PaCCS Policy Briefing

Maximising Impact from Serious Organised Crime Research

Understanding the Challenges.

Undermining the Threat.

Partnership for
Conflict, Crime &
Security Research

Foreword:

Serious organised crime (SOC) presents an urgent and complex challenge that the academic research community has substantial capacity to address. In the autumn of 2021, the Partnership for Conflict, Crime & Security Research (PaCCS) convened more than 130 participants for a virtual conference on *Maximising Impact from Serious Organised Crime Research.* This created a space for academics, policymakers, and practitioners to come together to explore how insights from research can help us understand and undermine SOC.

Through participation in roundtables, networking sessions, keynote addresses, and *Snapshot* presentations, we explored the following seven workstreams:

- Modern Slavery & Human Trafficking
- Economic & Financial Crime
- Blue & Green Crimes (Maritime & Environmental)
- Gangs & Syndicates (Arms, Drugs & Extortion)
- Victims & Harms (including Child Sexual Exploitation)
- Cyber-Crime & Online Criminal Markets
- Criminal Conflict & Political Violence.

In this PaCCS Policy Briefing, we share insights into how policymakers and practitioners can better understand and undermine SOC. Throughout, readers will encounter the strategic and systemic challenges faced by those seeking to combat transnational organised crime. We then present opportunities to improve responses through the *'5Cs'* of Culture, Comprehension, Communication, Capacity, and Capabilities.

Dr Tristram Riley-Smith, PaCCS Champion

Understanding the Challenges:

A. The Elusiveness of the SOC Threat

1. The Enigmatic Nature of Local Root Causes

1.1 **Local factors** play a critical role in engendering and evolving SOC (combined with the shaping effects of global environmental & geopolitical factors). *This leads to great variance in the manifestation of SOC, making it difficult to grasp root causes without detailed knowledge of the context.*

1.2 Counterintuitively, **SOC Groups can be popular at a local level**, especially if providing a public service where the state fails to meet primary human needs. *Their social capital can be further strengthened if criminal activities are combined with the pursuit of a political / ideological mission.*

2. The Confusion of Actors & Activities

2.1 Lines between the **licit & illicit** can be ambiguous and fluid. This can extend to the state (and/or its ruling elite) being SOC actors themselves. SOC Groups benefit from this uncertainty and the vulnerable can become criminalised.

2.2 Lines can be blurred between **victim and offender**, disorienting those involved in Criminal Justice and/or Victim Support.

3. The Entrepreneurial Qualities of SOC Enterprises

3.1 SOC enterprises are like **innovative entrepreneurs exploiting new opportunities** with speed and agility. They are free from shackles of regulation or legislation, with unfettered access to cyberspace and with access to compliant human capital.

3.2 Dynamic and covert interactions between different **types of serious & organised criminality** add to the confusion and lack of comprehension. Money-laundering and cyber operations touch on many SOC activities.

B. The Vulnerability of the Counter-SOC Domain

1. Data Paucity Impairs Strategy (and vice versa)

1.1 There is a major problem with **paucity of data** (which is either lacking or locked away in silos). Administrative obstacles and a culture of "need to know" too often stand in the way, creating blind spots that inhibit the understanding that is so critical to an effective response.

1.2 This problem is reinforced (in the UK at least) by the absence of a coherent, strategy to tackle SOC. There is over-reliance on Criminal Justice System, with no underpinning Risk Management process (informed by threat/harm analysis) to devise, evaluate and action countermeasures (including deterrence & disruption).

2. Scant Communications Reduce Impact

2.1 There is a **lack of awareness** of the SOC threat (in terms of intention and harm). This affects targets & victims of SOC, as well as those responsible for countering it.

2.2 There is no **coherent communications strategy** to deter SOC (for instance, to dissuade/discourage people to join or facilitate SOC operations and/or to avoid procuring SOC products & services.

3. Borders and Bureaucratic Boundaries Frustrate Collaboration

3.1 **Political territories and jurisdictions** are ill-suited to the transnational nature of SOC. Cyberspace is borderless for the criminal, but border-full for Criminal Justice Systems (with 18,528 borders in cyberspace – between one country and 193 others).

3.2 The strategic tasks of pursuit, prevention and protection fall to a **multiplicity** of domestic Government Agencies, Private Companies and NGOs which are too easily disengaged or mis-connected. There is little incentive to cooperate with others.

Undermining the Threat

A. Culture

1. Risk Management

1.1 There is an urgent need to build **a Risk Management culture** to drive the strategic fight against SOC, with the authority to guide efforts that collect/analyse empirical evidence to understand harms (as well as threats); identify / prioritise vulnerabilities; and to formulate / instigate mitigations based on growing knowledge of what works.

1.2 This should underpin an **operational culture where measured risks are taken** in a collective effort committed to agility, transparency, and movement at pace, while still maintaining excellence.

2. Strategy

2.1 A strategic mindset must inform and drive the work of those involved in countering SOC. Early action is needed to review the “Four Ps” (Pursue, Prevent, Protect and Prepare) and consider alternatives (e.g., Scotland’s “Five Ds”: Divert, Deter, Detect, Disrupt and Develop).

