's pay structures are complex and no longer fit for purpose; salaries are lagging those of the police (officer salaries are set at 90 per cent of police pay), making it difficult to recruit and retain talented and experienced officers.[90]

Funding arrangements can create perverse incentives and make it harder to respond to SOC effectively. For example, ROCUs are funded from a multitude of sources, often on a short-term basis, which creates uncertainty and limits their ability to deliver on long-term priorities. Law-enforcement capital funding (which includes investment in technology) is tiny compared with resource funding; in the year ending March 2024 policing received £17.5 billion in resource funding but just £100 million in capital funding. This stymies investment in capabilities such as data analysis, communications and technologies – all vital for an effective SOC response. Both the NAO and HMICFRS have previously highlighted the need to reform SOC funding structures. In addition, while law-enforcement agencies can generate substantial revenue through the seizure of criminal assets and fines, they currently lack an incentive to do so. Anti-corruption campaign group Spotlight on Corruption estimates that agencies generated £3.9 billion in confiscation and fines between 2016 and 2021 but kept just 38 per cent of recovered assets.[91]

Recommendation
The government should match what it spends on counterterrorism to fund its SOC response – an increase of more than £2 billion. To do this, it could take the following action.

- *In the first instance, create a dedicated SOC fund by ringfencing money raised through asset recovery and fines levied for economic crimes. Although amounts recovered vary year by year, based on the past three years we estimate that this represents approximately £300 million recovered from confiscation and fortitude orders and £250 million recovered from fines.*[92] *This fund should be accompanied by reforms of the confiscation regime to increase the amount of assets recovered (see* *next section).*

- *Over the longer term, reinvest the cost savings generated from reduced demand and improved efficiency into the SOC response, using insights generated by the SOC Lab on the scale and extent of SOC-related crime to determine what proportion of the savings should be reinvested. Efficiency could be improved by reforming the asylum system to accelerate case processing or cutting the number of crossings by disrupting the operation of OCGs.*

Alongside additional investment, the government should introduce long-term funding models to provide certainty and enable longer-term investments. It should also review the NCA's pay and employment framework to enable it to recruit a higher calibre of staff, including – where necessary – by matching salaries to those of police officers.

2. Strengthen the UK's infrastructure and legislative framework to disrupt criminal enablers, resources and tools

Target professional enablers

Organised criminals rely on a multitude of actors, known as enablers, who provide tools and resources to enable criminality. These enablers span the range of professional services, from lawyers and accountants, to financiers, hackers and developers. Disrupting the highest-harm criminals relies on targeting those who enable their illegal activity.

To incentivise cooperation from professional services, there needs to be far greater consequences for senior executives at the helm of firms that engage in financial wrongdoing or regulatory breaches that enable SOC. Recent efforts to strengthen corporate-liability laws and give businesses more confidence to share information to tackle economic crime[93] are welcome but too few individuals are being held to account for their role in facilitating organised crime. Spotlight on Corruption found that the Financial Conduct Authority's (FCA) use of regulatory fines and prohibition orders against individuals has declined over the past decade, with the FCA taking just one regulatory action against an individual in response to fines totalling £777 million imposed on 17 banks for money-laundering failures.[94]

Here, the UK could learn from the US. Mandatory clawback rules – the recovery of incentive-based compensation awarded to executives in the event of an accounting restatement – were recently introduced for all firms listed on the New York Stock Exchange and Nasdaq, alongside greater incentives for companies to claw back director remuneration where criminal investigations are underway.[95] These powers are robustly enforced by the Securities and Exchange Commission (SEC). Measures to strengthen malus and clawback[96] provisions were proposed by the UK government in a 2021 White Paper before being dropped and replaced by much weaker proposals.

Recommendation
The government should introduce a package of measures aimed at increasing senior-executive accountability. It should implement the stronger malus and clawback provisions originally proposed in 2021, requiring minimum conditions within which malus and clawback provisions would be triggered and widening the scope of such trigger points to include misconduct, reputational damage and material failure of risk management.[97] *As part of the package, the attorney general should issue a strategic steer to the FCA regarding the importance of individual liability for corporate crime.*

Alongside measures to tackle professional enablers, greater efforts must be made to address the threat of corruption. OCGs rely on access to insiders in key sectors, such as at the border or in prisons. For example, between 2019 and June 2023, 992 prison staff have been investigated, 114 arrested and 42 charged in relation to the conveyance of drugs.[98]

Staffing deficits, fuelled by under-resourcing and leading to the increasing use of contractors or temporary staff, offer opportunities for corrupt associates to apply for key posts. Degradations in pay and the rising cost of living have also made current staff more susceptible[99] to corruption attempts. These issues are exacerbated by a lack of data to understand the threat. A recent inspection by the Independent Chief Inspector of Borders and Immigration concluded that "at present no one is able to see the full picture of insider threat across Border Force".[100] Even when corruption is identified, the law of misconduct in public office is, in the words of the Law Commission, "in need of reform, in order to ensure that public officials are appropriately held to account for misconduct committed in connection with their official duties".[101] Despite this, the UK does not currently have an anti-corruption strategy – the last one ended in December 2022 – and the post of anti-corruption champion has been left vacant for over two years.

Recommendation
The government should publish a new anti-corruption strategy and re-appoint an anti-corruption champion. The strategy should set out a roadmap to further digitalise key sectors, such as borders and prisons, and set meaningful targets to measure progress. In addition, the government should replace the "misconduct in public office" offence with a "corruption in public office" offence, as recommended by the Law Commission.[102]

The new strategy should be accompanied by a public campaign to raise awareness of the nature and costs of corruption, including its impact on the rise of SOC, and encourage relevant professions to report related offences. The campaign should include a series of rapid trials to test the efficacy of various messages, building on evidence from the behavioural sciences on the range of motivations behind corruption – such as by justifying one's actions morally, holding the impression that others are doing the same thing or the perception that corrupt acts are victimless. The campaign should then be robustly evaluated.

