Public Understanding of Cyber Security and Digital Forensics within the UK

Georgina Humphries[1] and Joseph Williams[2]

[1]Computing, Digital Forensics and Cybersecurity, Canterbury Christ Church University, Canterbury, United Kingdom
e-mail: georgina.humphries@canterbury.ac.uk
[2]Cyber Security Centre, School of Engineering and Computer Science, University of Hertfordshire, Hatfield, United Kingdom
e-mail: j.williams30@herts.ac.uk

Abstract

Little narrative exists within the literature which focuses on the understanding of cyber security and digital forensics to a much wider audience: the public. This paper's aim is to capture and examine the perceptions of the public by adding insight into what is understood by the terms and disciplines of 'digital forensics' and 'cyber security'. While cyber security and digital forensics can be recognised by their interdisciplinary nature, the two disciplines are distinct in their approach to criminality. At its simplest, cyber security is concerned with the prevention of an incident and implementation of robust systems, while digital forensics focuses on the response to crime and recovering digital evidence. Public perceptions of these areas are important, as security of systems and digital technologies have been heightened in recent years due to high profile cases where notable and large corporations have seen breaches of sensitive information. This study draws on responses from the public using an online survey taken by 102 participants that asked their views on cyber security and digital forensics. This paper demonstrates that there is an awareness among respondents of both disciplines where participants have associated cyber security predominately with the protection of data and systems and digital forensics as the examination and inspection of digital devices. Additionally, responses have also shown there is a need for further awareness in these fields.

Keywords

Cyber Security, Digital Forensics, Public Understanding, Human Factors

1. Introduction

As data volumes rise there are growing concerns for prevention and detection of criminal actions. With the growth of online and digital criminality, human factors such as knowledge, attitudes and behaviours all play a key role in ensuring security. Where security measures are insufficient, risks are intensified, and criminality is examined by both cyber security and digital forensic practitioners at different stages within the criminal timeline.

Often discussed are the human factors which relate to passwords for ensuring security. The UK Cyber Security Strategy published by the Cabinet Office (2016, p. 22)

highlights awareness surrounding "poor cyber hygiene and compliance" has increased in the last few years; predominately due to high profile incidents. Aytes and Conolly (2003), Aytes and Connolly (2004) and Parsons *et al.* (2017) highlight tendencies in Information Security and how awareness and education is just one branch in the model for understanding end users' efforts toward computer security. Parsons *et al.* (2017) also note how human influence on computer and Internet security including behaviours which effect password validity and security can, and will, be exploited. Last Pass (2018, p. 6), a password management company, reported "91% [of participants] know that using the same passwords for multiple accounts is a security risk, yet 59% mostly or always use the same password". While the potential bias of this report can be questioned, a trait of behaviours linking to ignorance and neglect as well as the challenges of creating unique and strong passwords time after time are often exposed. Authors such as Merdenyan and Petrie (2018) report that news of a breach does not often entice an end user to change their password or behaviour.

Existing literature which focuses on the narrative views and understanding of both digital forensics and cyber security from a widespread audience (i.e., the public) is limited. Schatz, Bashroush and Wall (2017) discuss how similarities among terminology such as Computer Security and IT Security for the wider audience can reduce clarity in their meaning; but recognises that professionals understand differences of the two. The same can be said of cyber security and digital forensics, where similarities and dependencies of both can be identified, along with the main difference between the two being their application within the timeline of a crime. Simply put, cyber security is the prevention of an incident, where systems and security techniques be it physical or people-driven are implemented to defend against an attack. Furthermore, digital forensics is conducted in the response to criminal incidents where digital devices are examined to collect, recover and analyse any digital artifacts which can shed light on what role digital technologies played through to what data was compromised in the crime.

The definitions and positions of professionals within these fields exist with many similarities yet substantial differences. Some describe the two disciplines "as two essential sides of the same coin" (Krakoff, no date). Though the two are not one and the same, they are dependent upon one another for success in preventing and investigating online and digital crime. Table 1 below highlights, but is not restricted to, some of the similarities and differences of the two fields in their simplest form; while recognising there are numerous definitions and methodologies adopted within both disciplines across jurisdictions. A common similarity of the two is the essential ingredient to "increase the coordination between [both fields as well as government and corporations] … to best track and convict cyber criminals" (Dlamini, Eloff and Eloff, 2009, p. 196).