2.2 This should lead, as soon as possible, to the design of a full suite of SOC countermeasures (subject to periodic review). This will balance out different strands of mitigation, almost certainly reducing the burden on the Criminal Justice System.

3. Collaboration

3.1 There is a necessity to create **a collaborative culture** between all UK organisations with a part to play in undermining SOC. This can begin with public sector agencies, but must extend to the private sector, NGOs, and academia.

3.2 We should look for opportunities to build **international collaboration**, to overcome the challenges of international borders and jurisdictions.

B. Comprehension & Communication

1. SOC Information Management Strategy

1.1 There is an urgent need for a strategic approach to data collection and storage, overcoming compartmentalised and/or inadequately curated data and generating new information sources.

1.2 There needs to be a change in approach to Data Protection and Data Release combining “need to know” with “dare to share”.

2. SOC Knowledge Management Strategy

2.1 We need to enhance understanding of the SOC phenomenon in all its varieties, ensuring knowledge is widely available to those who need to know. As a high priority, Risk Management processes need clarity over **harms, threats & mitigations** (so that priorities are set based on what matters and what works).

2.2 A **strategic research programme** must emerge from the above. In the short-term, research is needed into understanding root causes, supply chains & harms; and uncovering SOC interactions with key enablers such as money-laundering and cyberspace Research is also needed into best practice and what works?

3. SOC Communications Strategy

3.1 A SOC Communication Strategy, informed by targeted audience analysis, should lead to engagement with key sectors to deliver **Threat Awareness, Deterrence, Community Engagement, & Market Intervention**.

3.2 This Strategy must be about **<u>listening</u> as well as messaging**. SOC Research has shown the benefit of including innovative communication techniques (such as use of collage and *Spoken Word*).

<u>C. Capacity & Capability</u>

1. Strategic Structures and Delivery Teams

1.1 We need to strengthen structures delivering SOC Threat Analysis (with a greater emphasis on harms / what matters) and establish a separate centre to conduct Risk Management (considering the full range of mitigating actions / what works).

1.2 We need parallel & blended workforces to counter SOC, bringing public, private and third sectors together to deliver the full range of solutions (e.g. “4Ps” or “5Ds”).

2. Skills & Expertise

2.1 We need a **national approach to capability development**, to make the most use of innovation and creativity across all sectors; and to optimise the use of scarce resources. It should start with Risk Management experts to lay and maintain the foundations of any strategic effort directed against SOC.

2.2 The **shape, quality & weight of any network** will emerge over the medium-term, determined by strategic plans. In the short-term, we should extend technical literacy to inform policymakers & practitioners; review/enhance specialist skills supporting the Criminal Justice System; and invest in those working with survivors & victims.

3. Systems & Tools

3.1 We need greater **coherence about the acquisition of systems & tools** to counter the SOC threat, tapping into innovative solutions emerging from UK industry (including small and medium-sized enterprises).

3.2 The **SOC Information Management Strategy should inform procurement**. There appears to be an urgent need to replace/upgrade the UK’s Police National Database and to maximise access to / involvement with relevant international data sources

BAC
POLICE

PaCCS:

The Partnership for Conflict, Crime & Security Research was initiated by the research councils which now form part of UK Research and Innovation (UKRI). The Partnership aimed to deliver high quality and cutting-edge research to help improve our understanding of current and future global security challenges (focusing on the themes of Conflict, Cybersecurity and Transnational Organised Crime). It has brought together researchers from across disciplines to work on innovative projects and created opportunities for knowledge exchange between academia, government, industry, and the not-for-profit sector. The partnership is supported by a Research Integrator (Dr Tristram Riley-Smith) based at the University of Cambridge.

This policy briefing was authored by Dr Tristram Riley-Smith and was edited and designed by PaCCS Communications Officer Kate McNeil.

Acknowledgements:

This conference was made possible with the support of PaCCS' funders ESRC and AHRC.

In 2018, PaCCS funded 5 awards to researchers conducting work on deepening and broadening our understanding of transnational organised crime. We are grateful to these projects for the critical contribution they made to this conference:

Dr Ella Cockbain (University College London) *Deciphering and disrupting the social, spatial, and temporal systems behind transnational human trafficking: a data science approach*

Professor Timothy Edmunds (University of Bristol) *Transnational organised crime at sea: new evidence for better responses*

Dr Gernot Klantschnig (University of York) *Hidden narratives of transnational organised crime in West Africa*

Dr Raphaël Lefèvre (University of Oxford) *The crime-terror nexus: Investigating the overlap between criminal and extremist practices, narratives and networks in Tripoli, Lebanon.*

Professor Michael Levi (Cardiff University) *How online technologies are transforming transnational organised crime (Cyber-TNOC)*

We would also like to acknowledge the important role played by our keynote speakers (Professor Jennifer Rubin and Martin Hewitt) and chairs: Sir Craig Mackey, Deeph Chana, Gloria Laycock, Mike Barton, Sebastian Madden, Suzanne Raine, Tim Symington, and Tim Wilson.

Partnership for
Conflict, Crime &
Security Research

This Policy Briefing was created by The Partnership for Conflict, Crime & Security Research.