Criminal minds

Social science helps to tackle organised crime

Law enforcement authorities are increasingly turning to behavioural sciences to help with the fight against organised crime. Drawing on research conducted with the UK National Crime Agency, Anna Sergi examines how this new approach is being put to practical use.

Key points

- Governments and law enforcement agencies are exploring new ways to tackle organised crime, including the use of social and behavioural science.
- Behavioural sciences can be deployed to both online and offline criminality, with psychological concepts particularly useful in investigations into child sexual exploitation.
- Such an approach can be used to develop effective strategies for preventing and disrupting crime, and will also facilitate alternative approaches to fighting criminal exploitation of technology and cyber-crime.

A total of 414 illegal websites on the 'dark net' (parts of the internet outside the reach of traditional search engines) were closed and 17 people were arrested in early November 2014 following Operation Onymous – a joint operation between Europol, the US Federal Bureau of Investigation (FBI) and the US Homeland Security Investigations (HSI).

The closed websites (including Topix, Cloud 9, Black Market, and Silk Road 2.0) granted anonymity to users and were accessible through the The Onion Router (Tor) proxy browser. Some were involved in selling drugs, arms, stolen credit cards, and even the services of contract killers. The investigation, according to law enforcement sources consulted by *IHS Jane's*, involved various approaches and techniques, some of which employed the discipline of social and behavioural science.

In conjunction with traditional policing responses, governments and law enforcement agencies have started to explore other ways to tackle organised crime. The use of theories, models, and methodology from social and behavioural science helps law enforcement authorities to better understand organised crime and to design appropriate responses.

States need to operate against organised crime at different levels and from different angles. Institutional reactions to serious and organised crime – such as drug trafficking, human trafficking, counterfeiting, fraud, and arms trafficking – often function primarily through policing and prosecution. However, policies that focus on reactive responses and that only counter organised crime through criminal justice channels risk missing opportunities to prevent criminal threats.

Social and behavioural science deals with relationships, interactions, communications, networks, associations, and relational strategies or dynamics between individuals or networks. It involves studies of sociology, criminology, psychology, anthropology, communication, and economics. Its use in relation to crime prevention and disruption has led to analytical benefits that are rooted in reality, rather than abstract models, in areas such as youth delinquency, street crimes, and public order, and the treatment of victims.

In these cases, the use of social and behavioural science has allowed law enforcement officers to focus on crime in relation to society. The results have been research analyses by academics working in conjunction with governments on how involvement in crime is affected by urbanisation, schooling and housing systems, employability, peer pressures, and family dynamics. All these research areas have a common denominator in that they aim to find techniques to anticipate and predict individual and group behaviour to reduce opportunities for criminal activities.

When dealing with organised crime, law enforcement prevention techniques have tended to focus on the reasons for victimisation, the factors that increase risks for victims and opportunities for criminals, and ways to reduce harm arising from crime. However, social and behavioural science can stretch such research to prevent and disrupt organised crime.

More specifically, this type of approach can help prevent, disrupt, and reduce organised crime by focusing mainly on communication techniques between law enforcement and criminals to influence criminal behaviour, predict scenarios, and detect truthfulness or deception by victims and perpetrators. Such strategies can also be used to study the motivation of offenders and their roles within criminal groups; this could challenge the assumption of rationalising organised crime as a profit-oriented set of activities.

Using social and behavioural science

In 2011, the United Kingdom Home Office

published a paper on the ways social and behavioural science could be used in the UK's national anti-terrorism strategy. According to the Home Office paper *Countering the terrorist threat: Social and Behavioural Science. How academia and industry can play their part*, "Application of social and behavioural sciences can improve our understanding of terrorism and its consequences. Social and behavioural science can directly inform strategy, policy and operations and help ensure that the Government's response is robust and effective."

Similarly, in the field of organised crime policy and policing, the Behavioural Science Unit at the UK's National Crime Agency (NCA) implements policies for what it calls 'Influence Activity and Remote Assessment', to support intelligence and work in the rest of the agency. Through such policies, the NCA can strengthen its capability to attribute particular characteristics to suspects; detect how many individuals are (or should be) involved in investigations; and identify the best way to understand, predict, and influence suspects' intentions.

In the fight against online organised crime or organised cyber-criminality, the National Cyber Crime Unit at the NCA and the European Cyber Crime Centre (EC3) at Europol have identified the need to develop their ability to gain trust and show credibility as operators in cyber-space so they can understand, infiltrate, and disrupt criminal networks online. This can involve setting up 'honey traps' and approaching criminals online from within their own networks.

