NCC Group plc – Written evidence (FRS0044)

1. About NCC Group

1.1. NCC Group plc is delighted to respond to the Science and Technology Committee’s inquiry into Forensic Science, specifically the Committee’s interest in understanding the UK government’s preparedness for the anticipated increase in the volume of digital forensic evidence.

1.2. Headquartered in Manchester, NCC Group employs more than 2,000 people across 35 offices worldwide, providing more than 15,000 organisations with research & development, penetration testing and full spectrum attack simulation services, security operations centre (SOC) and networking monitoring support; cyber defence and threat intelligence services.

1.3. NCC Group also provides cyber incident response and digital forensics services to clients worldwide. Our consultants hold qualifications from recognised bodies including EnCE\(^1\) and X-PERT\(^2\) and act in accordance with ACPO guidelines\(^3\). NCC Group has experience in a wide range of investigations including computer misuse, network forensics, live forensics and volatile memory analysis, bespoke technical analysis and portable electronic devices forensics. NCC Group is an NCSC accredited company for Cyber Incident Response.

1.4. In addition to undertaking corporate investigations, NCC Group has a proud history of working in collaboration with government, law enforcement and intelligence agencies as well as acting as experts in civil, administrative and criminal cases.

1.5. Moreover, NCC Group continues to innovate to safeguard our ability to conduct scientifically based and legally admissible forensic investigations amidst the challenges presented by rapid technological developments.

1.6. In light of our experience of undertaking digital forensic investigations, we assess the current challenges regarding the UK Government’s preparedness for the significant increase in digital forensic evidence, and set out our recommendations for the future.

2. Executive Summary

2.1. We argue that:

---

1 [https://www.x-ways.net/x-pert/](https://www.x-ways.net/x-pert/)
2.1.1. The Committee’s forward-looking work should be seen in the context of more than a decade of political attempts to address the challenges of digital forensics;

2.1.2. The increasing role of digital forensics is an incredibly challenging concept to define in light of the rapid increase in data volumes, varied nature of criminality, and technological advances, making it very difficult to assess when “enough is enough”;

2.1.3. The proliferation of embedded and cloud technologies challenge digital evidence collection; and

2.1.4. Addressing the Criminal Justice System’s significant capacity gap necessarily needs to include a review of the regulatory and legislative landscape.

2.2. We believe that:

2.2.1. Open discussion and cross-disciplinary working is required clearly to scope and define the contribution and limits of digital forensics in tackling evolving digital crimes and other activities of interest, and identifying priorities for research into workable technological solutions to provide scalability and timely analysis;

2.2.2. Any legislative review should take account of the limitations of the current patchwork of rules governing digital forensics, including in relation to the Computer Misuse Act 1990, identify new ways of strategic collaboration between public and private sector and assess the impact of forthcoming European legislation on the availability of and access to data and digital evidence.

3. Introductory Remarks

3.1. Digital forensics was first mentioned in the UK Parliament in 2006, referred to as “a newly emerging area”⁴. As early as 2008, questions were put to the Home Office Minister regarding the adequacy of resources for digital forensic services in England and Wales⁵. From 2011 onwards, based in part on a perceived need to communicate the scientific and technical basis of digital forensics, the UK government has undertaken a series of reviews, strategic investment decisions and strategies to “ensure we have the digital forensics – the digital information to fight new crime types”⁶. The 2016 Forensic Science Strategy acknowledged the unique challenges created by the rapid growth and development of digital

⁴ http://www.publications.parliament.uk/pa/cm200506/cmhansrd/vo060420/halltext/60420h01.htm#60420h01_spnew21
⁵ http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080722/text/80722w0081.htm#08072427007284
⁶ http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm150323/debtext/150323-0001.htm#150323-0001.htm_spnew15
technology though concluded that digital forensics remained fundamentally similar to other forensic disciplines and should be treated as such\(^7\).

3.2. While the Forensic Science Regulator required all digital forensics practitioners undertaking criminal justice work to be accredited to ISO 17025 by 2017, its 2016/17 Annual Report\(^8\) concluded that contracts were still being awarded to digital forensics companies without sufficient due diligence regarding their accreditation, but also outlined continuing work on defining new standards for network capture and analysis, open source investigations and analysis of communications data.

3.3. Earlier this year, the House of Commons Justice Committee’s report into the disclosure of evidence in criminal cases\(^9\) reiterated that the growth in digital technology had led to an increase in the volume and complexity of material and issued calls for increased funding for frontline digital forensics, emphasising, in particular, the training requirements of digital forensics as an investigative skill.

3.4. Yet despite more than a decade of reviewing digital forensics, the UK government has not developed a comprehensive strategy to address the evolution of the discipline and the challenges it faces as a result of technological developments.

4. Comments and Recommendations

4.1. It is in this context that NCC Group addresses the Committee’s forward-looking questions regarding digital forensics:

4.2. Is enough being done to prepare for the increasing role that digital forensics will have in the future?

4.2.1. The growth and diversification of digital technology and the proliferation of digital devices alongside the rapid growth in the volume of data stored on digital devices significantly increases the complexity of digital evidence which requires forensic analysis. Triage mechanisms and machine analysis solutions have been put in place to address backlogs and delays but further work is required to develop sustainable technological and processual solutions as the increase in data volume shows no sign of abating.

4.2.2. Cross-disciplinary collaboration covering computer science, big data analytics and machine learning and artificial intelligence should inform


\(^9\) [https://publications.parliament.uk/pa/cm201719/cmselect/cmjust/859/859.pdf](https://publications.parliament.uk/pa/cm201719/cmselect/cmjust/859/859.pdf)
strategic responses to improving the data analysis and investigation capabilities of digital forensic investigations.

