Project Morpheus 2.0: A strategy to utilise data harmonisation to enhance international organised crime policing capabilities

Centre for Study of Organised Crime

Dr Chris Allen, Senior Associate Fellow

In Partnership with

Precis- Morpheus 1.0

Published in Autumn 2024 Project Morpheus1.0 was a piece of blue-sky research on Data harmonisation (DH) and the impact it could have countering organised crime - the idea that all law enforcement information could be pooled, and all knowledge shared, in the fight against crime.

In Greek Mythology, Morpheus is the God of dreams. But while the project name is mythical its aims and objectives are based firmly in reality, with implications for tactical and strategic law enforcement capability in the long term.

This report considered the potential of new technology, and the opportunities and challenges it brings, for developing new intelligence databases and merging existing ones. Specifically, through a mixed method approach the report tested the validity of the concept of DH to gain operational, tactical and strategic benefits as a viable future path for policing.

The paper consistently highlighted the difficulties in countering organised crime. These challenges arise from the diverse standards, priorities, and resources , coupled with the varied nature of criminal activity and organised crime structures.

Harmonising data can significantly improve the fight against organised crime. Firstly, it leads to more effective international investigations by allowing efficient cross-border or cross force data sharing. This allows police officers working in joint investigative teams to access and analyse information quickly, using a common terminology. Secondly, creating specialised systems that allow access to existing databases across different countries provides a more comprehensive view of criminal activity. This increased access to information can be vital in identifying and disrupting organised crime.

Data Harmonisation offers significant benefits in the fight against organised crime. It provides advanced analytical capacity, allowing investigators to 'join the dots' and gain enhanced insights. By providing access to a richer and more complete dataset, including historical context, it gives investigators an operational advantage and improves team situational awareness during operations.

Currently, investigators often rely on keyword searches in police databases, requiring them to guess every possible synonym for a topic. This makes it difficult to collate and cross-reference information from different international sources. A standardised lexicon would solve this problem and enable the development of effective text-mining software.

Artificial Intelligence offers a broader approach, capturing diverse data not limited to crime systems. By pulling in information from non-specialist sources, it builds a richer picture of the criminal context. This convergence of technology creates new demands for law enforcement, allowing for a more integrated view of information and increased efficiency.

However, it also presents a risk: if UK law enforcement remains outside these processes for managing large-scale IT systems in the areas of freedom, security, and justice, it will become less effective in combating organised crime and will be sidelined as a key contributor and receiver of information.

There are multiple barriers to a 'one database fits all' approach to intelligence sharing.

Firstly, even in developed nations like the UK, sharing data effectively within and between forces, let alone internationally, is a huge challenge. While systems like the organised crime group mapping system exist, they operate on a very basic level. Devising a solution that surpasses the current capabilities of agencies like Europol or Interpol is a significant undertaking.

Secondly, many countries lack the policing capabilities of developed nations. For example, a cybercrime unit in an African country may lack basic resources like computers, making data harmonisation a low priority. Similarly, nations that are still developing economically and act as strongholds for organised crime, such as Macedonia, lack the necessary national intelligence infrastructure to participate in data harmonisation efforts. While the UK also lacks a single national intelligence system, its capacity to share and analyse data far exceeds that of less developed countries.

The Morpheus recommendations are:

1. Transform Organised Crime Group (OCG) Mapping into a National Intelligence Hub: Significantly expand the scope and functionality of OCG Mapping to create a single, comprehensive source of OCG intelligence for all UK law enforcement agencies. This will improve collaboration and intelligence sharing, enabling a more coordinated and effective response to organised crime.

2. Establish a Unified National Body to Combat Organised Crime: Consolidate organised crime responsibilities currently divided between the National Crime Agency and Regional Organised Crime Units into a single, powerful national body. This would streamline operations, eliminate jurisdictional barriers, and foster a cohesive approach to tackling organised crime across the country.

3. Resolve Legal Barriers to Cloud Adoption: Conduct a comprehensive review of legal and regulatory issues surrounding cloud computing within UK policing. Address these challenges to pave the way for secure and efficient data storage and access, enabling effective data harmonisation across different platforms and systems.