Social and behavioural science also feature in the general methodology that Europol designed for its Serious Organised Crime Threat Assessment (SOCTA), and refers to 'crime-relevant factors' – such as geographical locations, the behaviour of criminals, and the behaviour of victims – to identify vulnerabilities influencing the success of organised crime.

Measuring the impact of social and behavioural science as a tool for supporting disruption and prevention tactics is a challenge. The Behavioural Insight Team in the UK Cabinet Office supports evidence-based trials of approaches using behavioural sciences to design policies to improve and influence behaviour in certain contexts. A 'test, learn, adapt' approach to apply and measure the effects of social and behavioural science in policy-making, and therefore to also generate innovations in policing approaches, is used by a growing number of institutions, such as Europol in its *Internet Organised Crime Threat Assessment* (*iOCTA*), published in September 2014. Such innovations include the use of 'randomised control trials' that allow the comparison of new policies with what would have happened if nothing had been changed.

A member of the Europol Cyber Crime Centre in a lab in The Hague, Netherlands, during a media tour in January 2013. The centre employs categories of cyber-psychology relevant to organised crime.

PA: 1535245

Tackling crime online

Developments in technology affect the work of law enforcement agencies in many ways, for example by changing the nature of criminal markets, both for conventional crimes (such as the sale of illegal drugs) and new types of crime. The growth of communication techniques that foster anonymity online (such as encryption) and increase the speed of information exchange also widen the gap between law enforcement agencies and criminal markets.

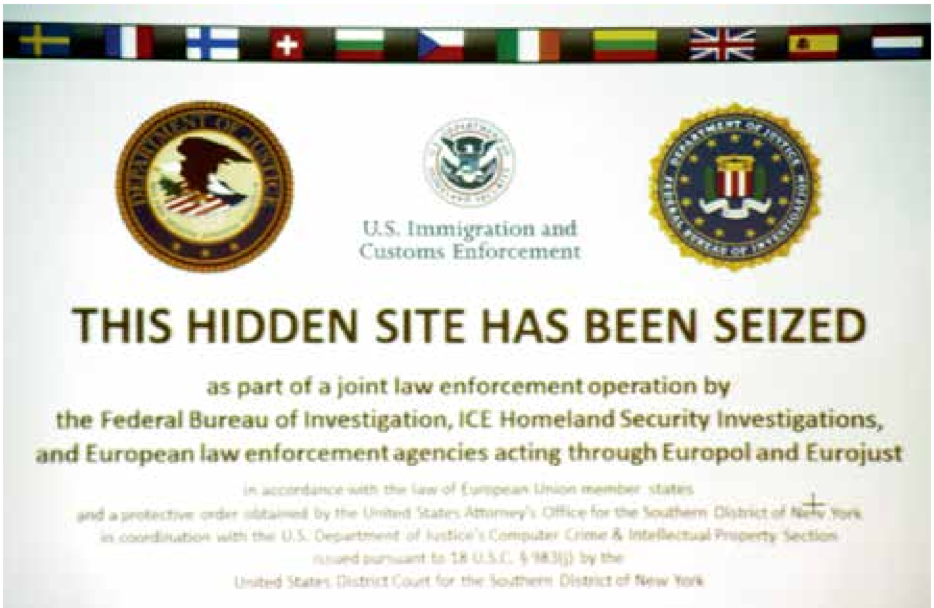
Social and behavioural science allows law enforcement agencies to target behaviour rather than struggling to keep pace with technological advances exploited by criminals. This has three advantages. First, it helps law enforcement officers to better understand the criminal world; second, it costs less than investing in more advanced technology; and third, the knowledge gathered can help to change the way law enforcement agencies can intervene on a medium- or long-term basis that partially defeats the short-term character of technology advancements.

By targeting behaviour through penetrating communication techniques and networks, law enforcement agencies can improve their knowledge of organised crime online. Such a strategy enables them to investigate how criminal recruitment works online; how criminal networks are maintained and constructed; how those networks succeed and fail; how sub-groups are formed; how networks interact, either in competition or in collaboration; and whether or not it is possible to identify a leader or a leading group.

The EC3 at Europol employs categories of cyber-psychology relevant to organised crime investigations online in *iOCTA*. The categories of psychology used by the EC3 are: anonymity and self-disclosure; cyber-immersion/presence; self-presentation online; pseudo-paradoxical privacy; escalation online (the magnification of pathological behaviour in cyberspace); impulsiveness and problematic internet use; and the so-called 'dark tetrad' of personality related to sub-clinical sadism, psychopathy, narcissism, and Machiavellianism.

