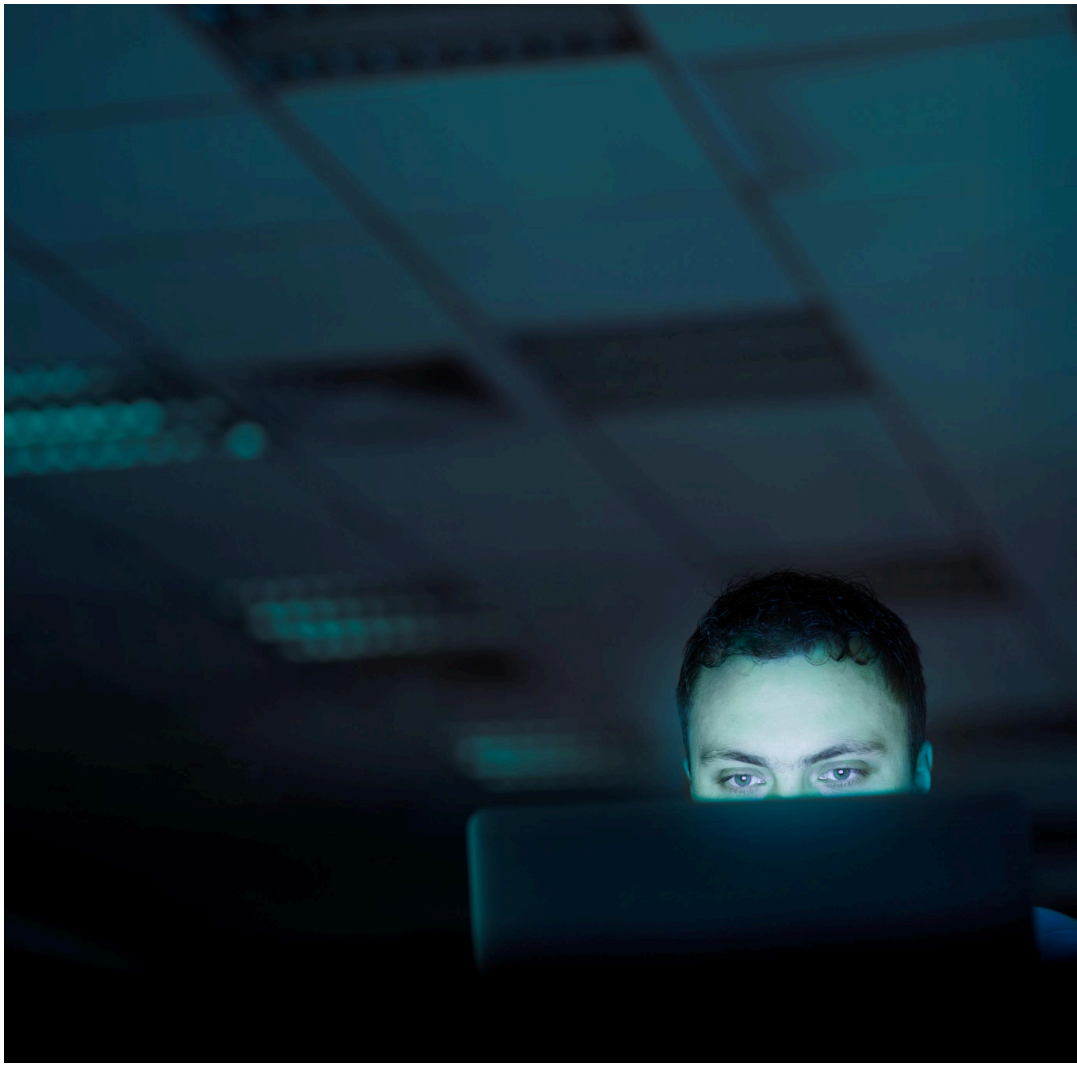
AUGUST 2025

LAURA BRITTON
SOPHIE DAVIS
CATRINA BOMFORD
ALEXANDER IOSAD
TIM RHYDDERCH



A New International Approach to Beating Serious and Organised Crime

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Contents

Contributors: Manon Roberts (Crest Advisory)

Foreword

It almost feels like a cliché to say that serious and organised crime (SOC) is evolving rapidly and continuously in scale, shape and sophistication. However, after five years leading INTERPOL's global operational responses to crime and terrorism, I've seen first-hand how far these escalating threats are outstripping our well-intentioned but linear, dated and fragmented response mechanisms.

In any losing battle, it is necessary to draw back and reconsider one's approach. That is why it is time for us to recognise that SOC is no longer simply a criminal-justice matter alone – it has become a societal threat, and it is time it was treated with the seriousness, focus and renewal of tactics this demands.

My time as Executive Director of Police Services at INTERPOL fundamentally changed not just the way I see crime but the way I see the business models behind that crime. I came into this role from specialist commands at New Scotland Yard and geographic leadership as Chief Constable of Essex. But when I began looking at crime through its actual drivers and enablers – technology, transport, communication and broader logistical systems – it became impossible to ignore just how far our current models were falling short.

The implications are profound. This unique role offered a rare perspective and it was an immense privilege. Whether it was the fallout of the Afghan government's collapse on drug flows and human trafficking, or the levels of sophistication, reach and ruthlessness of West African organised crime groups, the conclusion was the same: the criminal threats have moved on, and we haven't.

Working internationally, it is clear how SOC embeds itself in our economies, institutions and in some cases governance and political systems. These subtle, malign networks are built to avoid law-enforcement attention, to adapt on the fly, to exploit our media and political distractions, and our global obsession with "perimeter" mindsets. The reality is that not only is law enforcement often too busy and too consumed by existing threats to notice the emergence of new, more sinister ones, but its global architecture is fractured, duplicative and falling behind.

Nowhere is this as evident as in the use of technology, which has become the ultimate enabler for SOC. From AI and deepfakes to encrypted comms and crypto flows, organised crime groups are exploiting every tool at their disposal. They're using entrepreneurial models to recruit, move money, manage their supply chains and to attack at speeds and volumes that overwhelm traditional policing models.

This paper makes the case plainly: in the face of such technically enabled criminal business models, if we don't treat our data and computing power as strategic assets, we are choosing to lose.

Law enforcement is still chasing symptoms, not systems. Exceptional individuals working in law enforcement are constrained by legacy tools, bureaucratic structures and performance frameworks that were created for a bygone age. Prosecutions take years. Trials are complex and juries are expected to seize complex legal and evidential issues. Meanwhile, the criminal networks regenerate.

This paper highlights the urgent need for a bolder, more strategic and proactive set of tools that sit beyond law enforcement – including sanctions, online disruption and new global mechanisms that match the transnational nature of the threat. It is refreshing because it challenges the orthodoxy and questions the institutional inertia that prevents us from taking a fundamentally different tack: one that focuses on enablers, is rooted in disruption and built on bold, trusted partnerships.

Arrests alone will never dismantle criminal economies. Organised crime functions as an economy, and must be considered and tackled accordingly. This will require disrupting logistics, targeting financial facilitators, and redirecting seized assets to strengthen the very systems needed to fight back.

This situation also means the private sector must at long last be integrated into the frontline response. Finance, tech, logistics and data systems are being exploited daily, yet their operators remain on the sidelines, or are brought in through fragmented, ad hoc efforts. These sectors can see the damage, and wish to help, yet we just haven't made it easy for them. This paper rightly calls for their operational integration, as part of a strategic design, as essential and included partners, not as an afterthought.

No matter how imperfect or distasteful, we must be willing to put a value on serious and organised criminal harms, exactly in the way we do with other global security threats. Too often politicians avoid attaching a price to abuse and exploitation as it highlights the scale of what is happening to the public and the media. But if we're serious about resourcing a meaningful and sustainable response, we can no longer afford to look away. Influence, funding and political attention follow data. A serious response must follow the same logic.

In the same vein, we cannot afford to ignore the geopolitics of SOC. Today on the global stage and even at a domestic level, consensus is hard-won in a world defined by distrust, instability and polarised politics. But that's no excuse to retreat. Democracies cannot afford to treat SOC as an abstract or future concern. We must learn the lessons from across the world – just because it is difficult to see, does not mean it is not already here, not already shaping global systems, and it demands a response as strategic, coordinated and relentless as the threat itself.

The path forward will not be easy, but the case for change is clear. Conventional structures and risk-averse strategies will not meet the moment. It is time for a new mindset: one that treats data and computing

power as strategic assets, accepts disruption as vital tools, and one that is willing to experiment with new institutional models that break with convention.

The ideas set out here reflect that new mindset. They propose not incremental reform, but a fundamental rethink of how the international community responds to SOC. The goal is not simply to cope with today's threat landscape, but to get ahead of it.

This moment demands strategic ambition and operational realism, and, above all, urgency. Criminals relish our adherence to old models. SOC has already shaped the world around us.

Our response must now do the same.

Sir Stephen Kavanagh, DCMG, QPM, DLSecretary General of the International Centre for Missing and Exploited Children, and former Executive Director of Police Services at INTERPOL

Executive Summary

Serious and organised crime (SOC) is escalating – becoming more quickly and more deeply embedded in the global economy than ever before. It is no longer just a law-enforcement challenge; it is a strategic threat that destabilises communities, distorts markets and undermines national security.

Transnational criminal networks are adapting at pace. They exploit geopolitical instability, emerging technologies and gaps between national systems. Their operations are decentralised, digitally enabled and remarkably resilient. Meanwhile, global responses remain slow, siloed and reactive. The world – with the UK in a pivotal position – must act now, or the cost will be catastrophic.

The financial impact of SOC is staggering. In 2023 alone, an estimated $3.1 trillion in illicit funds moved through the global financial system. Drug trafficking accounted for $782.9 billion, human trafficking for more than $346 billion. These are not abstract numbers – they represent human suffering, institutional corrosion and economic distortion on a vast scale.

Organised criminal groups (OCGs) are poly-criminal and borderless, relying on legitimate systems – logistics chains, financial networks, shell companies, digital platforms – to operate. They innovate faster than enforcement can respond. The boundaries between state, legal and criminal actors are blurring, with hostile states increasingly using OCGs as proxies for strategic and financial gain.

The UK has taken important steps since the Tony Blair Institute for Global Change's *A New Approach to Serious and Organised Crime in the UK*, including new counter-terrorism-style powers, a dedicated sanctions regime for organised immigration crime and a stronger focus on dismantling gang business models. But these remain national measures in an international context. Without deeper, faster, more strategic global coordination, domestic reforms will always be outpaced.

The diagnosis is clear: SOC thrives on fragmentation, loopholes and lagging cooperation, and the solution must match its scale and agility – not with incremental tweaks, but with a fundamental reset of the international approach.

TBI proposes an International Serious and Organised Crime Alliance – a core group of trusted nations and private-sector partners, operating with speed, trust and shared purpose.

This Alliance would:

- Forge an agile partnership for intelligence, technology and operational coordination.
- Target criminal networks at their source, dismantling infrastructure and enablers.
- Leverage technology and public–private innovation to stay ahead of adversaries.

Its mission would be not simply to expand existing enforcement, but to deliver sustained disruption – pre-empting and dismantling the systems that make SOC possible.

The Alliance would concentrate on two overriding objectives:

First, **disrupt criminal business models** by raising the cost of illicit activity through coordinated sanctions, targeting enablers, choking logistics and reinvesting seized assets to strengthen vulnerable communities.

Second, **deploy technology at pace and scale** by creating a shared technology advantage through federated data infrastructure, pooled compute power and rapid innovation in detection and disruption tools.

Membership would require active data-sharing and a commitment to common operational standards, enabling real-time joint action.