4. Develop a Specialist Cadre of Data-Savvy Investigators: Implement a new training and recruitment programme to create a dedicated cadre of officers skilled in navigating multiple systems and digital media investigations. These specialists will be equipped to leverage sophisticated analytical tools and maximise the potential of data harmonisation for complex investigations.

5. Foster Trust and Collaboration through Formal Agreements: Establish a formal agreement between stakeholders and agencies to address the existing trust deficit. This agreement should clearly define roles, responsibilities, data access protocols, and information sharing frameworks, ensuring transparency and accountability within the data harmonisation process.

6. Standardise Terminology for International Compatibility: Develop a standardised glossary of common terminology for data entry into police databases. This glossary should be adopted nationally and aligned with international standards to facilitate seamless information exchange and collaboration with international law enforcement agencies.

Morpheus 2.0 report takes these recommendations and looks at how we can put them into practice, providing a strategy as to how law enforcement could utilise a DH approach within their own systems and processes, and crucially outlining some of the key issues that they are likely to face when doing so.

Strategy to Enhance Data Harmonisation within Law Enforcement

A strategy to enhance data harmonisation within law enforcement should focus on practical, phased implementation while ensuring alignment with national and international standards, fostering collaboration across borders, and addressing the existing gaps in technology, resources, and legal frameworks.

While each police force and nation will undoubtedly have its own requirements, challenges and idiosyncrasies, below is a broad-brush strategy to move forward and can be adapted to a local, regional, national and international level.

1. Establish a Centralised Data Harmonisation Task Force

Create a dedicated task force focused on advancing data harmonisation across law enforcement agencies. This task force will:

- Oversee the development and implementation of data-sharing frameworks.
- Coordinate between stakeholders
- Address issues related to terminology standardisation, legal and regulatory barriers, and technological requirements.

Key Actions:

- Appoint a leadership team and define roles and responsibilities.
- Conduct an audit of existing data systems, identifying key barriers to harmonisation and gaps in infrastructure.
- Ensure that legal, political, and jurisdictional concerns are addressed in collaboration with national legal bodies and international partners.

Steps:

1. **Appoint Leadership:**
    - Identify key leaders within national law enforcement, technology, and legal sectors.
    - Form a diverse task force with representatives from various agencies, including law enforcement, IT experts, legal advisors, and international liaison officers.
2. **Define Roles and Responsibilities:**
    - Develop a clear organisational structure with assigned roles (e.g., project manager, data security lead, liaison officers for international cooperation).
    - Create a mission statement outlining the task force's primary goals.
3. **Conduct Initial Assessment:**
    - Perform an audit of current data systems, processes, and technologies used across agencies.

- Identify key barriers to harmonisation, including technology gaps, legal restrictions, or operational challenges.

4. **Set Milestones and Deadlines:**
    - Define short-term and long-term milestones, such as technology updates, international agreements, and training programs.
    - Set quarterly review deadlines to track progress.
5. **Create a Communication Plan:**
    - Establish a communication strategy for internal and external stakeholders (e.g., regular reports, briefing sessions).
    - Set up a secure, centralised platform for task force communications and documentation.

2. Develop a Unified Organised Crime Intelligence Platform

This system should:

- Integrate and standardise data from all law enforcement agencies and external intelligence sources.
- Serve as the primary tool for intra and inter force as well as cross-border information exchange, leveraging both traditional policing data and newer sources such as social media, financial records, and cybersecurity intelligence.
- Incorporate AI-driven analysis and machine learning to enhance data mining, pattern recognition, and predictive analytics.

Key Actions:

- Expand the functionality of existing OCG mapping and analysis systems to include real-time data integration from multiple sources.
- Ensure scalability and flexibility to accommodate future technological advancements.
- Train users in data entry standards, system operations, and effective data sharing protocols.
- Establish secure cloud-based storage solutions, addressing legal and regulatory barriers to cloud adoption.