Case study: The Netherlands approach to preventing SOC offences in prisons

The Netherlands has seen a rise in SOC, with the number of murder or manslaughter victims rising.[103] This is likely being fuelled by the strategic importance of Amsterdam as a key transit point for cocaine trafficking into Western Europe. Between 2012 and 2021, the volume of cocaine seized in the Netherlands increased by more than 600 per cent.[104]

In 2023, the Dutch government planned to invest an additional €34 million into measures to prevent criminal activities during detainment. Steps taken include enhanced prisoner supervision, additional funds to enable prisons to gather information about their detainees and investment into safer forms of adjudication such as eliminating the need for transportation to court by videoconferencing instead.[105]

Limit Criminals' Ability to Operate Online

Criminals communicate and commit crimes online, where they rely on a range of platforms and leave digital traces. In recent years, the government has taken some steps to tackle the rise of online criminality – such as passing the Online Safety Act[106] or requiring platforms to report illegal content on their websites. These, however, remain largely reactive. While the 2023–2028 strategy prioritises boosting the ability of law-enforcement agencies to investigate online crime,[107] it contains little detail on plans to improve the safety-by-design principles of online services.

Collaboration between law-enforcement agencies and the private sector and effective, real-time data sharing are crucial to staying ahead of the criminals. Positive examples already exist. One of these is the use of behavioural biometrics to prevent fraud, which many UK banks already employ. When a user interacts with an app or website, behavioural signals, such as how they type and move between apps, are collected and analysed and an authenticity score is generated. While this doesn't authenticate the user, and data are protected using tokenisation or hashing methods,[108] it does allow the software to spot suspicious patterns of behaviour on that device that might amount to fraud. A bank receiving this information can then act to prevent the fraud.

Yet these examples are too often siloed and effective data sharing remains hampered by a number of barriers. Collaboration between tech companies and law-enforcement agencies is challenging due to a lack of clear legal frameworks and appropriate structures for sharing information and a lack of personnel dedicated to liaising with statutory agencies. In addition, the private sector often lacks incentives to collaborate. Initiatives such as the Online Fraud Charter and the NCA's new public private partnership are welcome but they remain voluntary.

Recommendation

The government should introduce measures to facilitate collaboration and data sharing with the private sector. This should include issuing guidance (and, if necessary, legislating) to clarify the application of data protection laws; supporting the development of interoperability standards and data-sharing specifications and creating measures to protect commercially sensitive information. The NCA's public private partnership should be expanded to include other sectors (telco, social media platforms etc), taking a coalition approach such as the one used by the Centre for Finance, Innovation and Technology to rapidly prototype solutions for each relevant sector.[109]

Case Study: Australia and Singapore's data-sharing hubs

The Fintel Alliance's partners include major banks, remittance-service providers and gambling operators, as well as law enforcement and security agencies from Australia and overseas. Working with these organisations, Fintel Alliance develops shared intelligence and delivers innovative solutions to detect, disrupt and prevent serious crime.

Fintel Alliance has an established programme of work that is based on targeting priority themes. Some of these themes include crimes that prey on vulnerable community members, the exploitation of government revenue or professional money laundering.

Fintel Alliance partners work together at the Australian Transaction Reports and Analysis Centre (AUSTRAC) offices in Sydney and Melbourne, where they share and analyse financial intelligence to investigate and disrupt criminal and terrorist activity.

In 2022, the Singapore Police Force established the Anti-Scam Command to consolidate expertise and resources to combat scams. There, staff from major banks are co-located with police. In the first half of 2023, the Anti-Scam Command froze more than 9,000 bank accounts and recovered about $50.8 million.

The use of online anonymity is a major driver of internet-based crime. Yet restricting anonymity could create further risks for vulnerable groups, from whistleblowers to those seeking refuge from persecution. TBI has previously recommended the implementation of a digital-ID system, allowing individuals to store digital representations of their identity and verified credentials in a digital wallet. Through this wallet users can control when and how their information is shared while accessing government services and transacting with the private sector. Users would be able to use digital identities and credentials to demonstrate they are over 18, prove their citizenship or show that they have passed a criminal-record check, without also revealing other sensitive data. With this digital-identity infrastructure in place, online services could verify specific pieces of information, asking questions such as "are you a real person?" or "are you old enough to use this service?" without forcing users to reveal any identifying information. Just as law enforcement can work with banks to identify specific accounts and individuals involved in financial fraud, social media and the police would be able to de-anonymise accounts with a warrant. Digital verification could be used to verify businesses, as well as individuals.

Recommendation
The government should rapidly proceed with the Digital Information and Smart Data Bill, which would put digital-verification services[110] *on a statutory footing and give them parity with existing ID documents such as passport and driving licences. Therefore, official credentials could be securely stored and shared through digital wallets. Digital-verification services should include mechanisms to verify businesses as well as individuals.*

TACKLE ILLICIT FINANCE

OCGs rely on money laundering and illicit finance to facilitate their activities. The NCA estimates that more than £10 billion in non-cash and cash-based money-mule activity is laundered in the UK annually, while Transparency International has identified 2,189 companies registered in the UK that have been involved in money laundering on behalf of Russian citizens.[111] Hardening the UK against organised crime requires renewed efforts to limit criminals' access to illicit finance.

The supervisory regime for money laundering must be improved. The existing system is overly complex; for example, more than 20 regulatory bodies oversee the legal and accountancy sector, with the system lacking effectiveness and having previously been criticised by the Financial Action Task Force and the Office for Professional Body Anti-Money Laundering Supervision.[112] The creation of a Single Professional Services Supervisor (SPSS) for the legal and accountancy sector received the support of a range of organisations in a recent government consultation and could provide a more coherent approach.[113] Its establishment should be considered alongside guidance on how the regulations apply to different sectors and types of businesses, to make it easier for businesses to comply.

Recommendation
The government should simplify the framework for anti-money-laundering supervision, including by creating a Single Professional Services Supervisor (SPSS) role for the legal and accountancy sector. This role would be performed by a public body, either existing or new, that would replace existing professional body supervisors to take responsibility for the AML supervision of all legal and accountancy-sector firms. An appropriate fee structure should be introduced to enable the SPSS to have the necessary resources and strength. Supervisors should also be granted additional powers to monitor sanction systems and controls effectively.