Without bold, coordinated action, SOC will continue to erode resilience, institutional integrity and economic security worldwide. The Alliance offers a practical, systemic and vision-driven path to regain the initiative – shifting the balance of power away from criminal networks and towards states and communities.

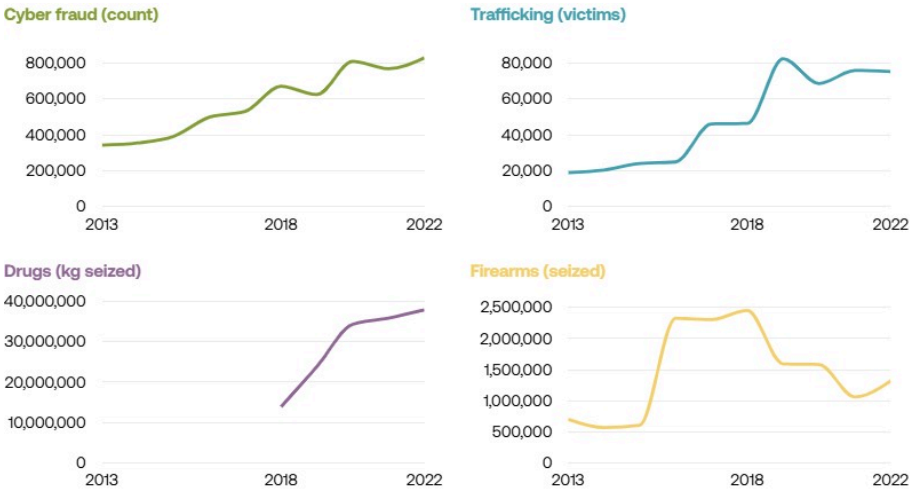
01

The Strategic Threat of Serious and Organised Crime

The threat posed by serious and organised crime (SOC) is increasing across the world. Global trends show that between 2013 and 2022, detected human-trafficking victims increased by 292 per cent, the number of cyber-fraud cases rose by 142 per cent and drug seizures grew by 172 per cent. Firearms trafficking, though growing more gradually, has increased by 88 per cent since 2013, driven partly by weapons leaking from conflict zones. The 2023 Global Initiative Against Transnational Organized Crime (GI-TOC) Index found that every criminal market tracked since 2021 had grown more pervasive globally.[1] The evidence is clear: SOC is expanding, evolving and becoming increasingly difficult to stop.

FIGURE 1

Threats across SOC categories have increased roughly two- to four-fold in just ten years



Source: UNDOC

Note: Values divided by 100 for display.

These headline figures only scratch the surface. SOC does not lend itself to straightforward metrics. It transcends borders, operates in the grey zones of law-enforcement capabilities and exploits weak institutional capacity, while also taking advantage of licit trade infrastructure, internet platforms, financial services and banking systems. To measure SOC is to grapple with the trafficking of people, arms, commodities and drugs, as well as environmental and cyber-crime conducted by multinational networks across porous borders with diverse enforcement regimes.

At the global level, the United Nations Office on Drugs and Crime (UNODC) provides the most comprehensive data set on SOC, covering drug trafficking, human exploitation and environmental crime. But its estimates are constrained. Seizure data, often used as a proxy, reflects law-enforcement activity as much as criminal prevalence. Increases may indicate better detection rather than more crime while, similarly, national reporting relies on domestic capacity, consistency and reputational incentives.

Still, some forms of SOC are easier to track. The trafficking of drugs and people is more often exposed to law enforcement because of its cross-border nature. When the Covid-19 pandemic shuttered international travel, a clear dip in detected human-trafficking victims followed. Conversely, the dramatic rise in cyber-crime has created new challenges, operating in a murkier area of SOC where jurisdiction is less well defined and detection remains more challenging.

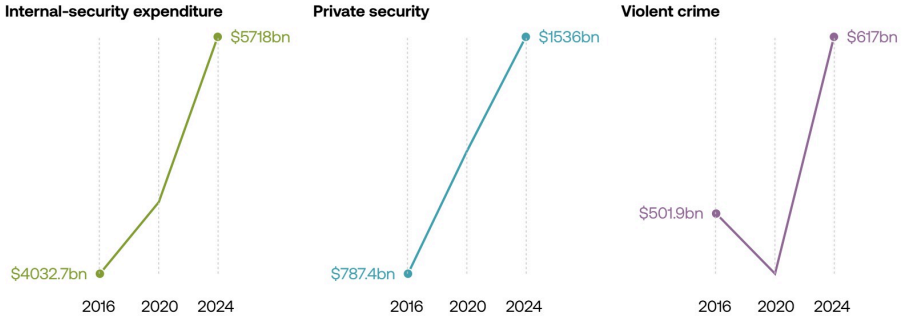
The Growing Cost of Serious and Organised Crime

The story of SOC's rise is clear and unambiguous – and so too are its costs. In 2023, $3.1 trillion in illicit funds – or 3 per cent of global GDP – flowed through the global financial system.[2] Drug trafficking alone accounted for $782.9 billion, making it the single largest category, followed by human trafficking with $346.7 billion in illicit proceeds.

But revenue is not commensurate with the true global cost of SOC to society. Drawing on the 2025 Global Peace Index and isolating key cost categories plausibly driven by organised crime, the economic burden includes $5.7 trillion in internal-security expenditure, $1.5 trillion in private security and $617 billion in violent crime.[3] The social and institutional costs of responding to organised crime are massive and have grown markedly since 2016, with internal security rising by 42 per cent, private security by 95 per cent and violent crime by 23 per cent.

FIGURE 2

The global cost of serious and organised crime has increased massively since 2016



Source: IEP 2017, 2021, 2025

Note: Values are shown in billions of PPP-adjusted US dollars for each respective year. While not inflation-adjusted, the consistent upward trend reflects real increases over time. For reference, 2016 values in 2024 PPP terms would be approximately 51 per cent higher.

SOC does not only generate revenue, it also exports instability and imports long-term social and economic harm. The impact on victims and communities is devastating. Organised crime groups (OCGs) can wield significant social control, sometimes creating entire parallel economies and governance structures, exploiting vulnerable individuals, and instilling fear and intimidation throughout communities. They also contribute to broader economic and social pressures, such as increased costs for goods, labour and housing, which hit low-income families especially hard. Legitimate businesses face unfair competition from illicit actors and are often extorted or pushed out of the market. Over time, this fosters a sense of abandonment, resignation and powerlessness, further destabilising communities and stoking frustration.

SOC plays a key role in reshaping political priorities and exacerbating social tensions. A striking example is the role of organised immigration crime – as exemplified by the surge in illegal Channel crossings by small boats – which has elevated immigration to the top of the political agenda in several countries. In doing so, it has intensified public anxiety and strengthened populist rhetoric across the political spectrum.

At the same time, SOC is increasingly entangled with broader geopolitical dynamics. Some hostile states are working with criminal networks to try to undermine Western democracies, weaponising organised crime tactics. So-called hybrid-threat actors blend traditional criminal activities with strategic disinformation, cyber-attacks and subversion. These operations do not only target economic weaknesses, they also divide societies, increase political tensions and reduce trust in public institutions. In October 2024, MI5 Director General Ken McCallum described state threats as a key risk facing the organisation.[4]

If left unchecked, these developments threaten the very foundations of democratic societies: weakening economies, undermining trust in government and sowing division among communities. Consequently, SOC is not just a law-enforcement issue: it is a strategic threat to national resilience and a destabilising force in international relations.

The New Face of SOC: Global, Entrepreneurial and Digitally Enabled

SOC is undergoing momentous change: it is dynamic, decentralised and increasingly difficult to contain. It is progressively connected and global, with networks operating across borders, exploiting advanced technology, and moving goods, people and money faster and further than enforcement agencies can keep up with.

FIGURE 3

Organised crime groups are increasingly poly-criminal, operating across multiple borders

Source: SOCTA 2021

The line between state, legal and criminal actors is becoming increasingly blurred. Hostile states are now leveraging criminal networks as proxies to pursue both financial and strategic goals. APT4, a group linked to the Chinese state, is one example, conducting cyber-espionage on behalf of government agencies while simultaneously engaging in financially motivated hacking.[5] Another example involved an attack on a warehouse containing humanitarian aid for Ukraine carried out by petty criminals in south London who had been recruited online (via Telegram) by the Russian Wagner Group. This was described by officials as “a clear example of Russian state-linked groups using British proxies for serious criminal activity”.[6] This erosion of boundaries shows how SOC now moves across national, institutional and ideological lines.

The Growth of State-Sponsored Cyber-Attacks

State-sponsored attacks are on the rise, becoming a key part of modern geopolitical warfare.

In August 2023, Graeme Biggar, director general of the National Crime Agency (NCA), highlighted ransomware – a type of malware that encrypts a victim's personal data until a ransom is paid – as one of the most sophisticated online crimes, with the biggest threat coming from groups "tolerated by, and sometimes linked to, the Russian state".[7] The Russian state enables ransomware groups by failing to investigate or disrupt their operations – and in some cases, by directly supporting their criminal activity.[8]

State-linked cyber-operations are not limited to making money. One notable example was a series of hacks and breaches targeting UK government departments and critical infrastructure, including the Electoral Commission, which were attributed to China. Europol also notes an increase in politically motivated cyber-attacks against infrastructure and public institutions, particularly those originating from Russia. OCGs increasingly act as state-aligned proxies, engaging in sabotage or espionage on behalf of hostile governments.

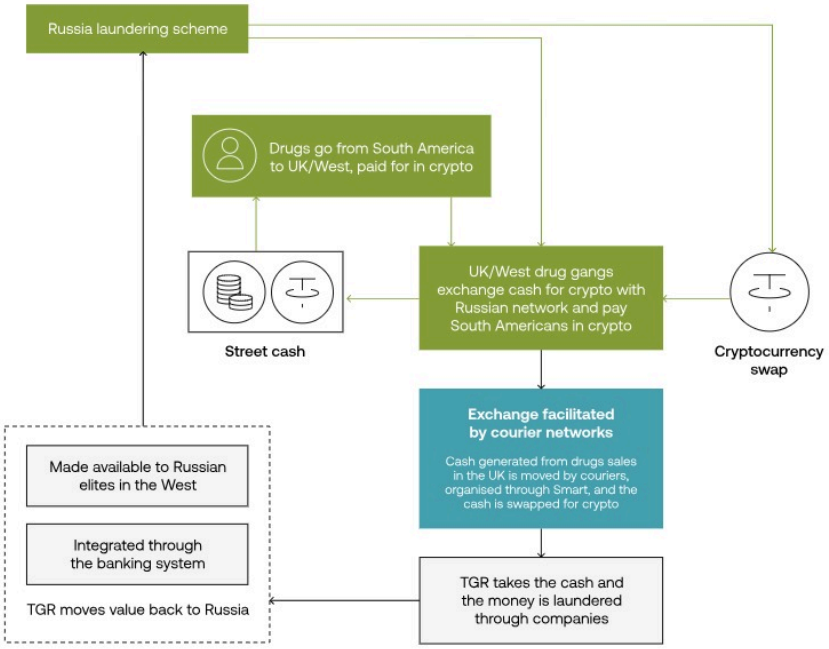
Moreover, the rise of ransomware-as-a-service models has made attacks more accessible to non-technical actors.[9] AI-driven tools further enhance both the scale and strategic nature of ransomware.

Today's OCGs operate less like the mafia and more like startups, adopting many of the same features that define modern business – outsourcing, technological innovation, use of AI, agile structures and cross-border scale. Traditionally hierarchical and loyalty-driven, many criminal groups are now fluid, decentralised and ruthlessly entrepreneurial. They adopt flexible business models, diversify operations, scale quickly and manage risk with a focus on profitability.