Steps:

1. **Map Current Systems:**
    - Survey existing Organised Crime Group (OCG) Mapping and intelligence-sharing systems.
    - Identify data sources to integrate (e.g., regional police systems, national databases, Europol, Interpol).
2. **Design the Unified System:**
    - Define technical specifications for the platform, ensuring scalability, security, and compatibility with current and future technologies.
    - Collaborate with IT experts to develop an architecture that can support large datasets, AI integration, and real-time data sharing.
3. **Secure Funding and Resources:**
    - Estimate costs for development, training, and operational support.
    - Submit funding proposals to the government or relevant agencies.
4. **Develop the Platform:**
    - Choose a development team with expertise in large-scale law enforcement systems.

- Begin building the platform, focusing on data integration, AI capabilities, and user interface.

5. **Pilot Testing and Rollout:**
    - Conduct pilot testing with a select number of agencies.
    - Gather feedback and make necessary improvements before launching the platform nationwide.
6. **Ongoing Support and Maintenance:**
    - Establish an IT support team for troubleshooting and system maintenance.
    - Schedule regular system updates and security audits.

3. Integrate International Data Sharing Standards

To facilitate seamless data sharing across borders, a standardised lexicon for terminology and classification should be developed and adopted both nationally and internationally. This will support more effective cross-border investigations and increase the accuracy and relevance of shared intelligence.

Key Actions:

- Create a working group to develop and implement a comprehensive glossary of terms used in criminal investigations (e.g., for organised crime, trafficking, cybercrime, etc.).
- Collaborate with international partners to ensure that the glossary aligns with EU and global data-sharing frameworks.
- Implement automatic text-mining tools to standardise the analysis of unstructured data from diverse sources, including police databases and public information.

Steps:

1. **Establish a Working Group:**
    - Form a group with national and international law enforcement agencies, including Europol, Interpol, and other relevant bodies.
    - Involve linguistic experts and data scientists to design the terminology framework.
2. **Develop a Comprehensive Glossary:**
    - Create a glossary of standardised terms for criminal activities, categories, and investigative processes.
    - Align the glossary with existing international standards used by organisations like Interpol and Europol.
3. **Pilot the Terminology:**
    - Introduce the glossary within a limited region or agency, conducting tests on data entry and retrieval.
    - Evaluate the ease of use and clarity of terms for investigators.
4. **Rollout:**
    - Ensure that all participating agencies adopt the glossary.
    - Offer training programs for investigators and database administrators to familiarise them with the new terms.
5. **Monitor and Update:**
    - Set up a committee to review the glossary annually and incorporate new terms or adapt existing ones based on emerging crime trends.

4. Invest in Digital Training and Recruitment

Given the growing complexity of data analysis and the integration of diverse datasets, a new cadre of data-savvy investigators is essential. This initiative should focus on:

- Recruiting individuals with expertise in data science, digital forensics, and cybercrime investigation.
- Providing comprehensive training for current officers on emerging technologies such as artificial intelligence, machine learning, and big data analytics.
- Incorporating best practices from other sectors (e.g., cybersecurity, finance) into law enforcement training programs.

Key Actions:

- Design a new training curriculum focused on advanced data analysis techniques, cloud computing, and the operation of integrated intelligence systems.
- Promote cross-disciplinary training to foster collaboration between traditional investigators and IT/data experts.
- Establish a professional development programme that includes ongoing training to keep investigators updated on the latest technological advancements.

Steps:

1. **Design a Training Curriculum:**
    - Collaborate with educational institutions, technology companies, and law enforcement agencies to create a curriculum on data science, digital forensics, and AI in criminal investigations.
    - Ensure that the curriculum covers both technical and operational aspects of data harmonisation.
2. **Launch a Recruitment Campaign:**
    - Advertise vacancies for officers with data science or cybersecurity backgrounds.
    - Focus on attracting individuals who can bridge the gap between law enforcement and technology.
3. **Implement Training Programs:**
    - Begin with a core group of investigators who will receive intensive training on using the new systems and tools.
    - Roll out regular, ongoing training sessions for the wider force, including in-field training for using the unified intelligence platform.
4. **Assess and Certify:**
    - Create assessment criteria for participants to ensure they have mastered necessary skills.

    - Provide certifications for successful completion of training to ensure standards are maintained.