Efforts to reduce money laundering should be accompanied by greater transparency in the UK's offshore financial centres and companies. The UK's offshore financial centres are targets for international criminals: the ability to hide assets behind opaque trusts and the lack of transparency over company ownership make them a haven for money laundering. Research by Transparency International UK and Spotlight on Corruption identified more than £6.7 billion worth of UK property bought with suspect funds, with most of these held via secretive offshore companies.[114]

Recommendation
The government should require information about overseas trusts with a significant UK connection to be published in a public register. It should also accelerate its work with the crown dependencies and overseas territories to create public registers of beneficial ownership.

Companies House operates the UK's open and flexible corporate-registration framework. However, until recently Companies House had no statutory powers, and it could not verify the information provided to it. This, together with the ease and speed with which companies can be incorporated – the government has in the past claimed that it is "among the fastest and cheapest in the world"[115] – has been exploited by criminals to create fraudulent shell companies. These provide OCGs with a veneer of legitimacy that enables them to commit a range of crimes. The UK leads the world for shell-company-related risks, according to Moody's research.[116]

The Economic Crime and Corporate Transparency Act 2023 has introduced a number of reforms to Companies House that aim to bolster the integrity and accuracy of the register and increase scrutiny on registered companies. From 2024, Companies House will have enhanced powers to ensure that anyone required to register does so, that information is accurate and complete, and that records do not create misleading or false impressions – all measures to prevent companies from carrying out or facilitating unlawful activities.[117] Nevertheless, the volumes involved and speed at which Companies House must process information still risk leaving it vulnerable. Here, too, the use of AI could help. At a basic level, the use of digital-identity solutions could enable remote customer identification and verification and make the authentication of large financial transactions more robust. Natural-language processing can support more accurate, flexible and timely analysis of customer information, while AI and machine learning could be used to automatically analyse vast amounts of financial data.[118]

Recommendation

The government should invest in a new dedicated technical team within Companies House to design and implement cutting-edge tools that would identify and combat potential fraud. In line with previous recommendations made in TBI paper Governing in the Age of AI: A New Model to Transform the State*, Companies House could be named as an "AI exemplar" executive agency, providing it with a clear mandate to identify AI-enabled opportunities for improvements to productivity and efficiency and showcase their use.*

RECOVER MORE OF THE PROCEEDS OF CRIME

Recent media reports that several criminals were able to buy property in Dubai while in prison in the UK[119] illustrate the scale of the challenge when it comes to recovering criminal assets. In 2022 the Law Commission described the UK's regime for recovering the proceeds of crime as "inefficient, complex and ineffective".[120] It suggested a range of reforms, including accelerating the confiscation process, strengthening "restraint orders" to stop a defendant from protecting funds that might later be confiscated, updating the provisions that factor in a defendant's "criminal lifestyle" when assessing their benefit from crime and giving courts the power to impose "contingent enforcement orders" to recover criminals' assets if they do not pay back the proceeds of crime within a set time.

Earlier this year, the previous government introduced a number of these measures as part of the Criminal Justice Bill. As the Bill was not passed before Parliament was prorogued in May 2024, there is a risk that these measures will get lost unless reintroduced. Going further, the new government could take up another of the Law Commission's recommendations: establishing a national Criminal Asset Recovery Board accompanied by a national asset-management strategy. The strategy would join up law-enforcement agencies' responses, and crucially address the challenges posed by new technologies, including crypto-assets.

Recommendation
The government should implement the Law Commission's recommendations to improve the confiscation regime in full, including the creation of a national Criminal Asset Recovery Board and a national asset-management strategy. As recommended previously, recovered assets should be ringfenced to the SOC response.

Case study: Tracfin: financial intelligence to tackle illicit finance

According to the Global Organized Crime Index,[121] France has the highest organised-crime score in Western Europe.[122] A rise in homicides[123] in several French cities has been driven by violent competition between gangs linked to the drugs trade. In 2021, France had the highest national homicide rate[124] in Western Europe.

Tracfin, the French financial-intelligence unit, plays a crucial role in the fight against organised crime by analysing financial transactions and identifying suspicious patterns indicative of involvement in organised crime. Tracfin and other French authorities work closely with international partners and financial institutions to track and disrupt the flow of illicit funds across borders. In 2019, this way of working led to the dismantling of a major drug-trafficking network in Europe.

STRENGTHEN THE BORDER

Organised immigration crime is a persistent threat, due in part to increasing geopolitical instability causing forced displacement. Demand is growing for the services of OCGs offering illegal passage into Europe via road, air or sea routes; many involve the use of refrigerated HGVs or small boats, and all are highly dangerous for migrants and lucrative for criminals.[125] Organised immigration crime, particularly the influx of small-boat crossings to the UK,[126] places strain on the UK Border Force and dominated the UK political agenda under the last government. The higher volume of crossings and number of people arriving via small boat may point to an increase in professionalism amongst OCGs, and the increasing profitability of this type of crime.[127]

Beyond simply transporting people across borders, there is evidence of OCGs using migration to fuel other forms of SOC committed within the UK – through modern slavery and human trafficking. “Irregular” migrants are highly vulnerable to exploitation; there is evidence that OCGs prey on migrants who are already in the UK or offer crossings in return for forced criminal labour, particularly in the drugs trade.[128] Behind UK citizens, Albanian, Vietnamese, Indian and Romanian nationals are most commonly referred to the NRM as victims. The NCA reports that “exploitation in criminal activity” is the form of exploitation most often reported, making up 65 per cent of total referrals in 2023.[129] This exploitation refers to victims who are forced or compelled to commit crime, often drug offences such as county-lines drug trafficking.[130]

Recommendation
The government has already promised a new Border Security, Asylum and Immigration Bill. To make the UK a less attractive target for OCGs involved in exploiting migrants, the government should introduce a set of measures to strengthen the border, such as:

- *Opening safe and legal asylum routes by creating a new humanitarian visa that would grant asylum seekers the right to have their claims properly considered in British embassies abroad*
- *Deterring asylum seekers from arriving outside of these routes by negotiating a new agreement with the EU, or selected EU countries, to cover the safe return of those who have had their asylum claims rejected*
- *Speeding up processing times by establishing a taskforce to examine the drivers behind slower processing times and falling returns, reintroducing targets and establishing stronger case-management processes, including AI systems that would better triage and prioritise cases of the most vulnerable applicants*
- *Implementing a digital-ID system, as previously mentioned, to streamline employment and residency checks and reduce OCGs’ ability to exploit migrants seeking employment in the informal labour market*

3. Bolster law enforcement's ability to respond

CREATE A MORE JOINED-UP AND EFFECTIVE POLICING STRUCTURE

The current policing model is based around 43 individual forces and was designed for an age when most recorded crimes were geographically bounded – committed by local offenders against local victims. It is fundamentally ill suited to 21st-century SOC, most of which takes place online and extends beyond policing boundaries (often across borders), creating severe challenges for the police's ability to respond. The changing nature of SOC also increasingly requires the police to be able to access certain specialist capabilities, many of which require considerable investment and training. These would be better developed at scale, rather than replicated inconsistently up to 43 times. Limited dedicated SOC funding, inefficient governance structures and an unambitious legal framework hamper innovation and create an ineffective response. The SOC threat is rapidly evolving: the UK needs a system which can respond with agility and efficiency.

The NCA was established in 2013 to lead and coordinate the UK's efforts to combat SOC. It is supported by a network of ROCUs, which lead the regional response and provide specialist policing capabilities to forces. Together, they were designed to improve the response to cross-border threats, yet efforts to tackle SOC remain disjointed. A 2020 inspection by HMICFRS found that the tasking of ROCUs and forces lacked effectiveness[131] and that capabilities were duplicated between the NCA and ROCUs.[132] Part of this comes from a lack of clout; the NCA is too small and ROCUs are not statutory bodies, so do not have the power to task police forces, despite coordinating regional law-enforcement activity.

Recommendation
Oversight of the UK's SOC response should be strengthened at a national level with the appointment of a dedicated minister. This could be a cross-government post sitting in the Cabinet Office and covering the Home Office, the Ministry of Justice, the Foreign, Commonwealth & Development Office and HM Treasury. Tackling SOC should form part of the government's "take

back our streets" mission.

Recommendation

The government should create a single UK-wide police force to lead on all crimes and threats that cross force boundaries – encompassing counterterrorism, SOC and cyber-enabled crime. The Home Office should consult on the optimal relationship between the UK-wide force, ROCUs and local forces to ensure effective information sharing, collaboration on shared tasks and adequate victim support. The new force would have a stronger operational focus than the current NCA.

As an interim step, the government should create a powerful regional tier of policing by putting the existing network of ROCUs on a statutory footing. This change would empower them to invest in specialist capabilities and, where necessary, direct anti-SOC operations carried out by local forces.[133] *Those forces would remain overseen by police and crime commissioners, but would be limited to policing geographically bounded crimes. The NCA should be given explicit authority to direct ROCUs so their efforts are aligned with the national SOC strategy. In time, ROCUs could be subsumed into the UK-wide force and act as its operational arm.*

ENABLE POLICING TO HARNESS THE POWER OF AI

The scale of online criminality dwarfs the resources and capabilities available to law enforcement. Even if the UK could afford to substantially expand police numbers, forces would struggle to keep up with the volumes involved and the pace at which crime is changing. The UK needs to rethink traditional approaches to fighting crime. The technology available today – especially AI – could transform law enforcement's ability to tackle SOC.

Goals for and timelines for how AI could transform policing

During this parliament: every force uses AI

Technology has the potential to maximise the use of police resources. Currently, police and law-enforcement officers spend a significant portion of their time on administrative tasks. The capability to help automate many time-consuming processes already exists and could be implemented widely and systematically. For example:

- Office-productivity tools such as Copilot and Gemini could be used to auto-summarise and auto-translate documents, which could streamline research.
- Redaction tools could be used, for example, to systematically blur out faces and number plates from videos, making them ready to use in court.
- Natural-language-processing (NLP) software – built using a type of AI which enables computers to understand, analyse and generate human language – can transcribe bodycam footage and automate analysis of police reports and emergency-call transcripts.

Beyond administrative tasks, generative AI has the capability to aid investigations and disrupt criminals. For example:

- Computer-vision technology, which involves teaching computer systems to understand, interpret and analyse digital images and video footage, could be used to survey CCTV footage.
- The search capabilities of large-language models could improve the searchability of digital evidence across multiple large law-enforcement data sets.

- Machine-learning technology is already being used to identify and remove illegal websites and deep-fake images.
- Forces are increasingly using software that allows the public to easily upload digital evidence, such as photos and videos, to a secure location. The Queensland Police Service have integrated this software into their dispatch system, allowing them to receive significantly more submissions from the public.[134]

Within ten years: an AI-aided police force

Over the longer term we can imagine an AI-aided police force.

In line with a recommendation previously made in the TBI paper *Governing in the Age of AI: A New Model to Transform the State*, we could envisage police officers being supported in their day-to-day tasks by a multidisciplinary-AI-support-team (or MAST) platform that would integrate a wide range of AI-enabled tools. This platform wouldn't replace the role of officers but would allow them to deal with the volume of online criminality and focus their skills and time where they are needed most.

AI agents would carry out a number of tasks. For example, they could survey the vast quantities of unstructured free-text data commonly collected by forces during investigations to identify additional leads and patterns. AI agents could also trawl the dark web for illicit activity, identifying and engaging with potential criminals in chat rooms and reporting back to human officers.

In addition, computational twins[135] could be used by police forces to simulate and assess their response to anything from city-wide emergencies to the day-to-day distribution of resources. For example, in London the

SafeStats portal securely aggregates geographically linked public-safety data to support better decision-making across the city.[136] In Guangdong province, the provisional police department has worked with city authorities to create a real-time map of the city, showing where incidents are happening, as well as mapping public interactions, calls, use of police resources, and potential threats. Feeds from ten separate departments are consolidated in the model, giving the police force a complete and real-time overview.