This shift is demonstrated in Operation Destabilise, a multi-billion-pound money-laundering network that acted as a financial bridge linking organised crime, cyber-criminals and hostile state actors, particularly Russia. At its core were two companies, Smart and TGR, which operated across more than 30 countries. They facilitated the movement of illicit funds using a combination of old-school cash-couriering and sophisticated cryptocurrency transfers. Their clients included more than 22 criminal groups, ranging from the Kinahan cartel – Irish cocaine traffickers implicated in contract killings – to UK street-level drug gangs and ransomware operators.[10]

FIGURE 4

The complex money-laundering scheme used by Russian spies and cocaine kingpins

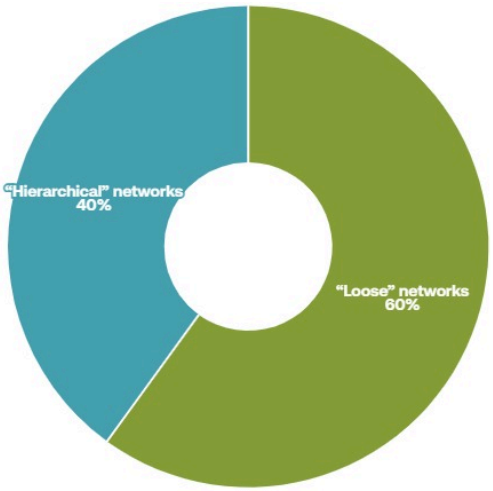


Source: Financial Times

As part of their ever-more sophisticated evolution, OCGs are embedding themselves in the legal economy, exploiting shell companies, logistics firms, import/export businesses and real-estate portfolios to launder profits and mask illegal activities. Europol estimates that 86 per cent of the most threatening criminal networks make use of legitimate business structures.[11] They operate across sectors – from construction and retail to finance and energy – creating a self-sustaining system that blurs legal and illicit economies, and deepens SOC's reach and resilience.[12]

FIGURE 5

Modern criminal networks are split 60/40 between “loose” and “hierarchical”



Source: SOCTA 2021

As legitimate business structures evolve, so too do OCGs, mirroring trends such as increased outsourcing, the commoditisation of services, and the use of innovative technology and AI. Just as legitimate firms rely on contractors, criminal groups turn to freelance specialists for money laundering, cyber-attacks, forgery and logistics. Europol notes the rise of loose criminal networks collaborating around shared objectives, often facilitated by a growing market of “crime-as-a-service” providers.[13] During the Covid-19 lockdowns, for instance, a Russian network used cryptocurrency to help UK drug gangs convert street cash into usable assets,[14] highlighting the seamless international outsourcing of high-risk tasks.

These developments allow even small or emerging groups to access high-level capabilities. Shared trafficking routes, pooled resources and reinvested profits further increase resilience and adaptability. This networked, service-orientated model lowers the barriers to entry and accelerates the spread of organised crime.

There is no doubt that technology is the single greatest enabler of SOC today and, according to the defence and security think-tank, the Royal United Services Institute, the majority of crime now takes place online or is digitally facilitated.[15] The EU's 2025 Serious and Organised Crime Threat Assessment found that "nearly all forms of SOC have a digital footprint".[16] Even criminal activities with a physical centre of gravity – such as human trafficking or drug smuggling – now rely heavily on online platforms for recruitment, logistics and payment.[17]

The cost and scale of tech-enabled SOC are staggering. Illicit cryptocurrency flows reached an estimated $51 billion in 2023.[18] The average ransomware payment made by UK organisations was £1.6 million, contributing to losses estimated at more than £300 million.[19] Recent high-profile cyber-attacks on UK organisations include the hacking of M&S's online store and purchasing systems in early 2025, which led to systems being affected for six weeks.[20] Personal-data breaches are increasing in frequency and severity, feeding back into the broader crime-as-a-service economy.

Criminal networks exploit digital tools to scale operations, automate attacks and avoid detection. Online platforms are used for recruitment, logistics, payments and laundering. Online marketplaces now offer a full criminal toolkit – from encrypted communications and malware kits to identity-theft tools and intrusion services – enabling even low-skilled actors to commit sophisticated crimes.[21] Data has become a key criminal commodity in itself. Identity documents, financial records, login credentials and other sensitive information are routinely stolen and traded on illicit marketplaces.[22] Cryptocurrency is widely used for transactions and money laundering, offering almost total anonymity. With more than 5,300 new tokens created daily and transactions taking place across fragmented systems, tracing this activity is extraordinarily hard. The dark web further compounds these

challenges. Sites are hidden behind scrambled addresses and protected by virtual private networks (VPNs) and encrypted routing, making them difficult to monitor or disrupt.

Artificial intelligence has further accelerated this trend – lowering the barriers to entry, expanding the reach of criminal operations and increasing their impact. AI is widely accessible, easy to use and versatile, enabling criminal groups to automate attacks, mimic identities and generate content at scale. It has already been used to produce child sexual-abuse material, facilitate cyber-attacks and conduct large-scale fraud through tools such as voice cloning and deepfakes. OCGs are rapidly adopting these tools, while law enforcement is "not adequately equipped to prevent, disrupt or investigate"[23] such crimes.

An Outdated Response to a Modern Threat

The nature of the SOC threat poses major challenges for law enforcement and regulatory systems, with the international response remaining rooted in traditional criminal-justice approaches, which are slow, reactive and heavily reliant on securing prosecutions.[24] Yet convictions are difficult to achieve and remain low. In England and Wales, just 6 per cent of Crown Court appearances between 2013 and 2020 met the standard criteria for SOC, amounting to only 3 per cent of all cases in that period where at least one defendant had been charged with a SOC-related offence.[25] Investigations are lengthy, fragmented across jurisdictions, and constrained by high evidentiary thresholds.

For example, the process for the Marengo Trial – involving high-ranking members of the Mocro Maffia, a Dutch-Moroccan criminal organisation – took six years between arrest to final sentencing, despite the severity of the crimes, which included five contract killings, multiple attempted murders and the deep infiltration of public institutions. The trial itself spanned 142 hearing days, required more than 800 pages of pleadings and generated more than 3,000 pages of legal submissions.[26]

Efforts to disrupt organised crime are increasingly sophisticated and often yield important short-term gains. However, many such efforts remain isolated and difficult to sustain – targeting individuals or platforms without always dismantling the broader networks behind them.[27] For example, the takedown of Encrochat by French, German and Dutch police in 2020 – which led to more than 4,000 arrests – marked a major operational success, yet many of the criminal groups involved were able to adapt and continue their activities. Similarly, the Pirate Bay, one of the best-known illegal content-sharing sites, has remained accessible via proxy servers despite repeated shutdowns since its launch in 2003, showing how easily digital criminal infrastructure can be rebuilt. As GI-TOC notes, "high-profile, short-term police operations usually displace the problem rather than curtail it, resulting in a never-ending 'whack-a-mole' chase."[28]

Most responses still depend on time-consuming legal processes rather than fast, flexible measures that can degrade criminal networks through economic pressure and targeted disruption. Sanctions – a tool now central to counterterrorism and responses to hostile states – offer a faster, more flexible alternative but remain underused in the SOC context.[29] INTERPOL has introduced tools such as the Silver Notice to trace assets and disrupt networks, but these are relatively new and their wider role in a sanctions-based strategy remains limited.

International frameworks are outdated, siloed and underused and, while a range of international strategies and treaties exist – such as the UN Convention against Corruption, the UN Convention against Transnational Organized Crime (UNTOC) and various sector-specific regimes – they typically provide legal frameworks rather than enforceable powers. Enforcement remains patchy and compliance is inconsistent. The most significant legal instrument, UNTOC, was created to strengthen global cooperation in tackling transnational threats, yet 25 years on, only two countries have undergone peer review on its implementation, giving useful insight into the limited tangible impact that formal adherence has delivered. Similarly, while the Financial Action Task Force plays a central role in setting global anti-money-laundering standards, its effectiveness is constrained by inconsistent national implementation and a lack of binding enforcement

tools. There is no central body promoting data availability, no consistent oversight mechanisms and still no universally agreed definition of organised crime – all of which weaken accountability and coordination.

This institutional weakness is compounded by a lack of operational coherence. In theory, mechanisms such as those under the Palermo Convention or the EU Justice and Home Affairs (JHA) framework are in place to enable intelligence-sharing, joint operations and electronic evidence exchange. In practice, political will, institutional trust, and legal and data harmonisation remain major barriers to cooperation. As the GI-TOC notes, "a lack of trust is often a barrier to exchanging intelligence or evidence" compounded by "different regulatory frameworks and legal systems, as well as a lack of harmonization of national definitions of crime, also hampers cross-border cooperation."[30]

Agencies designed to coordinate international policing, such as INTERPOL and Europol, are constrained by broad mandates, unwieldy governance and under-resourcing. Their ability to respond rapidly and strategically is often limited – especially in an environment where OCGs are fast, networked and cross-border by default. Further, there is some indication that INTERPOL mechanisms have been used by member states to further their own political agendas, for example, targeting opposition figures or journalists through INTERPOL Red Notices.[31]

Distrust in multilateral institutions has further eroded the credibility and effectiveness of international cooperation, not least because international frameworks were designed for a more cooperative era but are now strained by rising distrust, weak compliance and the inclusion of hostile or compromised states within multilateral systems. In this vacuum, many countries are turning instead to bilateral or small-scale multilateral arrangements, prioritising speed and control over scale and cohesion. The UK's cooperation with Albania, focused on disrupting networks involved in illegal migration, drug trafficking and human exploitation, offers one prominent example. These focused collaborations can deliver faster and more operationally effective responses to shared threats. However, they also

risk duplication, fragmentation and poor coordination. Often reactive, short-term and unscalable, they remain ill-suited to tackling the persistent, transnational nature of SOC.

Crucially, this fragmented response fails to address the structural enablers of organised crime – such as corruption, illicit financial flows and weak border regulation. Without a framework capable of coordinating the financial, legal and political levers of disruption, enforcement efforts will continue to skim the surface of the problem.

Key actors – especially in the private sector – are insufficiently embedded in the SOC response. Most of the infrastructure exploited by OCGs – from fintech platforms and logistics systems to encrypted messaging apps – is owned and operated by private companies, with limited oversight from government or law enforcement. As such, the private sector has a crucial role to play, not only in designing systems that are resilient to criminal exploitation, but also in developing the next generation of technologies that can support law-enforcement efforts. The wholesale move of the UK private sector to distance itself from Russian companies in the wake of the Ukraine invasion is a good example of the power of individual companies to disrupt. This is increasingly being recognised – agencies such as the UK's National Crime Agency (NCA) have begun establishing public–private partnerships and, for the first time, private-sector actors were included in the data-collection and reporting process for the EU's 2025 Serious and Organised Crime Threat Assessment (EU-SOCTA). INTERPOL's Gateway Project – a framework designed to facilitate information-sharing and collaboration between INTERPOL and private-sector entities to tackle cyber-crime – is another example of good practice. However, these initiatives remain fragmented and limited in scope. There is no clearly defined role for the private sector within international frameworks, and the absence of large-scale, coordinated public–private cooperation leaves yawning gaps in prevention, disruption and intelligence-sharing. Ultimately, the private sector remains on the margins of the organised-crime response, when it should be embedded at its core.

SOC is no longer simply a criminal-justice issue. It is a strategic, geopolitical threat – one that exploits the seams between legal and illegal economies, between public and private sectors, and between national and international governance systems. Yet the global response remains outdated, fragmented and misaligned with the nature of the threat. Without bold, integrated and sustained disruption, SOC will continue to evolve faster than the systems designed to contain it – deepening instability, fuelling corruption and undermining public trust at scale.