The divergence on the meaning of digital forensics and cyber security as distinct disciplines are a growing debate. Individual beliefs on the disparate nature of the two range from examples such as the two disciplines being distinct, albeit related, through to others who see digital forensics as a subset of cyber security or forensic science. Much of this may be described by what authors such as Omar, Venkatesan and Amamra (2018, p. 5) have identified as interdisciplinary workings of disciplines

focusing on a range of areas for example, computing, information security, business and management, law and governance.

	Digital Forensics	**Cyber Security**
Similarities	Interdisciplinary nature: computer science, information security, engineering, mathematics, forensics, law and criminal justice, criminology, policing, business and management (Irons, Stephens and Ferguson, 2009; Ramirez, 2017)	
	Fundamental knowledge of digital infrastructure: computer systems, operating systems, networks, risk assessment and management, software engineering/computer programming (Joint Task Force on Cybersecurity Education, 2017; NCSC, 2017; Newhouse *et al.*, 2017)	
	Governance: policies procedures and principles, legislation and standards) albeit different approaches and policies followed – a strong link with accountability (Grobler and Louwrens, 2006; Grobler and Dlamini, 2010)	
	Preservation: the idea of safeguarding, be it protecting a system from threats or preserving evidence for an investigation	
	Behavioural analysis: the ability to think like a criminal and to understand how/why/what a criminal thinks and acts like (Shinder and Cross, 2008, p. 81; Vidalis, Llewellyn and Angelopoulou, 2010)	
	Competence: the technical knowhow to handle duties, data and evidence (potentially outside the remit of known practices)	
	Skills: problem-solving, critical thinking, initiative, self-direction, creativity, management, accuracy, organisation, people skills and so on	
Differences	It is the collection, preservation, acquisition and analysis of digital devices to understand a crime (Reith, Carr and Gunsch, 2002, p. 2)	It is the process of protecting and defending information systems from threats in cyberspace (Luiijf, Besseling and De Graaf, 2013)
	DF practitioners are told of a system breach or criminal activity and asked to investigate using devices, data and records	CS practitioners identify the system breach or potential crime and alert forensic examiners or incident responders
	Investigates if a crime has taken place and potentially who committed it; reactive (Alharbi, Weber-Jahnke and Traore, 2011, p. 67)	Takes place before a crime is committed or after in order to improve security; requirement to be more proactive (Rowe and Gallaher, 2006)

Table 1: Some similarities and differences of two interchangeable disciplines: digital forensics and cyber security

Where we see continuous developing technologies, increased provisions around privacy, security and consent and a heavy reliance on the Internet as well as developing smarter devices we, arguably, see a continuous need for professionals mastering in areas of cyber security and digital forensics. Moreover, although the two work in tandem, they do deliver differences which can be used as a distinction when used interchangeably to many outsiders of each field. After having identified commonalities and differences among cyber security and digital forensics and recognising how previous authors have described similarities with related disciplines often having been well known to individuals within the field, yet often lacking clarity for a wider audience, the main aims of this paper look at the public's perception of these disciplines and their views on what needs be tackled.

2. Method

An online questionnaire totalling 21 questions was developed and distributed across messaging and social media platforms to capture public participants awareness and understanding of digital forensics and cyber security. Online deployment of the questionnaire was adopted due to advantages such as, wider geographic response rates, cost effectiveness and immediate data collection. The questionnaire was designed into sections, using both open and closed questioning and providing anonymity for respondents. Questions focussed on the following: participant demographics (e.g. age, gender, education and employment); participant's digital device, Internet and password usage; experience, awareness and views on cyber security and digital forensics; and, agreement or disagreement with statements pertaining to security, privacy and crimes online. A key focus of the questionnaire aimed towards an open-ended section which looked to identify thoughts on the terms: digital forensics and cyber security. These questions were addressed in the fulfilment for identifying the importance of forensics and security to the individuals.