While many such capabilities exist and are being used, their application at the national level is inconsistent and hampered by several barriers. The current supporting infrastructure is old and disjointed. The Police National Computer (PNC), a critical piece of technological infrastructure that holds records on more than 13 million citizens and is more than 50 years old, is gradually being replaced with the Law Enforcement Data Service (LEDS) but this has been slow and faced significant challenges. Meanwhile, forces rely on several different databases and systems that often do not speak to each other.

In addition, the ability to harness new technology depends on forces' ability to access and deploy specialist capabilities, many of which require large amounts of investment and training. Yet currently investment is fragmented across the 43 forces and standards vary hugely across the country. There are savings and efficiencies to be generated from these being pooled and developed at scale.

Concerns have also been raised about the capabilities of police forces to investigate and tackle crimes with a digital element. While some forces benefit from dedicated cyber units and specialist staff, access to specialist capability is largely a postcode lottery. Due to piecemeal training and poor recruitment, many officers report feeling unprepared to deal with online fraud and do not believe their force has the sufficient skills and capabilities to investigate cyber-crime.

Recommendation
Alongside finalising the delivery of LEDS, the government should accelerate the interoperability of police data by issuing a clear steer to forces that they should prioritise interoperability in their procurement. In addition, the government should direct additional capital funding towards accelerating the interoperability of police data, with a focus on "best affordable" solutions over a purely cost-based approach. The APA should develop interoperability principles and requirements to reduce duplication and ensure consistency between forces.

Recommendation
The National Policing Board should take the lead in developing a national workforce plan to address the skills and capability gaps identified in the SOC technology strategy and gap analysis that would be led by the SOC Lab. Within the next year, the College of Policing should review the skills of officers in SOC-related roles and develop appropriate training.

Recommendation
In the longer term, the new SOC Lab could work with the Department for Science, Innovation and Technology to create a database collating data from police forces, national bodies and partners in the financial sector as well as other relevant data sources. This database would feed into a SOC computational twin that would reflect the extent of SOC across the country and allow policymakers to model and simulate the impact of different interventions.

A significant barrier to SOC investigations is the exchange of data and information across borders. The processes by which the UK receives and shares data with Europe via Interpol, for example, are beset by problems. Police officers interviewed as part of a review into UK-EU law-enforcement cooperation post-Brexit stated that, on top of bureaucratic processes and insufficient links between systems, both of which slow down UK access to information, new processes introduced because of Brexit mean that information can be copied to UK systems incorrectly, leading to UK law-enforcement agencies holding inaccurate information. One officer stated that this can result in officers not knowing if foreign nationals are wanted, or even if they are in the UK.

The EU Strategy to Tackle Organised Crime 2021–2025 introduced Prüm II, an improved biometric data-sharing platform including new data-exchange categories, automated exchanges and biometric search services. Europol is now included in the Prüm II network, which allows direct data exchanges as well as access to third-country data stored by Europol. The UK is not currently part of Prüm II, which came into effect in March 2024. If the UK continues to choose to not participate in Prüm II, UK access to EU-wide databases could be withdrawn, with the UK losing access to biometric information on criminals operating in Europe.

Recommendation
The UK should quickly choose to participate in Prüm II, and prepare law-enforcement systems for the new technologies that must be put in place to be able to participate in it. It should also prioritise the implementation of I-LEAP, which connects the UK to INTERPOL's databases. This is helpful because the UK's connection with EU data-sharing systems was lost after Brexit. I-LEAP is currently only set to be implemented in 2027–2028 – which is far too slow.

The principle of policing by consent requires a careful and deliberative approach to the ethical questions raised by the application of technology in policing. The piecemeal approach to the use of technology has led to some forces operating without proper oversight. For example, in January 2024 the Justice and Home Affairs Committee published a letter to the home secretary stating that there are no rigorous standards or systems of regulation in respect of the use of live facial recognition,[137] exacerbating existing concerns around the use of new technology in policing. These concerns are not unfounded: many of these technologies are emerging and their application to policing is largely untested. The potential for misuse is important, with wide-ranging implications for citizens' rights and trust in law enforcement.

Recommendation
The Responsible Technology Adoption Unit should work with the NCA, NPCC and others to develop a governance model for the use of technology in law enforcement. As previously suggested by the NPCC, a core principle should be that the public's view is proactively built into an ethical assessment at the design stage of any digitally enabled service improvement.

How technology is being used to combat SOC around the world

The steps taken by countries around the world to tackle SOC crime illustrates the scale of the challenge the UK is facing when attempting to increase our defences against SOC.

China

In 2018, the Chinese government announced its plans to invest $150 billion by 2030 in machine-learning programmes to create an AI-powered security system that is “omnipresent, fully networked and fully controllable”. [138] The government is working with the AI company CloudWalk to develop a “police cloud” – a vast database of information on every citizen, including criminal and medical records, travel bookings, social-media comments and store visits. The result of this is a big-data rating system that claims to identify highly suspicious groups based on background and behaviour signals, helping police to identify high-risk individuals and streamline crime-monitoring and prevention efforts. The Chinese police are also working with big-data tools to analyse motion and behaviour data to detect criminal activities. For example, traffic authorities in Jinan used gait analysis – a form of biometric technology still in its infancy and lacking in evidence – to identify jaywalking and track down violators.

Saudi Arabia

Saudi Arabia is trialling the use of machine learning in policing. Algorithms analyse historical crime data to predict hotspots and times of increased criminal activity. The Saudi government has also partnered with Zenith

Technologies and developed the first electronic police car. The new vehicle leverages embedded AI cameras that in real time provide 360-degree situational awareness, automatic number-plate recognition, face recognition and traffic enforcement.

South Korea

In November 2023 South Korea unveiled a comprehensive four-year blueprint outlining how AI will be employed to predict and combat various criminal activities. The blueprint includes plans to use AI to:

- combat voice phishing, a crime that predominantly takes place through the exploitation of mobile telecommunications
- use security cameras to detect abnormal behaviour and whether someone is carrying a weapon
- build a real-time map that tracks drug cases, facilitating the tracing of drug-distribution routes
- establish a police-agency metaverse
- develop a system to automatically track banned virtual assets
- create a cyber-training institution at the Advanced Public Security Center[139]

04

Conclusion

The threat from SOC may seem remote but it is pervasive. It destroys lives, weakens communities, threatens national security and costs the UK economy billions of pounds a year.

