NEC

Future of Forensic Science

necsws.com

Introduction

In many criminal cases forensic science evidence is pivotal. The delivery of justice depends on the integrity and accuracy of that evidence, and the trust that society has in it.

Forensic science applies scientific methods to the recovery, analysis and interpretation of relevant materials and data in criminal investigations and court proceedings. It is both an intelligence and evidential tool to assist in the delivery of justice.

Forensic science is traditionally viewed as a collection of different sub-domains with shared overarching principles, processes, and activities. Within the different sub-domains there is a range of different primary aims, and variability in terms of the scientific underpinning and robustness of the methods employed.

Professor Peter Sommer, Professor of Digital Forensics at Birmingham City University, summarised the different categories of forensic science activity:

- 'Trace' or 'wet' forensics: where a laboratory carries out one of a series of standard tests to identify or match some material found at a scene of crime or associated with an individual
- Interpretation: where the result of the examination of the trace is ambiguous but nevertheless some sort of inference or conclusion is desired. "Interpretation" may mean assigning a statistical probability of likelihood, but it can also involve providing a contextual explanation or hypothesis about events
- Reconstruction of events: where large numbers of different "traces" plus observations and testimonial evidence are combined by a skilled investigator who produces a reconstruction of a sequence of events. Examples include road traffic accidents, murder scenes, the use of mobile phone geolocation data to plot the movements of its owner over time, and the examination of a computer or smart phone to show planning and a course of action related to a crime
- Opinion evidence: where an expert has looked at a range of circumstances and offers opinion on the basis of skill, training and experience
- Forensic science sits at the nexus of science, law, policy and investigation. It should be viewed as a process that encompasses the crime scene through to court.

Background

The rise of digital technology is transforming the ways in which people commit crime; technology has created new opportunities to commit long established forms of crime such as child abuse and fraud. It has also created the capability of wholly new types of criminal activity such as cybercrime e.g. phishing, malware, ransomware and identity theft. Furthermore, the omnipresence of digital devices and the centrality of the internet to most people's way of life mean that almost any crime will now generate a trail of digital evidence that is relevant to the work of the criminal justice system.

Prior to 2012, the leader in the provision of forensic science in the UK was the Forensic Science Service, a government agency funded by the Home Office. Following its abolition in 2012, police forces have commissioned forensics from the private sector or provided them in-house. The private sector predominates in some areas of forensics such as toxicology, whereas the police tend to provide other services such as digital forensics and fingerprint examination in-house.

The National Police Chiefs' Council (NPCC) established the Transforming Forensics Programme in 2018 with £30 million funding from the Police Transformation Fund. The Programme aims to develop a more strategic approach to forensics across policing, facilitating collaboration across police forces, tackling operational fragmentation, improving compliance with standards, and improving capability in areas of rapidly changing technology such as digital forensics and DNA. The Transforming Forensics Programme has led to the development and launch of the Forensic Capability Network, a network of police forces that will work collaboratively on a national basis to strengthen their forensic capability.

In July 2020, the NPCC published its Digital Forensic Science Strategy. This included measures intended to improve the coordination of forensic services across police forces.

The forensic science regulator confirmed in her 2019 annual report that the forensic capability network had been delivering support to police forces since its establishment. She also noted the network had been attempting to address instability in the commercial market for forensic science services. However, she said more needed to be done to stabilise the procurement and provision of forensic science services by police forces.

Digital Forensic Science Strategy

The data from victims, witnesses and suspects – the data for digital forensics – is from non-police sources and is about 20 times the volume of all other police data combined, and demands additional consideration around how it is captured, used and stored.

The Digital Forensic Science Strategy has been formulated to sit alongside the National Policing Digital Strategy, produced by the NPCC and APCC published in January 2020.

Key to the strategy is the industrialised, consistent and standardised approach to the use of technology, but the strategy also sets out a new approach to recruiting and retaining a workforce that will enable digital forensics to keep up with the constantly evolving digital landscape. It also highlights how more flexible and new commercial approaches can be used to get the best from partners and suppliers to create a forensics marketplace that is able to respond to fast-changing digital forensic science requirements. Importantly, the strategy also provides a path to restoring and maintaining public confidence in the way policing uses digital evidence, reassuring victims and witnesses that they will not be subject to unnecessary intrusion in the course of an investigation.

The Rising Tide of Digital Crime and Digital Evidence

If cyber criminals continue operating at their current rate, then, by 2025, research indicates that global cybercrime costs will reach $10.5 trillion.