3. Results and Discussion

102 responses were analysed from participants that were aged 18 or over. Participants were heavily distributed across mid-range age categories, with 12 participants aged between 18 and 24, 21 aged between 25 and 30, 17 aged between 31 and 40, 33 aged between 41 and 55, and 19 aged 56 and over. Of these, approximately 57.8% were females. Demographics also show that 72 respondents (70.6%) identified as being in full-time employment with the overall highest qualification held by respondents being a Bachelor's Degree (29.4%), followed by an A-Level or equivalent (17.6%).

3.1. Use of technology, the Internet and perceived risks

To examine respondent use and familiarity of technology and their online usage, individuals were asked to identify devices utilised to access the Internet. Questions presented to participants offered several checkbox items of example devices and activities and were asked to add additional responses where relevant. This questionnaire demonstrates the usage of both computers and smartphones are equally common of this sample for a range of activities. Analysis shows the most popular

devices selected were Computers, for example, desktops and laptops (93.1%), Smartphones (92.2%), Tablets (72.5%) and Televisions (46.1%). Other appliances included other smart/Internet of Things (IoT) devices and games consoles. Participants were also asked to identify activities they conducted online. Analysis shows that the most prevalent activities were Buying Goods, followed by Emails, Social Media and General Browsing of the Internet. Further activities are depicted in Table 2.

Activity	Respondents	
	Number	Percent
Buying Goods	96	94.1
Emails	93	91.2
Social Media	91	89.2
General Browsing	89	87.3
Reading the News	88	86.3
Online Banking	85	83.3
Research	69	67.6
Watching TV	63	61.8
Watching Videos	61	59.8
Playing Games	50	49.0
Selling Goods	44	43.1

Table 2: Prevalent online activities conducted by respondents

Participants were also asked several statements responding with answers on a five-point Likert scale which looked at their use of technology, concerns with privacy and to reflect on their ability to be able to protect themselves online. Results show that 54.9% of participants strongly agree or agree that they 'like to use and tinker with technology'; on the other hand, 30.4% neither agree nor disagree with the statement. With a high proportion of people expressing neutrality, it may arguably be suggested that many of the respondents use technology as a means to an end and as an everyday object.

Results show that 86.3% of participants strongly agreed or agree about concerns for the security of their devices, with 84.3% of respondents agreeing they were concerned about their privacy. 73.6% of respondents agreed towards the avoidance of disclosing their personal information online. However, 17.6% neither agreed nor disagreed to avoiding disclosure of personal information online. Arguably, suggesting that some people may be unaware or have no weighted opinion when it comes to the availability and use of their personally identifiable information online. However, this may otherwise suggest that these respondents are aware they must inevitably disclose personal data to use some online services. Further results found that 82.3% and 59.8% of respondents agreed they were concerned that their personal information is not kept secure by websites and public authorities respectively.

92% of respondents felt they were at risk of becoming a cybercrime victim. This may suggest a high concern for the risks and vulnerabilities off and on the Internet. Lastly, respondents were asked to think about whether they agree or disagree that they were able to protect themselves sufficiently against digital crimes. Participants were given

the suggestion of, for example, anti-virus software at minimum. 54.9% agreed, while 21.6% stated they neither agree nor disagree; and 20.6% disagreed, with 2.9% stating they did not know, or they felt the statement was not applicable to them.

3.2. Use and change of passwords

Participants were asked two questions pertaining to passwords and security. These were how often they changed their password and if they have ever used insecure and common passwords (e.g., 123456; password; 123456789; qwerty; 123123; google; 111111; qwertyuiop; 1q2w3e4r). Passwords are often a weakness of many simple hacks, however, for much larger data breaches these security weaknesses are often not the target, although, identification of common passwords and those of insecure length and type, are all easy targets for criminals. Results show that 94% of participants recognised that they have not used these examples. However, social desirability bias must be considered for these responses, highlighting the chance that respondents may have been less than truthful about the use of such passwords to provide a suitably perceived 'acceptable' answer.