The way the UK responds must adapt to the scale or nature of 21st-century SOC. In this paper we have set out an ambitious new framework which aims to make the UK a hostile environment for organised criminals. We propose a series of measures to make it more difficult and less attractive to commit crimes in the UK, and to reduce the scale of the threat, thereby making it easier for a reformed and bolstered law-enforcement framework to respond.

While this paper is focused on the national response, it is clear that the UK cannot tackle this threat alone. A separate set of responses is needed to improve cooperation with international partners. This will be the focus of a separate paper.

The new government has made “taking back our streets” one of its five missions of government. It will not achieve its aim unless it takes on the threat of serious organised crime.

05

Methodology

Deltapoll surveyed a representative sample of 1,519 adults in Great Britain between 16–19 February 2024 to understand their views of SOC and possible policy solutions to it. Data were weighted to age and education within gender, region, social grade, 2019 general-election vote and 2016 referendum vote. Deprivation was measured using data derived from the 2021 UK census.

Endnotes

[1] https://assets.publishing.service.gov.uk/media

[2] https://www.nationalcrimeagency.gov.uk/nsa-2024

[3] https://assets.publishing.service.gov.uk/media/65796db30467eb000d55f677/SOC%5FStrategy%5F2023%5F28.pdf

[4] 37 per cent, according to the latest NCA estimate: https://www.nationalcrimeagency.gov.uk/threats/nsa-fraud-2024

[5] https://www.nationalcrimeagency.gov.uk/news/online-is-the-new-frontline-in-fight-against-organised-crime-says-national-crime-agency-on-publication-of-annual-threat-assessment

[6] https://www.gov.uk/government/publications/the-terrorism-acts-in-2020/the-terrorism-acts-in-2020-report-of-the-independent-reviewer-of-terrorism-legislation-accessible-version

[7] This includes high-harm and cross-border burglary, vehicle crime, robbery, heritage and cultural-property crime, plant and agricultural theft, and metal and infrastructure crime.

[8] www.nationalcrimeagency.gov.uk/nsa-2024

[9] https://nationalcrimeagency.gov.uk/nsa-overview-of-soc

[10] https://assets.publishing.service.gov.uk/media/, page 11

[11] www.nationalcrimeagency.gov.uk/who-we-are, page six

[12] https://assets.publishing.service.gov.uk/media/65796db30467eb000d55f677/SOC%5FStrategy%5F2023%5F28.pdf, page nine

[13] https://assets.publishing.service.gov.uk/media, February 2019. Adjusted for inflation to 2023 equivalent: https://www.gov.uk/government/statistics

[14] https://assets.publishing.service.gov.uk/media

[15] Magdalena Andersson, then prime minister of Sweden, argued in 2022 that rising gang violence is due in part to a failure to integrate migrants into society. Links between migration and organised crime have also been drawn by prominent UK politicians: in 2023 Suella Braverman stated that “people coming here illegally possess values at odds with our country”, linking this with heightened levels of drug dealing.

[16] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime

[17] � https://www.nationalcrimeagency.gov.uk/threats/nsa-fraud-2024

[18] https://www.nationalcrimeagency.gov.uk/threats/nsa-fraud-2024

[19] https://www.nationalcrimeagency.gov.uk/images/NSA%5F2023%5FWebsite%5F-%5FPDF%5FVersion%5F1.pdf

20 https://www.ons.gov.uk/peoplepopulationandcommunity

21 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2023

22 https://www.somerset.gov.uk/finance-performance-and-legal/fraud/#:~:text=The%20National%20Crime%20Agency%20reports,on%20the%20year%202020%2F21

23 https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages

24 https://www.emcdda.europa.eu/publications/eu-drug-markets

25 https://www.statista.com/statistics/264806/worldwide-production-quantity-of-cocaine-since-1994/

26 https://www.gov.uk/government/publications/review-of-drugs-phase-one-report

27 Opium-poppy cultivation in Afghanistan saw a sharp decline after the Taliban takeover in 2021 and the ban on cultivation. Nevertheless, opium production in Afghanistan was higher in 2022 (6,200 tonnes) and at its peak in 2017 (9,000 tonnes), than in 2013 (5,500 tonnes): https://www.emcdda.europa.eu/publications/eu-drug-markets/heroin-and-other-opioids

28 https://www.nationalcrimeagency.gov.uk/threats/nsa-drugs-2024

29 The NCA estimates that there are around 600 active lines operating.

30 https://www.unodc.org/res

31 https://www.europol.europa.eu/crime-areas/drug-trafficking/synthetic-drugs

32 https://www.gov.uk/government/statistics/irregular-migration-to-the-uk-year-ending-december-2023/irregular-migration-to-the-uk-year-ending-december-2023

33 https://www.gov.uk/government/statistics/irregular-migration-to-the-uk-year-ending-december-2023

34 https://www.nationalcrimeagency.gov.uk/images/NSA%5F2023%5FWebsite%5F-%5FPDF%5FVersion%5F1.pdf

35 https://www.gov.uk/government/publications/from-harm-to-hope-a-10-year-drugs-plan-to-cut-crime-and-save-lives/from-harm-to-hope-a-10-year-drugs-plan-to-cut-crime-and-save-lives

36 https://www.nao.org.uk/wp-content/uploads/2019/03/Tackling-serious-and-organised-crime.pdf

37 https://www.gov.uk/government/statistics/modern-slavery-nrm-and-dtn-statistics-end-of-year-summary-2023/modern-slavery-national-referral-mechanism-and-duty-to-notify-statistics-uk-end-of-year-summary-2023

38 https://www.unseenuk.org/calls-to-modern-slavery-helpline-rise-for-fourth-year-running/

39 In 2024, the NCA also reported that 15 per cent of girls and 5 per cent of boys experience some form of sexual abuse before the age of 16: https://www.nationalcrimeagency.gov.uk/threats/nsa-child-sexual-abuse-2024

40 https://riskbulletins.globalinitiative.net/ukr-obs-001/04-gang-wars-in-sweden-indicate-a-

demand-driver.html

41 https://www.lemonde.fr/en/france/article/2023/05/24/drug-trafficking-in-france-perpetrators-and-victims-of-violence-are-increasingly-younger_6027864_7.html

42 https://www.bbc.co.uk/news/world-europe-64426289

43 https://www.interpol.int/en/News-and-Events

44 Ofcom estimated in 2023 that 90 per cent of UK individuals aged 16 or over use the internet at home. https://www.ofcom.org.uk

45 A well-known example is EncroChat, an encrypted communications tool often used by OCGs, which was dismantled in 2020 through a joint European operation.