These concepts, which stem from psychology but can become cyber-specific, have proven particularly useful in investigations into child exploitation and abuse online. This is because sexually driven online and offline behaviour increases the ability of law enforcement officials to identify offenders and safeguard the child. Investigations can benefit from findings in classic psychological, biological, and learning theories; addiction and arousal theories; and trait theories related to habitual patterns of behaviour, thought, and emotion.

Psychological analysis of criminal networks and offenders online can be undertaken, for example, through third-generation link analysis (involving social media behavioural analysis) and networked operational activity



U.S. Immigration and Customs Enforcement

THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

PA: 1535244

A screenshot of the seizure of illegal internet retail platform Silk Road 2.0 was presented during a press conference in Germany, on 11 November 2014. An undercover HSI agent had successfully infiltrated the site's support staff as part of Operation Onymous.

(involving the analysis of encrypted and unencrypted messages to detect communication patterns and links between people). These methods are all concerned with monitoring behaviour to improve law enforcement's knowledge of criminal groups' activities online. Such an approach has been used on a number of occasions in support of more traditional policing strategies.

One notable case was Operation Rescue, led by the UK's Child Exploitation and Online Protection (CEOP) agency, with the support of EC3 and authorities from Australia, Canada, New Zealand, and the US. Law enforcement authorities dismantled a large online forum of paedophiles with more than 70,000 members who hid behind a legal forum. Police made 184 arrests worldwide during the operation, which began in 2007 and ended in 2011. By early December 2014, this operation had resulted in at least 33 convictions in the UK alone.

In this case, the law enforcement intervention was successful because of a number of mistakes the offenders made in their attempts to disguise their identity using anonymising software such as Tor and other proxies. Three detectives then pretended to be members of the forum to identify those who posed the greatest risk to children. By working on their credentials as participants in the forum, the detectives posed as administrators. This allowed them to identify those who were interacting on the forum, using cyber-psychological concepts and approaches such as information collation, network analysis, and communication to influence behaviour.

Law enforcement officers also work against offenders who meet children on social media platforms and persuade them to send indecent images of themselves or force them to engage in sexual acts in front of webcams. After a first contact and once the children have complied with these illegal requests, the offender may threaten to disseminate the pictures to friends and family unless their demands are met. Even though offenders often hide their identity behind Tor or proxies, they sometimes make a number of errors that investigators are able to use to their advantage, using technology. Investigations also rely on profiling of offenders and understanding their behaviour online through the analysis of messages and data traffic they have generated online.

Social network analysis has also shown potential for targeting organised crime groups online, as well as offline. This analysis uses a sophisticated set of arithmetical techniques to convert large quantities of data into an image that reveals patterns in communication and connections that were not previously apparent. Following advances in technology, network mapping through social network analysis has undergone first-generation (manual), second-generation (graphics-based), and third-generation (identification-based) approaches. An approach within social network analysis known as 'blockmodelling' is designed to validate theories on social structures and may reveal interactions between groups and the structures of criminal networks by determining the existence or non-existence of associative bonds.

Third-generation analysis works towards preventing and disrupting crime through identifying a network involved in one or more criminal activities, and then identifying the chain structures (connections among groups or individuals) that become apparent through clustering (the aggregation of groups according to their connections) and blockmodelling. Sub-groups and their leaders are then identified, as well as relationships between groups; the central leaders and members of the groups are identified by degree, interaction, and closeness.

Operation Onymous, the investigation targeting illegal sales on the 'dark net', involved various approaches, some of which employed social and behavioural science and the use of social network analysis. For example, through social engineering techniques, an undercover HSI agent successfully infiltrated the support staff of Silk Road 2.0 and managed to gain their trust. The agent was granted access to private areas where he could have direct interactions with the website owner, while paying attention to potential mistakes by users that could lead to evidence of criminal activity. The operation is ongoing.

Similarly, use of traffic analysis to de-anonymise the Tor network seems to have been fundamental for the success of the operation, which has benefited from social network analysis approaches.

Offline behaviour

In human trafficking cases, prevention and disruption techniques aim to reduce the impact of the crime by focusing on the behaviour of both the offenders and the victims.

In terms of prosecution, witnesses to trafficking or modern-day slavery represent a source of information about the mindset of offenders, their motivations, and the way the market works. In terms of prevention, it is necessary to understand the mental status of vulnerable targets in order to prevent others in similar conditions from becoming victims. Similarly, it is vital to ensure the truthfulness of victim statements and detect whether they might be lying for this strategy to be effective.

Communication techniques to predict behaviour and gain trust can improve the outcome of any discussion with vulnerable victims. Cultural factors can affect the way victims are approached and the way their behaviour can be categorised and dealt with, such as in those cases where the lines are blurred and victims themselves become perpetrators. For example, former prostitutes may be used to entice new recruits into networks.