02

A New Approach to International SOC

Despite the scale, impact and strategic nature of SOC, it remains under-prioritised on the international stage. Unlike counter-terrorism, which benefits from deep-rooted alliances, common priorities and institutional frameworks, responses to SOC are underpowered, fragmented and reactive. With criminal networks becoming more agile, entrepreneurial and tech-enabled, states are consistently outpaced, undermining both national resilience and collective security. A new international approach is urgently needed: one that mirrors the seriousness of the threat, matches its sophistication and reflects the shared interests of like-minded states.

The creation of a new International SOC Alliance would go a long way in tackling the problem and would be based on three core pillars:

- A trusted, agile and scalable partnership between a group of committed states.
- A disruptive and mission-driven approach.
- A strong focus on innovation and technical capability.

It would be underpinned by a deeper collaboration with the private sector and civil society. Together, these elements would enable a more agile, coordinated and impactful response to SOC.

Building a New Serious and Organised Crime Alliance

The goal of the Alliance would be to create a lightweight, high-impact partnership that scales over time – not a new bureaucracy or a scaling up of existing enforcement efforts, but an engine for sustained disruption. This distinction is critical: whereas many existing international bodies are

designed to pursue justice after the fact, the Alliance would prioritise disruption at source and prevention, targeting the systemic enablers that allow organised crime to scale.

PRINCIPLES FOR THE ALLIANCE

There are lessons to learn from other sectors and alliances that have achieved global impact addressing challenging problems. The Five Eyes alliance, widely seen as one of the most effective intelligence-sharing partnerships in history, is one such example. Its strength stems from a foundation of deep mutual trust among a core group of nations and the strategic value of pooled intelligence. Five Eyes also illustrates how trusted intelligence partnerships can evolve and expand over time, fostering deeper cross-border and inter-institutional cooperation. Importantly, Five Eyes has demonstrated how core members can take responsibility for specific regions or functional areas (for example, surveillance in particular geographies or domains), enabling task-sharing and driving efficiency across the network. This offers a powerful precedent for the SOC Alliance, which could adopt a similar distributed model to avoid duplication and ensure optimal use of pooled capacity.

In the SOC space, operations such as Trojan Shield – a large-scale international sting operation targeting encrypted criminal communications – offer valuable lessons. While such efforts are currently isolated and open to criminal displacement, they nevertheless demonstrate the disruptive potential of agencies working together at speed to deliver coordinated impact.

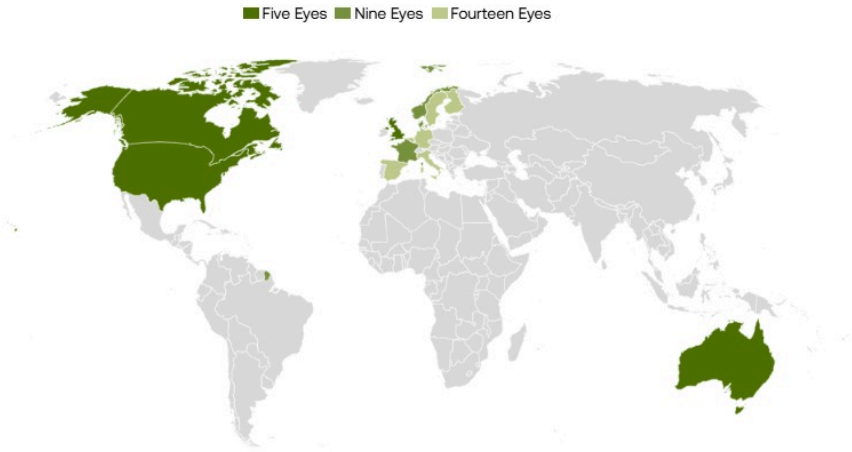
In other contexts, Operation Warp Speed, the US-led Covid-19 vaccine-acceleration programme, and the global GAVI vaccine alliance both showed how mission-driven, public–private partnerships can move rapidly to deliver results on a global scale. The Defense Advanced Research Projects Agency (DARPA), the US defence-innovation agency that is one of the world's most prolific producers of successful technologies, highlights the value of combining state direction with technical expertise, innovation pipelines and trusted industrial partnerships.

Together, these models demonstrate the value of trusted partnerships, fast and focused disruption, and state-led innovation – core principles that should underpin the new International SOC Alliance, providing the foundation for a scalable, high-impact approach:

- **Trust and a small, strategic core:** A foundation of deep mutual trust, shared risk and operational transparency among a small number of committed countries.
- **Agility and speed:** The ability to respond quickly and flexibly to emerging threats, without being hampered by consensus-based multilateralism.
- **Mission-driven focus:** Clarity of purpose, strategic alignment and sustained attention to delivering disruption at scale.
- **Public–private partnership:** Voluntary, co-designed collaboration with the private sector and civil society, especially in high-leverage domains such as finance and technology.

FIGURE 6

The "Five Eyes" model of counterterrorism intelligence-sharing



Source: Forbes

The Five Eyes Alliance

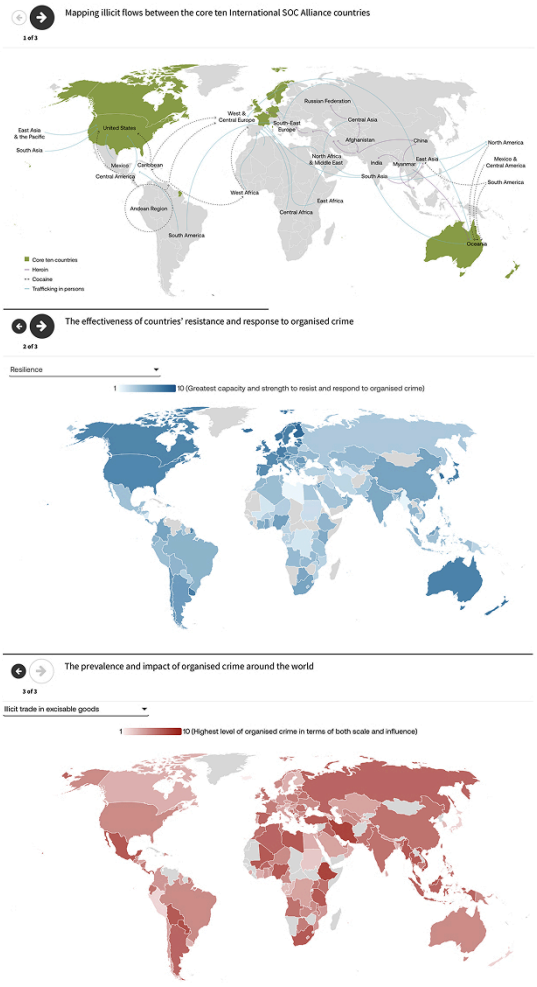
The Five Eyes alliance is a long-standing intelligence-sharing partnership between the United States, the United Kingdom, Canada, Australia and New Zealand, originally established in the aftermath of the second world war. Its roots lie in the 1946 UKUSA Agreement, which formalised a cooperative arrangement for the sharing of signals intelligence (SIGINT) between the UK and the US. The alliance later expanded to include Canada in 1948, followed by Australia and New Zealand in 1956. Over time, the Five Eyes has evolved into one of the most important intelligence alliances in the world, playing a central role in global intelligence and security cooperation. Its strength lies in a foundation of deep mutual trust, comprehensive intelligence-sharing across a range of domains and coordinated responses to shared threats. Although each member may focus on different geographic regions or areas of expertise, the Five Eyes framework enables highly integrated intelligence collection, analysis and collaboration across the alliance. In addition to the core Five Eyes members, broader networks have emerged: the Nine Eyes alliance includes Denmark, France, the Netherlands and Norway, while the Fourteen Eyes further extends participation to Germany, Belgium, Italy, Spain and Sweden.

While Five Eyes does engage in tackling SOC through mechanisms such as the Five Eyes Law Enforcement Group (FELEG), which brings together law-enforcement agencies from member countries to address issues like transnational organised crime, these efforts tend to be more reactive and operationally focused. Collaboration often centres on specific investigations or short-term joint operations, rather than forming part of a sustained, proactive and strategic approach to dismantling SOC networks. Compared

to the prioritisation and strategic cohesion seen in the countering-of-terrorism space, SOC remains less central and more fragmented within Five Eyes cooperation.

FIGURE 7

Organised crime flows, response effectiveness and prevalence



Source: TBI/Crest Advisory; UNODC; GITOC Organised Crime Index

MEMBERSHIP AND GOVERNANCE

The Alliance would launch as a trust-based coalition of committed states and private-sector partners, designed to scale over time through tiered membership, rewarding meaningful contributions with access to information, influence and innovation.

The initial structure of the proposed International SOC Alliance would mirror the Five Eyes intelligence-sharing model, organised into three tiers based on existing trust, operational capability and strategic relevance.

Tier 1 would comprise a tight, operationally coherent core of countries able to act jointly with speed and agility. This group would include the Five Eyes nations along with France, Germany, the Netherlands, Sweden and Norway. These countries are already deeply interconnected through intelligence-sharing infrastructure and law-enforcement ties, and share liberal democratic values, strong institutional capacity and a high degree of trust. Each also faces a significant threat from SOC, particularly immigration crime and drug trafficking, and are strategically placed with the resilience and capacity to tackle SOC.

Tier 2 would include close European allies and trusted regional partners. This would consist of the remaining members of the Fourteen Eyes grouping (Italy, Belgium, Spain), as well as strategically important partners in other regions such as Japan and Singapore. These countries would contribute to coordinated cross-border enforcement efforts, intelligence and data-sharing, and the disruption of identified SOC activity. Inclusion would be based on factors such as geographic relevance to trafficking routes, demonstrated capability in combating SOC and a willingness to align with the Alliance's principles and operations.

Tier 3 would consist of strategic disruption partners, that is, countries with relatively higher levels of criminality and weaker institutional resilience, such as Albania, Turkey, Mexico and Iraq. These states play a significant role in the global SOC ecosystem as source countries and would benefit from support

to restrict the activity of criminal groups. While full intelligence integration would not be possible due to governance or trust concerns, their inclusion would focus on targeted cooperation and joint disruption campaigns.

This tiered framework would allow the Alliance to expand its reach while preserving the integrity of its core. Over time, as countries in the outer tiers demonstrate reliability and effectiveness, they could move closer to the centre of the alliance and towards full membership of the core.

Membership of the coalition would be incentivised through a range of benefits aimed at encouraging deeper integration over time. These could include increased access to shared intelligence, tools and expertise made available through partnerships with the private sector, and the symbolic and diplomatic capital associated with being part of the coalition. In some cases, closer affiliation with the core may also bring economic or trade-related advantages. The overarching goal is to build a dynamic, layered framework of cooperation that strengthens collective efforts against SOC while rewarding meaningful contributions and trust.

The Alliance would also forge strategic partnerships with key private-sector actors, recognising their vital role in both enabling and disrupting SOC activity. This collaboration would be underpinned by voluntary partnerships and could involve:

- A core “trusted industry circle” – ongoing partnerships with key vetted firms focused on intelligence-sharing.
- A joint public–private task force and innovation hubs focused on specific threats.
- Ad-hoc, time-bound collaboration on disruptive and enforcement action.

For the private sector, engagement would not only mitigate operational and financial risks but also offer a route to shaping emerging standards and tools that enhance long-term resilience. It also offers the prospect of enhanced reputational standing through alignment with a high-profile, values-driven initiative.

To begin with, the Alliance could be established as a "coalition of the willing": a flexible, fast-moving framework involving close international collaboration without the pooling of sovereignty. This model would enable the Alliance to get off the ground quickly, without requiring a new international structure or treaty, and would avoid many of the legal and political complexities associated with binding agreements or supranational authorities.