There are a few factors at play driving the exponential rise of online criminal activity:

- Digital progress works both ways: Just as businesses and consumers have embraced technological innovation, so too have cyber criminals. More sophisticated attacks have arisen, including using artificial intelligence for email compromise and ransomware attacks
- The coronavirus pandemic: In the last year, cyber criminals have taken advantage of coronavirus anxiety levels. The Council of Europe reported a rise in phishing scams, where cyber criminals impersonated official health bodies in a bid to steal sensitive data, as well as an increase in ransomware attacks targeting medical organisations. Further research shows that phishing attacks increased more than 660% from 2019
- Remote and hybrid working: The pandemic has accelerated the shift towards remote working and, with it, a rise in new cyber threats. The increased security dynamic, employee mistakes and weak authentication practices are all factors that cyber criminals have been able to exploit when looking to breach an organisation. On top of this, the UK Government's Cyber Security Breaches Survey 2021 found that just 23% of businesses have cyber security policies in place to cover remote working, underscoring the vulnerability of many home working environments
- Lack of digital security awareness: There's a reason why phishing scams remain such a popular technique for cyber criminals: they rely on human error. A lack of knowledge and carelessness are often the difference between a successful or prevented cyber-attack. Human error caused 90% of cyber data breaches in 2019, according to a CybSafe analysis of data from the UK Information Commissioner's Office ("ICO")
- The digital supply chain: The increasing digital interconnection of organisations throughout supply chains means that third party suppliers can enable a cascade of breaches, whereby a hacker gains access to one organisation, and then moves from there to client and supplier systems. 2021 research indicated that 82% of UK organisations, who had experienced a cybersecurity breach, stated that the breach originated from vulnerabilities in their vendor ecosystem.

The ability to gather and analyse different types of evidence is one of the most important competencies for anyone who conducts investigations. There are many types of evidence that help the investigator make decisions during a case, even if they aren't direct proof of an event or claim.

Digital evidence can be any sort of digital file from an electronic source. This includes email, text messages, instant messages, social media posts, files and documents extracted from hard drives, electronic financial transactions, audio files, video files. Digital evidence can be found on any server or device that stores data, including some lesser-known sources such as home video game consoles, GPS sport watches and internet-enabled devices used in home automation. Digital evidence is often found through internet searches using open source intelligence.

Collecting digital evidence requires a skillset not always needed for physical evidence. There are many methods for extracting digital evidence from different devices and these methods, as well as the devices on which evidence is stored, change rapidly. Investigators need to either develop specific technical expertise or rely on experts to do the extraction for them.

Preserving digital evidence is also challenging because, unlike physical evidence, it can be altered or deleted remotely. Investigators need to be able to authenticate the evidence, and also provide documentation to prove its integrity.

Challenges

The Transforming Forensics Programme research identified three 'core challenges' that digital forensic science faces:

Volume

Driven by the number of devices, better communications and increased cloud storage, demand has been rising by 11-16% over the last few years, and we expect this to continue. The result? Backlogs and delays to investigations. These delays and backlogs impact victims, witnesses and suspects waiting for the outcome of investigations and often for the return of their devices.

Complexity

Digital examinations themselves present a complex challenge. There are more types of devices, more end-to-end encryption, more varieties of data format, and more data stored in the cloud. The 'Internet of Things' is growing rapidly – so we need to develop new techniques simply to maintain DF capability to extract and analyse information, to avoid cutting off the criminal justice system from critical sources of evidence.

Legitimacy

Although broadly supportive of police using digital forensic analysis, recent issues around disclosure and consent for digital device examinations mean the public are more aware and alive to the issues involved. Meeting the challenge of rising data volumes, encryption and cloud storage means policing needs to work in new ways and it is crucial to maintain public trust and confidence in doing so.

The solution

The Digital Forensic Science Strategy outlines six strategic objectives. These strategic objectives fully support and have been mapped to the ambitions and priorities of the National Policing Digital Strategy. These strategic objectives are outlined below:

1. Increase the digital forensics capability and capacity in order to improve investigative outcomes, reduce crime and increase public safety
2. Develop a sustainable Digital Forensics Science workforce that is equipped with quality-assured tools and has the skills, abilities and experience to take advantage of advances in technology in order to deliver justice
3. Develop a vibrant community with partners to focus on the underlying science in digital forensics, ensuring that research is targeted and harnessed and plays a central role in digital forensics culture and thinking
4. Develop a whole-system approach to the delivery of digital forensics underpinned by robust science and quality standards which can respond to all requirements of the criminal justice system and law enforcement
5. Support the Government in reviewing current legislative and policy framework to ensure it enables the criminal justice system to appropriately use digital forensics and big data to deliver the best judicial outcomes and increase public trust
6. Develop strong partnerships with private sector providers of technology and services to create a healthy and sustainable marketplace that is able to respond to fast-changing digital forensic science requirements.