According to the United Nations Office on Drugs and Crime (UNODC), in its *Anti-Human Trafficking Manual for Criminal Justice Practitioners* (2009) publication, “Victims are obviously a very significant source of evidence but if their basic needs are not taken care of, they are a source that may quickly disappear. Thus treating a trafficked victim purely as a source of evidence is a short-term approach likely to fail.”

The needs of victims have to be addressed through specific communication techniques, including using different languages, at every stage, especially in interviewing, and before or during trial. An informed psychological approach to victims during investigation and trial is also helpful for building knowledge about the phenomenon, and will support law enforcement agents in identifying victims and offenders during routine police activities.

As noted by the UNODC, “In a number of jurisdictions it has been found that traffickers do not necessarily change their methods, locations or transport used because of routine law enforcement activity (or what appears to be routine activity), even where that activity leads to arrests.”

With the support of behavioural scientists, the NCA secured evidence to track down offenders as part of Operation Visionary, which concluded in July 2014 with three Nigerians being convicted in London for their roles in the trafficking of a 23-year-old woman from Nigeria to the UK. The woman had been befriended, raped, trafficked, and threatened with black magic. The three men targeted women who were either orphans or who had particular financial or educational needs.

Specialist teams at the NCA ensured that the victim was handled by officers who were aware of the cultural issues involved, especially with regards to the role of black magic. Officers needed to orient interviewing techniques and preparation for trial through anthropological knowledge specific to the victim’s geographical origin, both to understand the factors making her vulnerable and to use the knowledge of this case in other cases.

In cases such as those of human trafficking, social and behavioural science can push the boundaries of analysis by explicitly investigating the logic behind trafficking both from the point of view of victims and offenders, and by offering orientation in cultural and social contexts. Rather than investigating single cases of human trafficking, prevention aims to address a number of issues: the market factors that facilitate trafficking, including the behaviour of traffickers and victims; the countries of origin, transit, and destination; the timeframes of trafficking in relation to seasons and trends in communities; supply and demand mechanisms; and understanding how the recruitment of offenders and transport of victims actually works.

In order to do this, the support from social and behavioural science is invaluable. An activity model of a human trafficking network can provide a risk assessment and generate new connections between existing variables, such as geographical locations, levels of demand and supply for services, the ability of groups to work across borders, typologies of victims, and law enforcement responses. As a qualitative tool, conceptual mapping is useful to a skilled analyst when approaching problems based on the behaviour of victims and offenders, such as in the case of human trafficking, which is dependent on social and economic conditions, as well as changes within criminal markets. Concept mapping is used by the NCA Behavioural Science Unit, for example, to explore illegal markets, formulate risk assessments, identify knowledge gaps, and to elaborate disruptive approaches.

Conclusion

Applying behavioural and social science can help the fight against organised crime. Intelligence data can be improved through horizon scanning and examining crime trends, using social and behavioural methods of analysis to assess information differently and predict future and current criminal trends.

Social and behavioural science can also be used to understand capability, vulnerability, and crime indicators in organised crime groups, using analysis of advances in technology, and even the analysis of geopolitical issues that might affect drug-trafficking routes or increase the chances for human trafficking, such as changes in government. An understanding of offenders’ motivation and how criminal groups function can be refined using social network analysis, improved interviewing skills with convicted organised criminals, and organisational studies in economics. This information can help law enforcement understand the way groups handle competition, manage niche markets, and track the emergence or disappearance of markets.

Subsequently, social and behavioural science can be used to develop effective strategies for crime disruption and prevention, and identify and deal with different types of criminal behaviour. It is particularly useful in detecting deception and evaluating truthfulness during interviews or contacts with offenders, suspects, and victims. This will lead to improvements in community safety and approaches to victims of organised crime. It is particularly useful in crimes such as child abuse or human trafficking, where anthropology and psychology can improve contact with victims by considering the cultural factors that might hinder or facilitate contact with the authorities.

Finally, the use of social and behavioural science will also facilitate alternative approaches to fighting criminal exploitation of technology, cyber-crime, and cyber-enabled crime. This can be done through applying network analysis and cultural studies to online group dynamics, or through the use of communication strategies aimed at gaining trust and establishing an online reputation. ■

This article was first published online at ***ihs.com/janes*** *on 8 December 2014.*

On the web

- Crime stoppers – UK overhauls organised crime policing
- Human trafficking finds its way onto the internet

Author
Dr Anna Sergi is a lecturer in policing and crime science at the University of West London.

ihs.com/janes