To provide structure and continuity, an Alliance secretariat could be established to coordinate activity and provide administrative support, with leadership rotating between participating countries. Over time, the Alliance could evolve into a more formal structure, depending on member appetite and results achieved.

STRATEGIC ACTIVITIES AND OPERATING MODEL

The Alliance's added value would lie in its ability to apply consistent, coordinated pressure on SOC through legal, operational and economic tools. Rather than focusing solely on individual actors, the Alliance would target the structural enablers of SOC.

To put this into operation, member states would voluntarily endorse the Alliance's core principles and commit to tangible, operational contributions, including:

- Workforce and expertise.
- Computational capacity and technical infrastructure.
- Data and intelligence inputs.
- Operational access, with national agencies leading or supporting coordinated disruption campaigns.

The Alliance's core operating model would be built around integrated action across three areas:

- **Shared intelligence and operational coordination:** Deeper collaboration on intelligence through the development of joint threat assessments, strategic analysis and shared typologies would help build a common

understanding of priority threats. Faster identification of cross-border links and emerging risks would enable faster disruption of transnational networks.

- **Coordinated cross-border disruption:** The Alliance would coordinate pressure on the economic infrastructure of organised crime, for example, by jointly applying sanctions and enforcing due diligence across high-risk sectors. To prevent displacement and legal arbitrage, members would work towards regulatory and legal alignment, including harmonised offence definitions, streamlined evidence-sharing and coordinated asset recovery.
- **Deployment of tech and innovation:** The Alliance would prioritise the deployment of advanced technology and the pooling of critical infrastructure – including computational capacity, shared models and technical expertise – to better understand the threat and disrupt SOC at greater scale. A shared innovation agenda would allow the Alliance to identify promising technologies, run cross-border pilot programmes and scale successful interventions quickly.

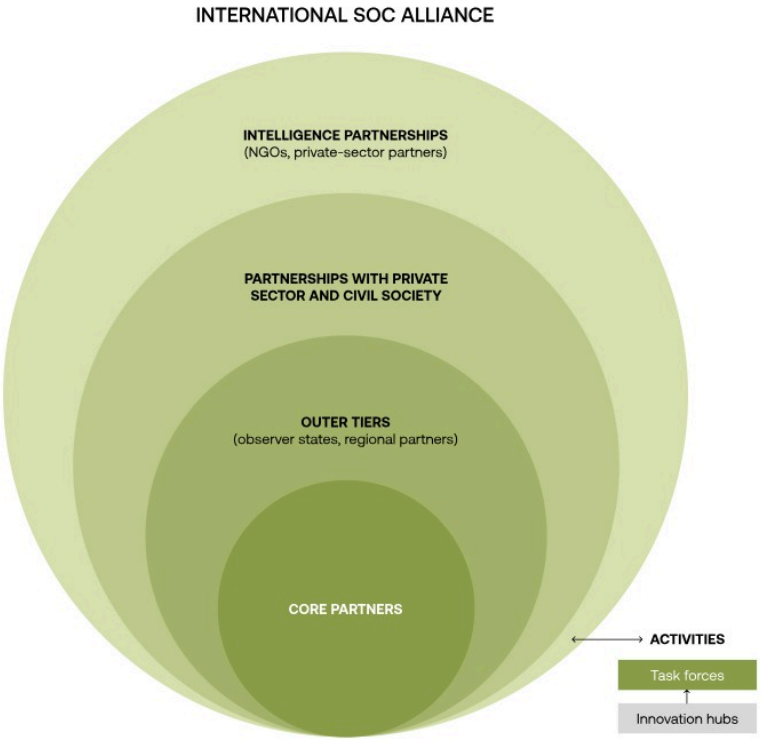
To complement these core activities, the Alliance would also establish dedicated task forces, each led by one member country in partnership with the private sector, focusing on the highest-value enablers of SOC: for example, illicit finance, cryptocurrency abuse and corrupt service providers. Task forces would bring in members across the tiers as needed. These teams would:

- Operate across sectors, including financial institutions, tech platforms and civil society.
- Use pooled intelligence and advanced analytics to identify and target systemic vulnerabilities.
- Pilot innovative regulatory or technological interventions.
- Coordinate cross-border enforcement action against key enablers.

Together, the task forces and the Alliance-wide core activities create a model not just for cooperation but for sustained disruption at scale – something that current bilateral or fragmented multilateral structures struggle to deliver.

FIGURE 8

How the International SOC Alliance would be structured



Source: TBI/Crest Advisory

Disrupt Criminal Networks by Dismantling Their Business Models

If OCGs function like startups, we need to start tackling them as startups, by undermining the very conditions that allow them to emerge, scale and thrive. Just as governments design policies to make countries attractive to legitimate business, these same policies also attract criminal enterprises.

Economic openness, ease of company registration, visa flexibility, access to capital and high-quality infrastructure are all features that benefit lawful and unlawful operators alike. The same ecosystem that nurtures innovation can, without proper safeguards, be exploited by criminal networks.

Understanding why startups collapse can offer a strategic framework for weakening OCGs. Most startups fail not because of external threats, but due to internal weaknesses: 35 per cent are unsuccessful because there is no market need, 38 per cent because they run out of cash and 23 per cent because they have the wrong team.[32] Pricing problems, flawed products and an inability to pivot are also significant contributors to collapse. In effect, even promising ventures crumble if they fail to meet demand, mismanage their resources or are outmanoeuvred by faster, leaner rivals.

OCGs succeed when they meet consumer demand, move money efficiently, iterate quickly and exploit regulatory vacuums. But they can fail when the environment becomes hostile, such as when trusted intermediaries are removed, revenue is disrupted or the product is no longer viable. Treating SOC as an economic system allows us to target its viability directly – by undercutting profits, raising operational costs and injecting uncertainty. It also requires altering the incentive structure, raising the risk and diminishing the potential gains of criminal activity to reduce its appeal. Critically, this means attacking the cross-cutting enablers that underpin criminal business models, including opaque financial systems, weak corporate transparency and fragmented regulation. Crisis-sensitive disruption, which limits illicit actors' ability to scale, adapt or pivot, can make these networks more fragile and less sustainable.

Dismantling OCGs in line with their startup models will require a three-pronged approach:

- Increasing the costs of operations via a new sanctions regime.
- Cutting the criminal supply line.
- Building community resilience.

FROM CASH FLOW TO CRACKDOWN: INCREASING THE COSTS OF ILLICIT OPERATIONS

The current reliance on slow and reactive criminal-justice approaches is falling short. A faster, more agile approach is needed: one that can be triggered rapidly based on intelligence and partnership-based assessments and that delivers sustained pressure on the economic infrastructure of organised crime.

Sanctions are increasingly being used to tackle a range of issues. Traditionally the domain of foreign policy and counter-terrorism, they are now being applied more often to tackle crime, including human-rights abuses and corruption. Major jurisdictions, including the UN, UK, US and EU, have begun targeting individuals and groups engaged in SOC, such as through the UK's recent migrant-smuggling sanctions. However, leveraging sanctions as part of core toolkit against SOC remains limited. This must change. To effectively counter the startup dynamics of organised crime, sanctions must be used to disrupt the conditions that allow these groups to scale – by freezing assets, restricting access to financial and logistical systems, and publicly signalling the cost of participation in illicit markets.

The UK government's recent announcement that it intends to use sanctions against people-smuggling gangs echoes proposals set out in TBI's *A New Approach to Serious and Organised Crime*.[33] But to be truly effective, the government must go further, launching a coordinated international effort that tackles organised criminal groups at their source.

The Alliance would coordinate a new sanctions regime, targeted at the top of the criminal supply chain, focusing on key decision-makers, financial facilitators and logistics providers. Rather than easing trade and enabling growth, this initiative would take the opposite tack: choking financial lifelines, severing cross-border links and dismantling the business infrastructure of transnational organised crime.

Alliance members would implement sanctions domestically but synchronised with each other. There is precedent for this: in 2022, countries of the G7, the EU and Australia came together to form the Russian Elites,

Proxies and Oligarchs (REPO) Task Force to coordinate sanctions and enforcement actions against Russian elites and enablers. While the task force aligned its actions, each member state acted under its own legal authority.

A genuinely coordinated approach is essential. Consistency across jurisdictions is what gives sanctions real force, ensuring that designated individuals and groups cannot simply relocate operations to more permissive environments. When sanctions are applied in a unified and coordinated manner, OCGs face a shrinking operating space, fewer financial loopholes and the reduced ability to adapt or exploit uneven enforcement. Only by acting together will the Alliance be able to truly raise the cost of organised crime and disrupt it at scale.

To operationalise this new sanctions regime and increase the costs of illicit operations, the Alliance would:

- **Establish a sanctions working group** composed of representatives from member countries to meet regularly and coordinate quick, decisive action. Underpinned by a shared data infrastructure, the working group would pool intelligence, align designation decisions and maintain a joint-threat picture across jurisdictions. Designations would be continually reviewed and updated using live intelligence to ensure sustained pressure on priority targets.
- **Impose targeted, coordinated sanctions on key targets based on risk intelligence.** Once a designation is made, sanctions would be applied simultaneously across member states, using existing national enforcement mechanisms, with countries free to go further by applying additional domestic measures where appropriate. Key components of sanctions would include:
  - **Freezing – and ideally seizing – the assets of designated individuals and proscribed organisations and their enablers**, including property, bank accounts, cryptocurrency wallets, offshore trusts, high-value vehicles, artworks and commercial holdings.
  - **Imposing coordinated restrictions on spouses and dependents** who materially benefit from the proceeds of organised crime. Like the sanctions employed to target oligarchs, measures would be based on

economic proximity rather than legal ownership.[34] Sanctions could include enrolment in elite educational institutions if tuition is proven to be paid with illicit funds, denial of access to private financial services and exclusion from residency-by-investment schemes.

- **Work together to penalise service providers** – including banks, law firms, real-estate agents, educational institutions and countries – that knowingly or recklessly enable designated actors. Sanctions would include fines, professional-licence suspensions and exclusion from public procurement or accreditation frameworks. The Alliance would maintain a public registry of non-compliant institutions, and regulators would be empowered to issue compliance notices and investigate breaches.
- **Track and assess the operational impact of sanctions**, monitoring behavioural changes among targets, disruption to financial and logistical systems, and adaptations in OCG operations. This would be supported by advanced technology, including AI-enabled monitoring tools and predictive analytics, to detect emerging threats, circumvention methods and displacement effects.
- **Use regular impact assessments to inform decision-making**, ensuring that the sanctions regime remains targeted, proportionate and responsive. A data-driven feedback loop would keep the strategy agile and effective over time.
- **Coordinate announcements and public justifications across member states**, clearly linking sanctions to specific harms caused – whether to communities, economies or national security. Public communication helps build support and undermine the legitimacy of criminal actors.

Coordinated sanctions could be further complemented by greater regulatory alignment on key frameworks, including anti-money-laundering compliance, beneficial ownership and professional-service-provider accountability, allowing the Alliance to erode the financial and institutional foundations that sustain criminal enterprises.[35]

CUTTING THE CRIMINAL SUPPLY LINE: DISRUPTING SUPPLY CHAINS AND LOGISTICS

To disrupt supply chains and logistics the Alliance would carry out a series of coordinated actions.