5. **Provide Continuous Learning:**

Organise annual refresher courses and keep investigators updated on technological advancements and evolving criminal tactics.

5. Build Trust through Formal Agreements and International Collaboration

The success of data harmonisation relies on trust and collaboration between stakeholders. A formal agreement between national law enforcement agencies, international bodies, and private sector partners (e.g., cloud service providers, tech companies) will help mitigate concerns over data security and usage.

Key Actions:

- Establish a Memorandum of Understanding (MoU) with international partners to formalise data-sharing agreements, outlining roles, responsibilities, and data access protocols.
- Introduce transparent oversight mechanisms to ensure accountability and compliance with legal standards.
- Develop a secure, encrypted framework for data sharing that allows for real-time access while maintaining control over sensitive information.

Steps:

1. **Identify Key Stakeholders:**
    - Identify national and international law enforcement bodies, private-sector partners (e.g., cloud providers), and regional agencies to involve in the agreements.
2. **Develop a Memorandum of Understanding (MoU):**
    - Draft an MoU that clearly defines data-sharing protocols, roles, responsibilities, and privacy measures.
    - Include terms for compliance with national and international data protection laws.
3. **Secure Legal and Political Endorsements:**
    - Work with legal advisors to ensure that the MoU adheres to relevant legislation and international law.
    - Present the MoU to senior law enforcement leaders and government officials for approval.
4. **Negotiate with International Partners:**
    - Engage with Interpol, Europol, and other agencies to formalise data-sharing agreements.
    - Ensure that data-sharing protocols are aligned with global standards.
5. **Establish Transparency and Accountability Mechanisms:**
    - Set up oversight committees to monitor the implementation of data-sharing protocols.
    - Ensure transparent reporting and regular audits of data-sharing activities.

6. Address Resource and Infrastructure Gaps in Less Developed Nations

While data harmonisation is critical, it is equally important to consider the resource disparities between law enforcement agencies in developed and less-developed nations. Specific strategies should be devised to:

- Provide technical support and infrastructure to countries with limited resources.
- Offer training and capacity-building initiatives in regions struggling to keep up with digital policing advancements (e.g., countries in Africa or the Balkans).
- Foster partnerships with international development organisations and the private sector to assist with resource allocation.

Key Actions:

- Develop tailored capacity-building programmes for developing countries, including remote training modules, hardware donations, and technology sharing agreements.
- Create global funding mechanisms for law enforcement agencies to improve their technological infrastructure.
- Encourage international cooperation through shared databases and joint operations that do not require all participants to have identical technological capabilities.

.

Steps:

1. **Assess Resource Gaps:**
    - Conduct a survey of law enforcement agencies in less-developed nations to identify technological and resource limitations.
2. **Develop Capacity-Building Programs:**
    - Design training modules and resource-sharing initiatives to help less-resourced countries improve their policing infrastructure (e.g., hardware, software, training).
3. **Partner with International Organisations:**
    - Engage with organisations like the UNODC or World Bank to secure funding and support for infrastructure development.
4. **Offer Technology Assistance:**
    - Provide cloud-based solutions and affordable technologies to help build local law enforcement capabilities.
5. **Create Regional Support Hubs:**
    - Set up regional hubs for technical support and training, where less-developed nations can receive hands-on guidance from experts.

7. Implement Regular Audits and Feedback Loops

To ensure that the data harmonisation strategy remains relevant and effective, it should include mechanisms for ongoing evaluation and refinement. Regular audits and feedback from frontline officers and international partners will allow law enforcement agencies to:

- Identify areas of improvement in terms of system interoperability, data sharing, and investigative effectiveness.
- Address emerging threats and challenges, including new forms of organised crime and technological advancements.

Key Actions:

- Set up an independent body to conduct regular audits on the effectiveness of the data harmonisation process.
- Organise periodic feedback sessions with investigators and international stakeholders to gather insights on the operational challenges.
- Continuously update training, infrastructure, and policy frameworks based on audit findings.