This strategy acknowledges that incremental improvements will not achieve the vision, which calls for a much more radical transformational attitude and the delivery of a nationally networked, integrated approach if forensics are to keep pace with a rapidly changing technological landscape. The approach is described through five interconnected themes, all of which play a key part in delivering the strategic objectives

1. **Improving operations** - The newly established Forensic Capability Network (FCN), formally launched in April 2020, is key to improving operations, providing central support services on a national basis. The FCN is a community of its members forensic science capabilities and expertise, comprised of a network of forensic science professionals across UK policing, a core team to co-ordinate and orchestrate forensic service delivery, and a technology platform and toolset to connect and enhance forces' existing forensic capabilities
2. **Improving commercial practices and R&D** - The recent House of Lords Science and Technology Committee inquiry into forensic science in the UK highlighted that policing could not solve the problems or deal with the structural challenges that affect digital forensics service delivery in isolation, but needed to act in partnership. Private sector providers are essential to delivering digital forensic service and key to a nationally networked approach. So too are other organisations – including higher education institutions, specialist research organisations, start-ups and existing digital forensic tool vendors - which can support innovation in the future
3. **Meeting the data challenge** - A structured data model for storage of digital forensic data will provide a foundation to develop more advanced tools, enabling investigators to extract meaning from the raw data ingested, searching for entities and attributes rather than being limited by keywords or previously known identifiers. This will enable a single overview of ingested data, regardless of its source, allowing an investigator to search in real-time across indexed data from all evidence items in a case. Integration of analytic capability will provide meaningful information insights and build up a rapid intelligence picture to speed up investigations
4. **Developing the Workforce** - Recruit and retain a skilled workforce who are motivated, fully trained, well managed and equipped with access to the right tools and processes to deliver a world-class digital forensic service to the criminal justice system. FCN Science, in partnership with the College of Policing (CoP), seeks to professionalise digital forensic science roles, improving career opportunities and ensuring a culture of continuous learning supported by a national competency framework, training and a workforce recruitment and retention plan
5. **Building Trust** - From crime to court there will be improvements to quality standards, effectiveness and efficiency by:
    - Providing tools and methods that are robust and assessed for accuracy for quality assurance
    - Following the 'validate once verify many' methodology for a more efficient and achievable approach to validation
    - Enabling a national network to share learning, knowledge and experience
    - Delivering a single online quality management system, accessible at point of need
    - Building a standard approach to accreditation.

These steps will provide the public, the courts, practitioners and investigators with the trust, confidence and assurance that independent assessment to external quality standards brings.

Regulation

The Home Secretary appointed Gary Pugh OBE as the new Forensic Science Regulator in May 2021 for a period of three years.

The Regulator ensures that the provision of forensic science services across the Criminal Justice System complies with an appropriately high standard of scientific quality and is carried out with objectivity and impartiality.

Responsibilities of the Forensic Science Regulator include:

- Establishing, and monitoring compliance with quality standards in the provision of forensic science services to the police service and the wider Criminal Justice System (CJS)
- Ensuring, where applicable, the accreditation of those supplying forensic science services to the police, including in-house police services and forensic suppliers to the wider CJS
- Setting and monitoring compliance with quality standards applying to national forensic science intelligence databases
- Providing advice to Ministers, CJS organisations, suppliers and others as seems appropriate, on matters related to quality standards in forensic science
- Dealing with complaints from stakeholders and members of the public in relation to quality standards in the provision of forensic science services.

The new Forensic Science Regulator Act 2021, enacted in parliament in April 2021, is intended to provide the Regulator with statutory powers in England and Wales.

The act:

- Places a duty on the Regulator to publish a 'code of practice' for "forensic science activities". The act defines "forensic science activities" as forensics within the criminal justice system but would give the Secretary of State delegated powers to expand the definition in the future.
- Empowers the Regulator to enforce forensic science standards. It gives the Regulator powers to investigate forensic science providers when it suspects they are putting the criminal justice system at "substantial risk". The Regulator is able to issue "compliance notices" to these providers requiring them to take specified steps and would be able to temporally shut facilities until they meet the terms of their compliance notice.

Conclusion

Technology is an essential part of digital forensic science and will be an essential component in its transformation. But it will take more than technology alone to deliver a rapid, quality-assured digital forensic service nationally. To do this, policing and stakeholders must come together on common ways of working. According to the authors of the Digital Forensic Science Strategy, a cultural shift in practice, supported by strong governance, is needed if we are to build up this national response to support digital forensic science to deliver an effective and efficient service.

The scale of change needed across digital forensic science means that full transformation will take time. It is proposed that a 'twin track' approach, combining transforming forensics activities which support the longer-term change with 'quick wins' delivering rapid operational benefit for digital forensic units and policing. Everyone involved will need to collaborate closely with partners to ensure measurable improvements in service and rapid benefits to the criminal justice system are delivered, at the same time ensuring that all activity supports and contributes to the longer-term transformation of digital forensic science.

Get in touch:

Visit our website:
necsws.com

Email us at:
hello@necsws.com

Connect with us
on social media

Sources:

House of Lords - Forensic science and the criminal justice system

Forensic science and the criminal justice system: a blueprint for change

Codes of Practice and Conduct For Forensic Science Providers and Practitioners in the Criminal Justice System

Digital Forensic Science Strategy

Unleashing the value of digital forensics

If you'd like to find out more about how we can help your organisation take advantage of the latest technology, let us know at hello@necsws.com or call us on 01442 768445

NEC

For more information visit **necsws.com**
or get in contact with us at **hello@necsws.com**