FIGURE 9

Six ways in which the Alliance could disrupt supply chains and logistics

Source: TBI/Crest Advisory

The secretariat could coordinate these efforts, ensuring the required level of analytical and operational capacity:

- **Coordinate cross-border enforcement at criminal logistics hubs:** The Alliance would synchronise action against sanctioned actors and their affiliates through shared intelligence at critical trade points including ports, airports, shipping routes and bonded warehouses. This can be put into operation through customs coordination, blacklisting of vessels and logistics firms, and the revocation of operating licences. States would also explore the use of digital cargo tagging and geofencing to monitor and restrict high-risk shipments, ensuring OCG supply chains are disrupted at multiple points of vulnerability.
- **Conduct coordinated but randomised enforcement operations across critical trade infrastructure:** Unlike isolated national crackdowns, the Alliance would coordinate staggered, cross-border inspections at high-risk infrastructure – including high-traffic ports, known air corridors and major precursor shipment routes. By deploying enforcement activity in a staggered and unpredictable manner, the Alliance would erode OCG confidence, drive up insurance costs, disrupt schedules and force OCGs to reroute through slower, less secure alternatives, increasing exposure and reducing profit margins across the OCG supply chain.
- **Establish and maintain a consolidated watchlist of high-risk vessels, aircraft, hauliers and containers:** The Alliance would develop a dynamic, intelligence-led tracking list of transport assets linked to SOC that enables rapid targeting of criminal logistics assets. This list would be shared across customs, aviation and maritime authorities in member states, enabling real-time action, including targeted inspections, denial of entry, licence revocation or forced deregistration. The working group's coordination role would ensure that action taken in one country is mirrored across the Alliance.
- **Track high-risk cargo routes, flagged logistics operators and emerging patterns of displacement:** Powered by machine-learning and customs-seizure data, the Alliance would identify shifting patterns in OCG logistics, helping member states stay ahead of evasive tactics. Drawing on seizure data and customs intelligence, this system would provide predictive insights to guide interdiction strategy, target sanctions designations and monitor shifts in criminal logistics behaviour. These insights would also highlight structural vulnerabilities – such as

unregulated trade corridors or lax customs regimes – that could be targeted through regulatory coordination to prevent OCGs from shifting activity into less governed spaces.

- **Undermine trust in the criminal supply chain through active disruption and covert capabilities:** Enabled by shared-intelligence infrastructure, the Alliance would deploy coordinated disruption operations to degrade the reliability and reputation of illicit logistics networks. These measures – which individual states may already use in isolated cases – would be elevated through Alliance-wide planning and intelligence-sharing. Activities would include:
  - Honey-trap operations targeting online brokers, dark-net intermediaries and chemical-sourcing agents, using false offers, decoy listings and controlled transactions.
  - Controlled delivery stings, in which criminal shipments are deliberately delayed, altered or rendered non-functional to disrupt trust in distribution.
  - Synthetic "ghost" listings posted on procurement forums to flood the market and crowd out legitimate supplier access.
  - Fake job campaigns, saturating illicit courier and logistics-recruitment channels with decoys or surveillance operatives.
  - Counterfeit-product substitution, quietly introducing faulty, traceable or degraded inputs into low-trust supply chains to undermine quality assurance and generate market confusion.
- **Target airborne and maritime smuggling technologies, including drones and submersibles:** Recognising the growing use of specialist technologies by OCGs, the Alliance could create a dedicated task force to tackle airborne and maritime smuggling. This collective approach would allow for the rapid identification and targeting of emerging logistics tools that no single country can effectively monitor or disrupt in isolation. Activities would include:
  - Sanctioning drone operators, component suppliers and vessel manufacturers linked to illicit use.
  - Joint investment in counter-drone and coastal-surveillance infrastructure to detect, intercept and neutralise airborne or underwater shipments in transit.

- Shared enforcement protocols enabling seamless cross-border interdiction and seizure.

Eurojust, Frontex and the G7 Roma-Lyon Group

Eurojust is the European Union Agency for Criminal Justice Cooperation, formed of judicial authorities across EU member states. Its aim is to coordinate the work of national authorities related to the investigation and prosecution of transnational crime.

The Agency is formed of seconded member-state personnel, as well as analysts, legal advisors and data experts. Eurojust hosts networks to enable greater collaboration between international criminal-justice partners, and leads the judicial response to threats in Europe, supporting partners and coordinating parallel investigations and hosting joint investigation teams. The agency also plans joint action days enabling coordinated arrests and action to dismantle OCGs and seize assets across Europe.

Frontex is the European Border and Coast Guard Agency, supporting EU member states and Schengen countries to manage the EU's external borders in the fight against cross-border crime. A centre for excellence in border-control activities, Frontex shares intelligence with EU states and others affected by migratory trends and cross-border crime, and operates under EU regulations.

Frontex coordinates operations along the EU's external borders, such as surveillance, crime-fighting and return operations, including as part of joint action days with other national law-enforcement authorities, international organisations and EU agencies. The intelligence gathered through their work is analysed and disseminated among partners.

Frontex also develops networks of partnerships with authorities of non-EU countries, particularly those neighbouring the EU, based on their strategic locations in the response to irregular migration.

The G7 Roma-Lyon Group offers a different but complementary model of international cooperation. While its focus is largely strategic rather than operational, the group brings together law-enforcement officials from G7 countries to review evolving threats in both the counter-terrorism and serious-organised-crime spaces. It provides a forum for sharing best practice, fostering trust between jurisdictions and coordinating strategic initiatives across borders.

These examples highlight the need for effective, coordinated international action to tackle cross-border threats. They also demonstrate the variety of models – both operational and strategic – that already exist and could be built upon. The proposed SOC Alliance would seek to connect, strengthen and scale such efforts, enabling partners to collaborate more systematically and deliver sustained disruption at a global level.

VULNERABLE TO VIGILANT: BUILDING COMMUNITY RESILIENCE

- **Build an Alliance-wide intelligence partnership to identify community vulnerability.** The Alliance would formalise a strategic partnership with NGOs and private-sector actors to develop a cross-border intelligence platform modelled, for example, on the STOP THE TRAFFIK model (see case study). This would enable frontline agencies, community groups and businesses to submit structured, anonymised reports of suspected SOC and exploitation activity. To ensure participation does not expose NGOs or communities to harm or retaliation, the platform would be underpinned

by robust safeguards, including clear operational guidelines, strict protocols around data handling and anonymity, and mechanisms for consent and redaction. A strong "do no harm" principle would govern all engagement, ensuring that information-sharing does not lead to reprisals, overreach or unintended consequences. The platform would:

- Aggregate intelligence across jurisdictions to build a shared, real-time understanding of recruitment tactics, grooming hotspots and movement routes.
- Use machine-learning to detect emerging risks and drive proactive interventions.
- Serve as a decision-support tool for Alliance members to coordinate joint enforcement and development initiatives.

- **Coordinate disruption and resilience efforts across community-vulnerability hotspots.** Using the Intelligence Platform, the Alliance would deploy coordinated and targeted development interventions to strengthen resilience in communities most vulnerable to OCG infiltration and recruitment. A key pillar of this approach should be the creation of scalable, cross-border pathways for high-risk youth. Working in partnership with the private sector, including technology firms, logistics companies, retailers and financial institutions, the Alliance could design tailored economic and employment opportunities. These could include coding bootcamps and digital freelancing platforms to generate sustainable remote income, alongside structured entry-level employment pathways in sectors such as warehousing, retail and transport.

Delivery would be most effective through established civil-society mechanisms with local reach and credibility. The Global Initiative's Resilience Fund, for example, is the leading civil-society resilience-building platform and would be well placed to channel support to the communities that need it most, using tested, adaptive and community-led approaches.[36] Leveraging this kind of infrastructure would enable the Alliance to scale interventions quickly, ensure context-sensitive implementation, and avoid duplication or misalignment with existing grassroots efforts.

- **Sanction linked assets to support vulnerable states.** Alliance members would agree to reinvest confiscated assets from SOC actors and their enablers, especially those states most affected by sanctions regimes, into

community-resilience funds in countries vulnerable to shadow economies. This addresses potential economic displacement caused by sanctions and ensures criminal proceeds are recycled into preventative interventions.[37] Italy and Albania, for example, offer compelling models: Italy has long repurposed confiscated mafia assets for social use through community projects such as *Casa Chiaravalle*, while Albania's CAUSE initiative has converted seized properties into social enterprises employing vulnerable groups.[38,39] These models offer proven pathways for channelling confiscated criminal assets into community resilience efforts and could serve as a foundation for a scalable reinvestment strategy across the Alliance.

STOP THE TRAFFIK

STOP THE TRAFFIK is an international non-profit organisation dedicated to disrupting human trafficking through a prevention-focused, intelligence-led approach. Its vision is simple: to create a world where people are not bought and sold. STOP THE TRAFFIK builds community resilience upstream and disrupts traffickers' ability to move money or products through financial institutions and commercial organisations, ultimately making the criminal business of human trafficking too high-risk and low-profit to operate.

We can't stop what we can't see. STOP THE TRAFFIK built the world's richest collection of lived-experience data on human trafficking and modern slavery, the Traffik Analysis Hub, which contains more than 10 million data points from open and closed sources. Data is gathered through a wide, global network of frontline organisations, as well as law enforcement, businesses and banks. Additionally, individuals who have experienced exploitation can safely share their story with STOP THE TRAFFIK to help others avoid the same abuse. When all this data comes together, STOP THE TRAFFIK can create a live, detailed picture of trends on the ground, helping all stakeholders in a position to act to stay one step ahead of traffickers.

STOP THE TRAFFIK leverages these insights to identify communities at the highest risk of recruitment and trafficking, providing them with lifesaving information via targeted social-media ads. This equips communities with the knowledge to recognise red flags and seek safety. In the UK alone, nearly two million people have been reached over the past two years.

Deploy Tech at Pace and Scale

OCGs weaponise technology to their advantage and it is extremely challenging to play them at their own technological game. They leverage encrypted messaging platforms such as Telegram, currently the most dominant app for cyber-criminal coordination, with more than 80 million unique identifiers linked to illicit Telegram channels shared across underground forums in recent analyses, while also dominating dark-web marketplaces, where more than 60 per cent of vendors now traffic in stolen financial credentials, fuelling a global shadow economy. Increasingly, OGC groups move billions through cryptocurrencies to bypass financial institutions and anti-money-laundering rules and, in 2024 alone, illicit crypto transactions were estimated at $40.9 billion. OGCs are also deploying emerging tools, such as deepfakes and generative AI, to impersonate officials and undermine trust. Between 2022 and 2023, deepfake-related fraud surged by 1,530 per cent in the Asia-Pacific region. At the operational level, OCGs have begun using drones and surveillance technologies to track rivals, smuggle goods and evade detection. This technological edge allows them to operate transnationally, scale faster than legitimate enterprises and stay several steps ahead of enforcement.

In contrast to the efficiencies exhibited by OCGs in adopting and utilising technology, the legislative landscape of the UK and other global partners makes it difficult for law enforcement and governments to compete. We are rightly bound by ethical and legal safeguards to moderate states' use of technology and its reach into private citizens' lives, which makes adopting new technology more difficult for large states than for small startups, and vastly more difficult than for OCGs. One example of this is the growing debate and concern over the UK police's use of live facial-recognition software.

One powerful asset, however, is the data that international governments and law-enforcement agencies hold, together with the computational capability of states, both of which vastly overshadow the tools at OCGs' disposal. Efforts would be better placed in using technological solutions to leverage these data and computational assets on an international level. These data

are currently utilised within individual countries and for specific initiatives – for example, the proactive screening of customer identity and financial data by banks to identify financial crime – but their full power is untapped.

To shift the balance, a new approach is needed. Strategic intelligence- and insight-sharing across key regions would not only improve situational awareness but also enable a broader, more consistent understanding of SOC networks, their enablers and cross-border operations. When combined with shared computational capacity, this pooled intelligence could multiply the impact of disruptive action, allowing for faster, smarter and more targeted interventions. Over time, increased innovation across the Alliance would be key to staying one step ahead of criminal networks, which are themselves quick to adapt, exploit and scale.