46 https://www.nationalcrimeagency.gov.uk/technological-tipping-point-reached-in-fight-against-child-sexual-abuse

47 https://www.nationalcrimeagency.gov.uk/nsa-overview-of-soc-2024/nsa-cross-cutting-enablers-2024

48 https://www.europol.europa.eu/media-press

49 https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cybercrime

50 https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups

51 https://64e09bbc

52 https://64e09bbc

53 https://www.rusi.org/explore-our-research

54 https://www.nao.org.uk/wp-content/uploads/2019/03/Tackling-serious-and-organised-crime.pdf

55 https://www.nationalcrimeagency.gov.uk/news/director-general-delivers-keynote-speech-at-the-rusi-soc-conference

56 Campbell, 2014; Levi et al, 2015; UNODC, 2015

57 https://assets.publishing.service.gov.uk/media

58 https://www.toexprogramme.co.uk/about-us/vision-and-mission/

59 https://www.toexprogramme.co.uk/workstreams/intelligence-operating-model/

60 https://assets.publishing.service.gov.uk/media

61 https://assets.publishing.service.gov.uk/media

62 https://www.nao.org.uk/wp-content/uploads/2023

63 HM Government, ***CONTEST – The United Kingdom's Strategy for Countering Terrorism,*** 2023; HM Government, ***No Place to Hide, Serious Organised Crime Strategy 2023-2028;*** National Audit Office, ***Home Office Departmental Overview, 2022-23***

[64] https://www.gov.uk/government/publications/serious-and-organised-crime-strategy-2023-to-2028

[65] https://committees.parliament.uk/writtenevidence

[66] https://assets-hmicfrs.justiceinspectorates.gov.uk/uploads

[67] https://rusi.org/explore-our-research/publications/commentary/bribery-and-corruption-unholy-cocktail-outsider-and-insider-threats

[68] https://www.nationalcrimeagency.gov.uk/news/director-general-delivers-keynote-speech

[69] https://www.nationalcrimeagency.gov.uk/news/director-general-delivers-keynote-speech

[70] The NAC acts as the NCA's centre for assessed intelligence reporting

[71] https://assets.publishing.service.gov.uk/media/5af1991040f0b642e2d8fa06/6.4391%5FCO%5FNational-Security-Review%5Fweb.pdf

[72] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2023/07/IRTL-Moret-Report.pdf

[73] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2022/04/Terrorism-Acts-in-2020.pdf

[74] The Independent Reviewer highlights the effective application of the power in relation to British citizens travelling across UK borders to Islamic State-controlled territories between 2013 and 2017: https://www.gov.uk/government/publications/the-terrorism-acts-in-2020/the-terrorism-acts-in-2020-report-of-the-independent-reviewer-of-terrorism-legislation-accessible-version

[75] A 2016 independent report rated London's counterterrorism measures, for example, as "among the best in the world" – David Omand, "Keeping Europe safe: counter-terrorism for the continent", *Foreign Affairs*, September/October 2016, 95(5):83. Another noted: "There can be no room for complacency, but the UK's measures to combat terror are more advanced than those of any of its near partners, except possibly the US": https://www.jstor.org/stable/resrep04249.13?searchText=&searchUri=&ab%5Fsegments=&searchKey=&refreqid=fastly-default%3A9ada9ee116cc20a9b2b74358ada17975&seq=6

[76] For example, in 2017, the former director of the Royal United Services Institute wrote that "the UK's measures to combat terror are more advanced than those of any of its near partners, except possibly the US": https://www.jstor.org/stable/resrep04249.13?searchText=&searchUri=&ab%5Fsegments=&searchKey=&refreqid=fastly-default%3A9ada9ee116cc20a9b2b74358ada17975&seq=6

[77] David Omand, who served as the first UK security and intelligence coordinator, wrote that "other European governments have lagged behind the United Kingdom in developing capabilities and legal frameworks for digital intelligence gathering and in cultivating effective cooperation between their many agencies" and "the British government adopted a counterterrorism strategy known as CONTEST, which aimed to 'reduce the risk to the UK and its interests overseas from terrorism, so that people can go about their lives freely and with confidence.'" He concluded that "So far, the British approach has worked": https://www.foreignaffairs.com/articles/europe/keeping-europe-safe

[78] https://www.jstor.org/stable/

resrep04249.13?searchText=&searchUri=&ab%5Fsegments=&searchKey=&refreqid=fastly-default%3A9ada9ee116cc20a9b2b74358ada17975&seq=4

[79] https://www.gov.uk/government/publications/separation-centre-policy-framework

[80] https://researchbriefings.files.parliament.uk/documents/CBP-9899/CBP-9899.pdf

[81] https://www.gov.uk/government/publications/handling-crimes-in-prison-protocol/annex-b-requirement-relating-to-terrorism-and-terrorism-connected-offences-and-prisoners-convicted-of-terrorism-tacttact-connected-offences-prisone

[82] https://www.gov.uk/government/publications/separation-centre-policy-framework

[83] https://www.justiceinspectorates.gov.uk/hmiprisons/wp-content/uploads/sites/4/2022/08/Separation-centres-web-2022.pdf

[84] https://eur-lex.europa.eu/legal-content

[85] www.westofengland-ca.gov.uk

[86] https://www.drewry.co.uk/maritime-research-opinion-browser/maritime-research-opinions/smart-container-fleet-to-expand-8-fold-over-the-next-5-years