4.2.3. The scope and relevance of digital forensics is constantly changing, making it difficult clearly to define the exact role the discipline will play in investigations, criminal justice proceedings and strategic operations. Political debate of digital forensics over the last 24 months illustrates the challenge, highlighting the near constantly changing context in which the role and contribution of the discipline is considered. The 2016 Forensic Science Strategy acknowledged that the growth of digital enabled new types of crime as well as traditional crimes to be committed in ways that leave digital and physical trails. In the debates around the Policing and Crime Bill in 2016, digital forensics were increasingly mentioned in relation to tackling child sexual abuse images on the Internet; in 2018, digital forensics have been given a role in fighting online manipulation and misinformation; Viscount Waverly, for example, has suggested devising “support programmes of fact checking, verification and digital forensic initiatives capable of exposing falsehoods and false claims of authority that underpin fake and propaganda pieces”\(^\text{10}\).

4.2.4. Open discussion is required clearly to define the capabilities and limits of digital forensics acknowledging that its remit might expand but equally resisting the temptation to consider the discipline a panacea to tackling newly emerging threats as they develop. This includes discussion on where digital forensics, such as the collection and distillation from raw data, stops, where investigation and analysis in the context of wider investigative activities begins, and what products and outputs digital forensics is required to produce.

4.2.5. The fluid nature of these developments makes it very challenging both to define clearly the increasing role of digital forensics, much less assess if it is being prepared for adequately. Moreover, they are compounded by technological developments across three areas:

4.2.5.1. Advances in data storage technologies, including DNA, silicon and carbon-based methods, presenting challenges in the future in accessing digital evidence and data using legacy techniques;

4.2.5.2. The proliferation of embedded technologies challenging the adequacy of practitioners’ tooling; and

4.2.5.3. The rise of the ‘black box’, often requiring substantial research & development investment into reverse engineering in order to be able to collect and interpret data.

4.3. Are there gaps in the current evidence base for digital evidence detection, recovery, integrity, storage and interpretation?

\(^\text{10}\) [https://www.theyworkforyou.com/lords/?id=2018-01-11a.393.0](https://www.theyworkforyou.com/lords/?id=2018-01-11a.393.0)
4.3.1. NCC Group believes that there are some significant evidence gaps arising due to data being held on various platforms, including embedded systems in cars, buildings and wider Internet of Things devices.

4.3.2. Despite efforts by Europol to encourage the adoption of a standard digital forensic format\textsuperscript{11}, heterogeneity across technologies and platforms, and a lack of standard interfaces persists.

4.3.3. In addition, we share concerns that the increasing popularity of cloud computing and cloud storage presents challenges for digital forensic investigations in terms of accessing materials, not least where cloud servers are based outside the domestic jurisdiction.

4.4. Does the Criminal Justice System have the capacity to deal with the increased evidence load that digital forensics generates?

4.4.1. NCC Group is clear that the Criminal Justice System currently lacks capacity to deal with digital forensics, in every sense and at every level. We note the Justice Committee’s recommendation for the Home Office to produce, by the end of the year, a comprehensive strategy to ensure police forces are equipped to handle the increasing volume and complexity of digital evidence, taking into account the required investment in skills and technology.

4.4.2. We believe that one way to address the capacity gap will be for law enforcement and private sector providers to collaborate much more closely than the current outsourced supplier model allows; though this will still require investment and financial resources for private sector partners to be remunerated adequately. For this to be feasible, we believe that commercial viability will need to be considered on the supply side to ensure appropriate investment and skills development.

4.4.3. Finally, NCC Group strongly believe that a comprehensive strategy to address the increasing role of digital forensics cannot be successfully undertaken without a meaningful review of the associated legal and regulatory framework. Digital forensics has evolved significantly over the past decade, and while efforts have been made to amend and reform pieces of legislation governing the discipline, the current patchwork of rules and regulations that applies is not necessarily conducive to the future development of the discipline and its practitioners. We believe that a review of the current regulatory landscape should consider:

4.4.3.1. The continued adequacy of the Computer Misuse Act 1990 in light of the increasing importance of digital investigations in the attribution of cyber crimes and its victims. Elements of cyber incident and threat intelligence research can form part of digital forensic investigations. A greater reliance on collaborating with

\textsuperscript{11} \url{https://www.europol.europa.eu/newsroom/news/eu-forensic-experts-call-for-action-new-cyber-investigation-standard}
the private sector, partially to address skills and capabilities challenges, requires an enabling legal framework that does not limit private sector investigative efforts by inadvertently criminalising them;

4.4.3.2. Options to introduce a new private investigator status for accredited digital forensics providers, allowing them to work in closer partnership and collaboration with public agencies beyond the current supplier relationship; and

4.4.3.3. The impact of the European data protection regime, including the General Data Protection Regulation, and the ePrivacy Directive to ensure continued balance between privacy rights and access to data and digital evidence, particularly in the context of the UK’s departure from the European Union.

5. Conclusion

5.1. NCC Group has sought to provide the Science and Technology Committee with considered evidence and recommendations on the basis of its operational and investigative experience in digital forensics and cyber incident investigations.

5.2. We would be delighted to provide oral evidence to the Committee to help elaborate on any of the arguments raised in our written submission and look forward to receiving the Committee’s final recommendations to the UK government in due course.

14 September 2018