International partners must take the opportunity to leverage this advantage by working together. The Alliance's approach to deploying technology should focus on the following key principles:

- **Pooling resources** (data and compute) to identify and generate innovative and effective disruptive solutions.
- **Coordinating action** to maximise its scale and impact, and reduce opportunities for OCGs to pivot operations and recover.

BRING DATA AND INTELLIGENCE TOGETHER TO IMPROVE THE THREAT PICTURE

Data-sharing between partner countries is both one of the greatest obstacles and most powerful opportunities in the fight against SOC. It is essential to building a real-time, dynamic understanding of the threat and enabling coordinating enforcement and disruption.

Yet today, international data-sharing is patchy, reactive and largely operational. Data-sharing between countries is primarily undertaken on an operation-by-operation basis, when law-enforcement activity requires it, or through bilateral agreements, as between the UK and its allies. One example of this is Joint Investigation Teams, facilitated by Europol, which allow law-enforcement agencies to collaborate and share information and resources

for specific operations. While effective for individual projects, this approach is reactive and siloed, and does not enable more systematic, strategic and long-term analysis of SOC trends that could be used to inform disruptive activity.

Some international data repositories do exist, including the Europol Information System, the Schengen Information System and INTERPOL databases. The UK's access to Europol and Schengen databases post-Brexit, however, remains a major stumbling block affecting law-enforcement operations internationally. Meaningful gains could be made by reducing friction in the way data are exchanged, accessed and acted upon.

ALLIANCE MEMBERS WOULD AGREE TO SHARE DATA AND INTELLIGENCE STRATEGICALLY

In the first instance, countries could agree to contributing insights, trends and targeted analysis drawn from national data sets using safe and scalable technological solutions. For each thematic enabler under focus by the Alliance, partners would agree on shared indicators and parameters. Requests for intelligence and analysis based on these parameters would then be issued to partner countries and agencies to fulfil, enabling better pattern and trend recognition.

Technological solutions can be deployed to mitigate against established data-sharing challenges. For example, AI "agents" in partner countries could analyse local data sets using a standardised framework, with only the results shared centrally. This approach would enable easier and more efficient sharing of data, as smaller quantities of raw data would need to be shared internationally, while also reducing the need for physical infrastructure, such as a shared data centre or legal agreements governing the sharing of raw data. Compute capability to complete the analysis could be housed via a private server (pending security considerations) or built into the UK's (and other countries') development of AI capacity and data centres.

Difficulties aligning legislation that governs the sharing of granular or personal-level data often hinders sharing between countries due to security concerns, and is further compounded by cultural willingness and political

considerations. Further, sharing and compiling evidence for use in prosecution is legally complicated and often leads to information being inadmissible as evidence in court. Clearly defining the purpose of information- and data-sharing under the Alliance would help to unlock these blockers. Where the goal is to detect patterns, identify targets for sanctions or guide disruptive activity rather than to meet evidentiary thresholds for court, different, more flexible approaches to data-sharing become possible, focused primarily on the sharing of large, aggregated data sets and trend-related intelligence rather than personal-level data. This would also reduce the risk of the Alliance becoming a target for OCGs and hostile states.

In a model scenario, sharing would be facilitated via established Europol and INTERPOL data-sharing mechanisms that operate under legal frameworks and data-protection rules. Legislation in Alliance member states can also facilitate sharing with global partners (for example, measures in the UK's recent Crime and Policing Bill seek to enable new international data-sharing agreements).[40]

In the longer term, Alliance partners would work towards true data interoperability – aligning formats, standards and definitions across partner countries. Today this is a significant challenge: differences in the way certain crimes and data are measured, recorded and collected, and the formats in which they are stored, make data integration extremely difficult. Differing laws for the collection and retention of evidence between states can also mean that evidence gathered in one country may not necessarily be able to be used in another.[41]

The more efficiently and effectively data can be shared across jurisdictions, the faster patterns can be detected, actors identified and responses deployed. As a long-term goal, partner countries would commit to reviewing and updating data-collection and storage processes in their own countries, with the ultimate aim of achieving data harmonisation, which would in turn allow raw data to be interoperable between law-enforcement agencies internationally. With interoperability achieved, partners can establish formal data-sharing agreements and work towards a federated learning model, in which AI models are trained using large-scale anonymised data sets.

Partnerships with the private sector – including the procurement of tools to clean, host and analyse data securely – can further accelerate this transition. Security features, and privacy and rights considerations would be built into all layers of this infrastructure, with costs and responsibilities shared across the Alliance, and high standards of cryptography, access control and resilience applied from the outset.

Private-Sector Tools Can Speed Up the Transition (Project Morpheus)

One example of how the private sector can support the secure design, delivery and integration of digital infrastructure is the UK Ministry of Defence's Project Morpheus, launched in 2017 under the Land Environment Tactical Communication and Information Systems (LE TacCIS) programme. It aims to replace the ageing Bowman system which has been in use since the early 2000s and is often criticised for its limited data capability, inflexible architecture and slow upgrade cycles. In contrast, Project Morpheus introduces a modular, open-architecture platform for secure, real-time communications across military units.

Though designed for the battlefield, Morpheus shows how large-scale public-private partnerships involving firms like General Dynamics can deliver scalable, secure systems that prioritise interoperability. These principles are highly relevant to law enforcement's efforts to improve international data-sharing, where aligning standards and investing in trusted infrastructure could enable more seamless cross-border cooperation.

COMBINE THE STRENGTH OF OUR COMPUTE TO DISRUPT AT SCALE

An approach characterised by individual small-scale disruptive efforts in individual countries or small partnerships is no longer sufficient to keep pace with SOC threats, let alone turn the tide. The Alliance must leverage one of its most powerful collective assets: computational capability.

The computational capabilities of coalition member states vastly outweigh those of OCGs. For example, an expanded AI research resource is currently being developed in the UK, as part of ongoing work to build a dedicated public-sector computational capability. France has also recently extended its Jean Zay supercomputer, making it one of the most powerful in Europe.[42] Other countries, such as the Netherlands, have identified a need for greater computing capacity to keep advancing in research.[43] Yet these national capabilities remain fragmented.

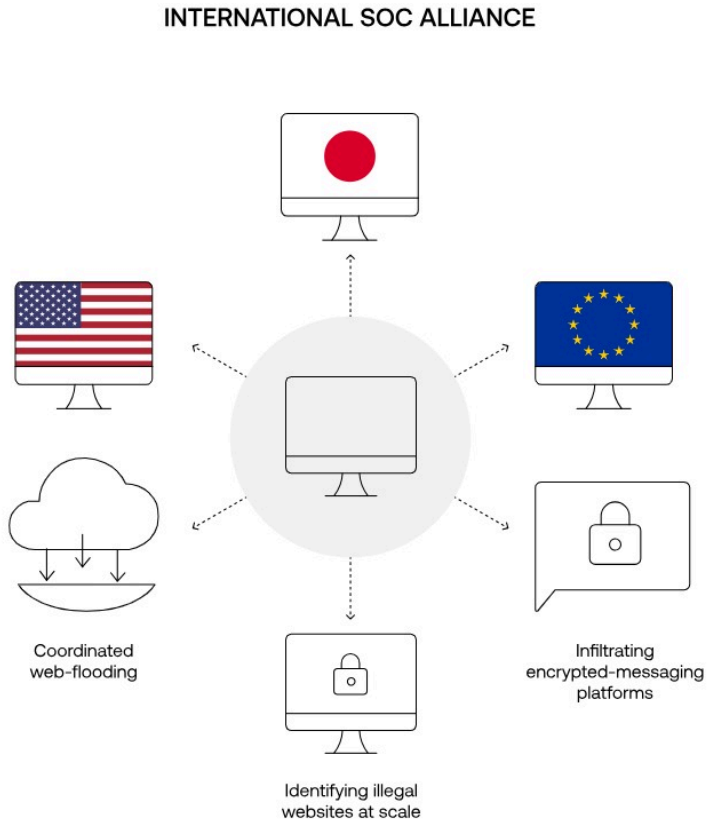
To address this, Alliance members would agree to designate a certain proportion of each country's existing computational capability to SOC. This would be preferable to centralising compute infrastructure, which would be expensive and may be seen as a national-security risk. Pooling the compute resources of member states would enable more efficient data analysis and effective, coordinated disruptive activity internationally, shifting the balance of power away from OCGs. Linking computational capability across borders, rather than merely coordinating discrete tasks, would allow for shared models, faster processing and a real-time collective response to SOC threats that no single country could achieve alone.

TACKLING ORGANISED CRIME THROUGH JOINT COMPUTATIONAL POWERS

Using the Alliance's combined computational powers would open the door to collective capabilities such as coordinated dark-web surveillance, the automated identification of fake websites, and the ability to run shared AI models across borders for real-time detection and intervention. Crucially, it could hugely increase the scale and impact of disruptive activity, both by expanding proven methods and unlocking new ones.

FIGURE 10

Tackling organised crime through joint computational powers



Source: TBI/Crest Advisory

By working together in this way, countries could tackle OCGs by:

- **Infiltrating and dismantling criminal platforms at scale.** Communications systems and online platforms used by OCGs can be a gold mine for intelligence. Some platforms host tens of thousands of users and deal in the trade or sale of illegal commodities or the planning and coordination of criminal activity. The infiltration of these platforms can yield vast quantities of information, which can be used to build a picture of criminal activity and methods, as well as enabling the identification and prosecution of key actors. Operation Trojan Shield – led by the FBI with Europol, the Australian Federal Police and others – used a Trojan-horse platform – ANOM – to capture millions of messages from criminal networks across 16 countries. More than 12,000 devices were distributed to criminal networks and all messages were automatically copied to controlled servers. The mass harvesting of data led to more than 1,000 arrests across 16 countries and the seizure of 32 tonnes of drugs, 250 firearms and more than $148 million in cash or cryptocurrency.[44] With pooled computational capacity, operations such as these can be scaled, making it possible to analyse captured data in real time, identify patterns and key actors faster, and to act globally with greater precision.
- **Deploying scalable digital-disruption tools.** Beyond infiltration, compute power can enable real-time, high-volume interventions targeting criminal infrastructure, such as denial-of-service (DoS) attacks or the flooding of platforms with fake data to degrade usability, which have been found to be effective. Recent research into interventions against booter services – platforms offering DoS attacks for hire – has found that large-scale actions such as mass takedowns and strategic disruption of online forums can significantly reduce attack volumes.[45] [46], For instance, interventions such as the Xmas 2018 operation[47] and the closure of Hackforums (see case study) led to a noticeable drop in attacks. While some displacement effects were observed (with activity shifting to remaining providers), this also made the market more brittle and susceptible to future disruption. When combined with strategic messaging to challenge perceptions of legality and harm within the offender community (for example, the NCA's targeted adverts), these interventions reduce both supply and demand. With greater compute, these tactics can be scaled up across platforms, increasing their disruptive effect.

Interventions Against Booter Services Offering Denial-Of-Service Attacks

Xmas2018 (FBI)

In 2018, the FBI seized 15 domains linked to booter websites and arrested the operators of DownThem, Ampnode and Quantum Stresser. These websites were well-known platforms in the cyber-criminal ecosystem that enabled users to pay to flood targeted websites or servers with traffic, overwhelming them and forcing them offline. These services were especially popular with low-skilled threat actors and were frequently used to disrupt gaming platforms, businesses and individual users. The intervention was timed just before Christmas to disrupt the seasonal spike in DoS activity over the holidays, and immediately took at least seven major services offline, destabilising the market and reducing attack volumes.

HackForums Closure

In 2016, following FBI engagement, HackForums – a prominent underground forum – removed its booter market and advertisements for booter services. The closure of HackForums as a booter marketplace created a significant gap in the ecosystem, reflected in reduced DoS attacks for 13 weeks globally.