[87] https://unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperSmartContainers.pdf

[88] https://assets.publishing.service.gov.uk/media/650b1b8d52e73c000d54dc82/CONTEST%5F2023%5FEnglish%5Fupdated.pdf

[89] https://assets.publishing.service.gov.uk/media/65796db30467eb000d55f677/SOC%5FStrategy%5F2023%5F28.pdf

[90] https://assets.publishing.service.gov.uk/media/65c34bf212d5f1000d375171/NCARRB_2023_report_-_web_accessible_version.pdf

[91] https://committees.parliament.uk/writtenevidence/127392/html/

[92] Between 2020–21 and 2022–23, £1.9 billion was raised. Specifically, £917 million was raised from every law-enforcement agency
orders, forfeiture orders and civil-recovery orders. In addition, £1 billion was raised from the FCA through fines. For more informat
https://www.gov.uk/government/statistics/asset-recovery-statistical-bulletin-financial-years-ending-2018-to-2023#:~:text=Asset%20Recovery%20Statistics%2C%20financial%20years%20ending%202018%20to%202

[93] As introduced by the Economic Crime and Corporate Transparency Act.

[94] https://www.spotlightcorruption.org

[95] https://www.spotlightcorruption.org

[96] Malus and clawback are the processes by which authorities can recover remuneration already paid to directors (clawback) or to withhold pending awards (malus), when specific “trigger points” or circumstances have occurred.

[97] https://assets.publishing.service.gov.uk/media

[98] https://questions-statements.parliament.uk/written-questions

[99] https://assets.publishing.service.gov.uk/media

[100] https://assets.publishing.service.gov.uk/media

[101] https://assets.publishing.service.gov.uk/media

[102] https://assets.publishing.service.gov.uk/media

[103] https://www.theguardian.com/world/2022/jul/03

[104] https://dataunodc.un.org/dp-drug-seizures

[105] https://web.archive.org/web/20231002181358/https://www.government.nl/latest/news/2022/09/20/investing-in-tackling-crime-and-access-to-justice

[106] https://dataunodc.un.org/dp-drug-seizures

[107] This aim was behind the creation of the NCA's National Cyber Crime Unit, and the development of Regional Cyber Crime Units.

[108] This involves turning identifiable data into a string of random characters, which can then be used to represent the original identifier but not to re-identify the data.

[109] https://cfit.org.uk/

[110] https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2

[111] https://www.transparency.org.uk/uk-money-laundering-stats-russia-suspicious-wealth

[112] https://assets.publishing.service.gov.uk/media

[113] https://assets.publishing.service.gov.uk/media/649e92d2bb13dc000cb2e3bf/AML%5FReform%5FConsultation%5FDocument%5F-%5FFINAL.pdf

[114] https://www.transparency.org.uk/uk-money-laundering-stats-russia-suspicious-wealth

[115] https://assets.publishing.service.gov.uk/media/5f7ed12ad3bf7f019966930f/corporate-transparency-register-reform-government-response.pdf

[116] https://www.ft.com/content/beed28a3-f08f-4d6c-bf5d-b3122d862a4a

[117] https://companieshouse.blog.gov.uk

[118] https://www.fatf-gafi.org/content

[119] https://www.thetimes.co.uk/article

[120] https://lawcom.gov.uk/project/confiscation-under-part-2-of-the-proceeds-of-crime-act-2002/

[121] The Global Organized Crime Index is run by the Global Initiative Against Transnational Organized Crime (GI-TOC). It is a multi-dimensional tool that assesses the level of criminality and resilience to organised crime for 193 countries along three key pillars: criminal markets, criminal actors and resilience. For more information, see here: https://ocindex.net/about

[122] https://ocindex.net/country/france

[123] https://www.france24.com/en/live-news; https://www.lemonde.fr/en/france/article/2023/05/24/drug-trafficking-in-france-perpetrators-and-victims-of-violence-are-increasingly-

younger%5F6027864%5F7.html

[124] https://www.unodc.org/documents/data-and-analysis

[125] https://www.nationalcrimeagency.gov.uk/threats/nsa-organised-immigration-crime-2024

[126] https://www.nationalcrimeagency.gov.uk/threats/nsa-organised-immigration-crime-2024

[127] https://www.rusi.org/explore-our-research/publications/commentary/organised-immigration-crime-uk-resilient-business-model

[128] https://www.rusi.org/explore-our-research/publications/commentary/organised-immigration-crime-uk-resilient-business-model; https://www.bbc.co.uk/news/uk-wales-61564660

[129] https://www.nationalcrimeagency.gov.uk/threats/nsa-modern-slavery-and-human-trafficking-2024#:~:text=Exploitation%20in%20criminal%20activity%20is,county%20lines%20or%20cannabis%20cultivatio

[130] https://www.nationalcrimeagency.gov.uk/threats/nsa-modern-slavery-and-human-trafficking-2024

[131] https://assets-hmicfrs.justiceinspectorates.gov.uk. Other issues highlighted are a lack of accountability and oversight of ROCU tasking, leading to inconsistencies in ROCU activity. Sometimes ROCUs were dealing with lower-level threats than police forces.

[132] https://www.nao.org.uk/wp-content

[133] The latest SOC strategy outlines the introduction of a NPCC ROCU Strategy, delivered by a national ROCU Executive Board. It is unclear to what extent these measures have been successful in strengthening the coordination of the regional and local response. No place to hide: serious and organised crime strategy 2023 to 2028 (accessible version) - GOV.UK (www.gov.uk)

[134] https://fst.net.au/government-news

[135] Computational twins are areas to which data can be added, and often serve as digital replicas of cities. Artificial intelligence is then applied to the data to forecast and create simulations.

[136] https://data.london.gov.uk/blog/future-proofing-access-to-crime-and-safety-data-in-london/

[137] https://committees.parliament.uk/committee

[138] Minority report: machine learning and crime prevention in China - Technology and Operations Management (harvard.edu)

[139] https://www.koreaherald.com

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Follow us

facebook.com/instituteglobal
x.com/instituteGC
instagram.com/institutegc

General enquiries

info@institute.global