Steps:

1. **Set up an Audit Committee:**
    - Appoint a group of independent experts to evaluate the data harmonisation efforts periodically.
2. **Design Audit Criteria:**
    - Develop a checklist based on performance metrics (e.g., data accuracy, system integration, user satisfaction).
3. **Conduct Regular Audits:**
    - Schedule annual audits to assess the effectiveness of the harmonisation process.
4. **Implement Feedback Loops:**
    - Collect feedback from investigators, international partners, and data users to identify pain points.
5. **Adjust Strategy Based on Findings:**
    - Use audit results and feedback to make improvements in training, systems, and operational processes.
    - Adjust the strategy annually to reflect changes in technology and criminal activity.

Challenges

Implementing a comprehensive strategy to enhance data harmonisation within law enforcement is a significant undertaking and will face several challenges. These challenges stem from technical, organisational, legal, and political issues. Below are the key challenges that could arise, along with some insights into how they might be addressed:

1. Resistance to Change from Law Enforcement Personnel

Law enforcement agencies are often characterised by established protocols, ingrained practices, and hierarchical structures. Officers and staff may resist changes that require adopting new systems, tools, and methodologies.

Potential Solutions:

- **Training and Communication:** Clearly communicate the benefits of data harmonisation, focusing on how it improves operational efficiency and crime-fighting capabilities.
- **Involvement in Design:** Involve frontline officers in the development and testing phases to ensure that the systems are user-friendly and meet real-world needs.
- **Ongoing Support:** Offer continuous training, mentorship, and feedback loops to help officers adapt to new systems and technologies.

2. Interoperability Between Different Systems and Agencies

Different law enforcement agencies and countries use diverse systems, platforms, and databases. Achieving seamless interoperability can be complex due to varying technological capabilities and software compatibility issues.

Potential Solutions:

- **Standardisation of Protocols and Formats:** Develop and implement standard data formats, communication protocols, and API standards that allow different systems to communicate effectively.
- **Phased Implementation:** Start by integrating small, manageable systems and scale up to more complex ones as systems mature and capabilities improve.
- **Partnership with Technology Providers:** Work with external vendors to help facilitate system integration and overcome technical barriers.

3. Legal and Regulatory Barriers

Legal frameworks governing data privacy, sovereignty, and sharing (such as GDPR in Europe) may conflict with the needs for open and efficient data sharing across borders. Laws may prevent certain types of data from being shared or stored in certain locations, particularly in international contexts.

Potential Solutions:

- **Legal Review and Adjustments:** Establish a working group with legal experts to review existing laws and propose changes that balance data sharing with privacy and data protection rights.
- **International Agreements:** Work on formal international agreements (e.g., Memorandums of Understanding, Bilateral Agreements) that allow for secure cross-border data sharing while respecting national laws.
- **Encryption and Anonymisation:** Employ advanced encryption and anonymisation techniques to ensure compliance with privacy regulations while facilitating effective data sharing.

4. Data Quality and Standardisation

Inconsistent data entry standards, terminology, and quality across different jurisdictions will make harmonisation difficult. For instance, different countries may use different terminologies for the same criminal activity or case, leading to confusion and errors in data interpretation.

Potential Solutions:

- **Development of a Unified Lexicon:** As mentioned, developing a standardised glossary of terminology that all agencies adopt is crucial. This lexicon should be periodically updated based on emerging trends in crime.
- **Data Quality Assurance Protocols:** Implement strict data quality assurance practices, including regular audits and training to ensure consistency in data collection, entry, and processing.

5. Resource Constraints in Developing Nations

Less-resourced countries, especially in regions like Africa, Latin America, or parts of Eastern Europe, may struggle to implement advanced data harmonisation initiatives due to lack of infrastructure, training, or financial resources.

Potential Solutions:

- **International Support and Partnerships:** Engage in partnerships with international organisations (e.g., the UNODC, World Bank) to provide technical and financial support for resource-limited nations.
- **Targeted Capacity Building:** Focus on building basic infrastructure (e.g., providing low-cost data storage solutions, offering remote training) that can help these countries catch up with international standards.

6. Data Security and Privacy Concerns

The more data that is shared and stored, the greater the risk of data breaches, misuse, or cyberattacks. Data security becomes a major concern, especially when dealing with sensitive criminal intelligence.