NCA Search-Advert Campaign

Following the ban on HackForums adverts for booter services, the NCA ran a preventative messaging campaign using Google search adverts. These were triggered when users on UK IP addresses searched for booter-related

terms. The adverts warned of the illegality of DoS attacks and aimed to deter young people from engaging in cyber-crime by raising awareness of potential consequences.

Operation Bayonet

In 2017, Dutch and German police covertly seized control of the dark-net marketplaces AlphaBay and Hansa Market, hosting the sale of more than 350,000 illicit commodities including drugs, firearms and computer malware. Police were able to monitor user activity in real time and inject malicious data files to reveal users' IP addresses, harvest data and capture funds.

In a coordinated strategy, police shut down AlphaBay to encourage the displacement of activity to Hansa and maximise the disruptive impact of the operation. Police were able to capture 27,000 illicit transactions on Hansa before shutting down the site. The operation also led to arrests and vast amounts of intelligence being harvested.

These findings demonstrate that scalable, multifaceted interventions – particularly those combining technical disruption with strategic messaging – can have a meaningful and lasting impact on cyber-criminal infrastructure.

SUPPORT RAPID INNOVATION TO ENHANCE DISRUPTION EFFORTS

As OCGs exploit emerging technologies to scale their operations and evade detection, agencies involved in the response must keep pace, capitalising on cutting-edge tools to act faster, smarter and at greater scale.

Individual private companies have already identified key opportunities to apply innovative technology to law enforcement or societal problems – both in analysis and triaging of threats, and in developing disruptive capabilities. They are early adopters of new technologies (in a similar way to how OCGs use technology) including in anomaly detection, behavioural-pattern analysis, fraud detection in the financial sector and wider AI-driven threat detection. New technologies and innovation such as these must be harnessed collectively by the Alliance in order to scale opportunities quickly.

Thematic task forces would focus on identifying high-impact operational challenges and areas where innovation – whether technological or analytical – could enhance the detection, disruption and prevention of SOC. This could include much-needed capabilities including the means to assess and counter the criminal use of generative-AI technologies and the development of automated data-cleaning and harmonisation technologies, as well as common platforms for use by international law-enforcement agencies. These task forces would bring together government, law enforcement, the private sector and academic actors, forming public–private partnerships to address shared priorities.

Each task force would be supported by a dedicated innovation hub – a specialised unit designed to rapidly prototype, test and deploy technological solutions. These hubs, functioning as accelerators, would work closely with private-sector partners to source cutting-edge tools, co-develop solutions, and respond proactively to emerging threats. They would also facilitate the sharing and pooling of computational assets, for example, training data for machine-learning models, models architecture or their operating environments.

The secretariat, acting as the coordinating body for the Alliance, would support this model by synthesising findings, managing cross-border collaboration, and facilitating the rapid exchange of knowledge. Once a task force identified a specific challenge, the secretariat would develop and circulate an innovation brief to member countries. Countries would be encouraged to trial selected solutions using agile procurement routes

already available within their domestic systems. As a key feature of this work, results of trials would be shared through the alliance, and successful pilots scaled.

Defense Advanced Research Projects Agency (DARPA)

DARPA, the US defence innovation agency, has successfully developed innovative technologies to solve challenges in the defence sector, using an approach based on mobilising small teams with specific expertise across academics, industry and government to rapidly develop and pilot new capabilities.

Notable innovations include a project to develop the deepfake-detection technology Semantic Forensics which uses AI and machine-learning to analyse and recognise inconsistencies in facial expressions, voice patterns and tone, while also identifying errors in logic and linguistics.

The speed of innovation would be facilitated by existing procurement and data-sharing processes that are already in place through the wider activities of the coalition. Lessons learnt from task forces such as those delivered through DARPA should be applied – including the pooling of crowdsourced and collaboratively developed ideas, the formation of small, expert teams, and the clear articulation of challenges to solve. The clear sharing of risk and responsibility across task forces will also help to overcome risk aversion within law enforcement and encourage innovation.

03

Conclusion

As states navigate an era of rising geopolitical tension, rapid technological change and growing institutional fragility, serious and organised crime is evolving faster than the systems built to stop it.

Criminal networks today are agile, global and deeply embedded in the legal economy. They exploit digital tools, operate across borders and thrive in the gaps between fragmented enforcement regimes. Yet the international response remains outdated, slow and siloed.

A new approach is needed: the creation of an International SOC Alliance, comprising a core group of trusted countries and private-sector partners, which would come together to deliver coordinated and sustained disruption by targeting the shared infrastructure that enables organised crime to operate.

The Alliance would focus on two priorities. First, coordinated disrupted action with a sanctions regime designed to dismantle criminal operations from the top down at its core, raising the cost of illicit activity, targeting enablers, disrupting supply chains and reinvesting seized assets into vulnerable communities. Second, the deployment of technology at pace, pooling data and compute to identify threats earlier, act faster and deliver cross-border disruption in real time.

The UK has both the opportunity and the responsibility to lead. It has already begun to take a more strategic approach to SOC at home. But this is a global threat, and without coordinated international action, domestic reforms will always have limited impact. By championing the creation of the Alliance, the UK can help reshape the global response, bringing together trusted partners, embedding innovation and restoring control.

The consequences of the current fragmented response are increasingly visible: weakened institutions, growing corruption and cross-border threats that enforcement bodies struggle to contain.

To meet this challenge, the international community must match the speed, reach and ambition of the threat. That means narrowing the space in which organised crime operates, rebuilding public trust in enforcement systems and regaining strategic control.

The current approach is no longer sufficient. Structures built for a different era are not equipped to deal with the complexity of today's threat. A coherent, targeted and collaborative approach is urgently needed.

Grateful acknowledgment is extended to all participants from law enforcement, security agencies, the private sector, third sector and academia who generously shared their insights during our roundtables and helped inform the development of this paper.

Endnotes

1 https://ocindex.net/report/2023/03-global-overview-results.html

2 https://www.nasdaq.com/global-financial-crime-report

3 https://www.visionofhumanity.org/wp-content/uploads/2025/06/Global-Peace-Index-2025-web.pdf

4 https://www.mi5.gov.uk/director-general-ken-mccallum-gives-latest-threat-update

5 https://www.hybridcoe.fi/wp-content/uploads/2022/05/20220609-Hybrid-CoE-Research-Report-6-Non-state-actors-WEB.pdf

6 https://www.thetimes.com/uk/crime/article/wagner-group-gang-london-arson-attack-cbvqdq2wh?utm%5Fsource=chatgpt.com

7 https://www.nationalcrimeagency.gov.uk/who-we-are/publications/720-director-general-public-speech-to-launch-national-strategic-assessment-2023/file

8 https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime

9 https://www.ncsc.gov.uk/files/White-paper-Ransomware-extortion-and-the-cyber-crime-ecosystem.pdf

10 https://www.rusi.org/explore-our-research/publications/commentary/operation-destabilise-russia-organised-crime-and-illicit-finance; https://www.ft.com/content/31b9053f-343e-4c47-ace9-2b0080ec8799

11 https://www.europol.europa.eu/sites/default/files/documents/Europol%5Freport%5F-%5FLeveraging%5Flegitimacy%5F-%5FHow%5Fthe%5FEU%5Fmost%5Fthreatening%5Fcrim%5Fnetworks%5Fabuse%5Flegal%5Fbusiness%5Fstructures.pdf

12 https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021

13 https://www.europol.europa.eu/sites/default/files/documents/Europol%5Freport%5F-%5FLeveraging%5Flegitimacy%5F-%5FHow%5Fthe%5FEU%5Fmost%5Fthreatening%5Fcrim%5Fnetworks%5Fabuse%5Flegal%5Fbusiness%5Fstructures.pdf

14 https://www.bbc.co.uk/news/articles/c70ezyrep1go

15 https://www.rusi.org/explore-our-research/publications/commentary/charting-future-organised-crime-and-uks-response

16 https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

17 https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

18 https://go.chainalysis.com/2025-Crypto-Crime-Report.html

19 https://cloudandmore.co.uk/biggest-uk-cyber-attacks-2025/

20 https://cloudandmore.co.uk/biggest-uk-cyber-attacks-2025/

21 https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021

22 https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

23 https://cetas.turing.ac.uk/publications/ai-and-serious-online-crime

24 https://www.rusi.org/networks/shoc/informer/evolution-serious-and-organised-crime-diversifying-nature-criminal-operations-digital-age https://icclr.org/wp-content/uploads/2020/11/Confronting-or-Disrupting-Organized-Crime%5FYD%5F10Nov2020.pdf

25 https://www.adruk.org/fileadmin/uploads/adruk/Documents/Data_Insights/Data_Insight__The_outcomes_of_serious_and_organised_crime_cases_appearancse_in_England_and_Wales.pdf

26 https://www.bbc.com/news/world-europe-68416287

27 https://www.tandfonline.com/doi/epdf/10.1080/17440572.2021.2012460

28 https://globalinitiative.net/analysis/global-strategy-against-organized-crime-intersections

29 https://www.rusi.org/explore-our-research/publications/commentary/new-frontier-organised-immigration-crime-and-uk-sanctions

30 https://globalinitiative.net/analysis/global-strategy-against-organized-crime/

31 https://www.theguardian.com/world/article/2024/may/28/rwanda-uk-diplomat-interpol-target-regime-opponents?utm%5Fsource

32 https://www.cbinsights.com/research/report/startup-failure-reasons-top/

33 https://www.bbc.co.uk/news/articles/ckg3lpwx41xo

34 https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-2230.12864; https://www.gov.uk/government/news/uk-sanctions-target-the-lavish-lifestyles-of-putins-daughters

35 See *A New Approach to Serious and Organised Crime in the UK* (Tony Blair Institute for Global Change, 2024) for recommendations on regulatory interventions aimed at disrupting SOC. Available at: https://institute.global/insights/public-services/a-new-approach-to-serious-and-organised-crime-in-the-uk

36 https://resiliencefund.globalinitiative.net/

37 https://static1.squarespace.com/static/63e4aef3ae07ad445eed03b5/t/64e475c92e4c9a18a632ec63/1731067227329/SOCACE-RP18-UnderTheRadar-Aug23.pdf

38 https://www.scena9.ro/en/article/crime-community-social-reuse-confiscated-assets-italy-spain-romania; https://www.journalismfund.eu/crime-community-social-reuse

39 https://www.partnersalbania.org/publication/cause-confiscated-assets-used-for-social-experimentation-initiative

40 https://www.gov.uk/government/publications/crime-and-policing-bill-2025-factsheets/crime-and-policing-bill-international-cooperation-factsheet

41 Allen, C., Lock, T. (2024) ***Project Morpheus: Examining the potential to utilise Data Harmonisation to enhance international organised crime policing capabilities.*** p19

42 https://sciencebusiness.net/network-updates/cnrs-france-has-increased-its-ai-dedicated-resources-fourfold#:~:text=After%20its%20new%20extension%2C%20which,million%20billion%20operations%20per%20second.

43 https://www.nwo.nl/en/news/research-shows-dutch-science-needs-more-computing-power

44 https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive?utm%5Fsource

45 Collier, B., Thomas, D. R., Clayton, R., & Hutchings, A. (2019, October). Booting the booters: Evaluating the effects of police interventions in the market for denial-of-service attacks. In ***Proceedings of the internet measurement conference*** (pp. 50-64).

46 Vu, A. V., Collier, B., Thomas, D. R., Kristoff, J., Clayton, R., & Hutchings, A. (2025). Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services.

47 https://www.bbc.co.uk/news/technology-46647390

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Follow us

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

General enquiries

info@institute.global