Potential Solutions:

- **Strong Encryption and Access Control:** Implement end-to-end encryption and enforce strict access controls based on roles, ensuring that only authorised personnel can access specific datasets.
- **Cybersecurity Infrastructure:** Invest in robust cybersecurity infrastructure to protect data integrity and prevent hacking, focusing on both national and international levels.
- **Regular Audits:** Conduct regular security audits to identify vulnerabilities and ensure compliance with data protection laws.

7. Political and Jurisdictional Differences

Political differences and competing national interests may hinder the creation of unified systems for data sharing. Countries may be reluctant to share data, fearing that it could undermine their sovereignty, security, or political relations.

Potential Solutions:

- **Diplomatic Efforts and Trust Building:** Establish diplomatic dialogue through law enforcement summits and international cooperation forums (e.g., G7, G20) to build trust and understanding of the shared benefits of data harmonisation.
- **Incremental International Cooperation:** Start with small, bilateral agreements with willing countries and gradually expand as trust grows and systems prove effective.
- **Transparency and Clear Protocols:** Develop clear and transparent data-sharing agreements that outline how the data will be used, who will have access, and what safeguards will be in place.

8. Technological Advancements and Rapid Change

The rapid pace of technological change means that data harmonisation systems must be adaptable to new tools and techniques, such as machine learning, AI, or blockchain, to stay effective against evolving criminal activities.

Potential Solutions:

- **Modular System Design:** Develop systems with modular, scalable architectures that can easily incorporate new technologies as they emerge.

- **Continuous Innovation:** Keep a dedicated team or innovation unit focused on monitoring emerging technologies in criminal justice and cybersecurity, ensuring that the law enforcement strategy evolves with advancements.
- **Public-Private Partnerships:** Work with tech companies and research institutions to stay at the forefront of technological innovation and integrate new tools into the harmonisation process.

9. Lack of Political Will and Resources for Long-Term Implementation

Securing the necessary funding, political support, and resources for long-term implementation may prove difficult, especially when immediate results are not visible.

Potential Solutions:

- **Demonstrating Early Wins:** Start with pilot projects or specific regional successes to demonstrate the effectiveness of data harmonisation and gain political backing.
- **Long-Term Planning and Funding:** Work with governments and international bodies to secure long-term funding, possibly through EU funds, public-private partnerships, or international law enforcement grants.
- **Advocacy and Lobbying:** Advocate for the long-term importance of data harmonisation by showcasing its impact on reducing organised crime and improving national security, thus ensuring sustained political and financial support.

10. Cybercrime and Digital Evidence Challenges

Organised crime often involves sophisticated cybercrime operations, where evidence may be scattered across multiple platforms and jurisdictions. Collecting and harmonising this data presents unique challenges.

Potential Solutions:

- **Cross-Border Digital Evidence Protocols:** Work with international bodies to develop standardised protocols for collecting, storing, and sharing digital evidence in a way that respects jurisdictional boundaries.
- **Cybercrime Task Forces:** Create specialised cybercrime task forces within the harmonisation framework, integrating digital forensics experts who can track and manage digital evidence across borders.

Conclusion:

This strategy provides a comprehensive and phased approach to enhancing data harmonisation within law enforcement. By focusing on system integration, standardisation, training, and international collaboration, it will ensure that law enforcement agencies are equipped with the tools, knowledge, and cooperation necessary to combat organised crime effectively. Addressing both technological and resource gaps, along with building trust across borders, will significantly enhance global efforts to dismantle criminal networks.

By following this step-by-step guide, law enforcement agencies can systematically enhance data harmonisation efforts. The guide provides a clear path from establishing a task force to implementing a continuous feedback and improvement cycle, ensuring the strategy remains effective and adaptive to new challenges in combating organised crime.

While implementing this strategy presents significant challenges, these can be mitigated through careful planning, cross-border collaboration, investment in infrastructure, and a commitment to long-term engagement. Addressing these challenges with a clear focus on the benefits of data harmonisation—such as improved coordination, faster intelligence-sharing, and enhanced crime-fighting capabilities—will ultimately lead to more effective global efforts against organised crime.

Any questions or inquires should be directed to chris.allen@centresoc.com