Of those who have used insecure passwords, three had become a victim of digital crimes. Although this study cannot provide concrete evidence to the correlation between participants usage of passwords, age or victimisation what can be said is there is still an apparent need for further education and awareness on preventative measures such as password hygiene and etiquette to reduce individual's weak password policy. One respondent of this questionnaire identifies the need for education in 'cyber', particularly referring to the use and security of passwords. They voice the concern that "education [is required], because 'cyber' is not tangible, people care less about their passwords than house keys." The results from this questionnaire support this claim, where password change schedules admitted by the 102 respondents presented 20 respondents who "Never" change their passwords. That is 19.6% of the sample. Along with those who never change their passwords, 15 respondents (14.7%) who change their passwords on a yearly basis; 16 individuals (15.7%) on a 6-monthly basis; 10 respondents (9.8%) every three months; 5 individuals (4.9%) every two months and 9 respondents (8.8%) every month. However, authors such as Merdenyan and Petrie (2018, p. 7) have shown that "self-reported responses from … participants … may [show] an effect of social desirability, especially in relation to some risky password behaviours".

Further analysis of participants in this questionnaire demonstrates a high proportion (26.5%) of people who changed their passwords infrequently. Many noting that they only change passwords when they have forgotten their latest one, feel they need to, or are requested to do so by a site or system. Example responses include: "when I feel I have to, need to, have forgotten the previous one", "when required by systems", "when asked to. I am very bad at this!", "only when hacked or if I cannot remember my password", "varies what it's for", "depending on what site/app the password is used for", and rather vague responses such as, "less frequently" (e.g. no timeframe) and "whenever…". One respondent voiced how they "don't change passwords on [their] personal devices just on the computers [they] use at work". While another stated: "work one monthly, others never". This, arguably, may be a cause for concern, where

there seems to be little transfer of learning of password security between the workplace and home. Although work place password policies are typically more stringent and enforce password changes, something a user is unlikely to be faced with using their own devices at home.

3.3. Perceptions of digital forensics and cyber security

To understand the public image and understanding of each discipline participants were asked two questions:

- What do you think of when you hear the term ‘Digital Forensics’?
- What do you think of when you hear the term 'Cyber Security'?

Analysis of the qualitative data collected for both these questions shows participants are largely aware of what each discipline entails. For example, respondents relate digital forensics to the “digital equivalent to traditional forensics, investigating the digital 'footprints' left by perpetrators of crime”, “analysis of digital and electronic devices”; “obtaining evidence of activities from (any type of) computing devices”, and “the ability to investigate and recover different materials found on different digital devices especially in relation to crimes”. Other responses covered the idea of professionals who were there to investigate whether a crime has occurred, one respondent describes these people as the “Detectives of the internet world”. Where again participants were able to identify crucial aspects of cyber security from “being secure online”; “trying to stop culprits”; “protecting digital assets from unintended access, modification or denial of their use” through to “passwords, personal details” and “OS, application and network security”. Another respondent states they think of cyber security as, “the protection of a computer system or digital device from damage or theft of its software or data and stopping any disruption of any services they may be providing.”

One respondent highlighted how they felt that digital forensics was about “tracing the culprits” while cyber security was about “trying to stop the culprits”. This is a broad view of the fields which resonated through many of the examples of thoughts when hearing each term provided by respondents. However, responses varied with examples such those depicted in Table 3. This collection of responses shows how some participants relate cyber security to the protection of data and/or devices through to advice, awareness and protocols or techniques which can be adopted in a corporate or personal setting to help minimise openness to attack. Whereas digital forensics is more commonly related to policing or cyber crime investigations; which one respondent epitomises as “tracking a trail of clues left by digital naughtiness”.

While online questionnaire distribution harvests advantages such as, cost effectiveness, time efficiency and unrestricted geographic boundaries, equally it provides potential for negatively influenced responses and reliability issues. It must be considered that while responses above show some awareness, participant deception may be possible e.g., participant use of the Internet to research and shape their understanding and thus misrepresenting their true views. Though this is plausible,

there may be deception in, and challenges to, any mechanism of questionnaire distribution.

Digital Forensics	Cyber Security
Detectives of the internet world.	Policing of the internet world
Something that the police might do to examine illegal digital activity.	Protecting yourself or your company from potential attacks.
Obtaining evidence of activities from (any type of) computing devices.	Protecting digital assets from unintended access, modification or denial of their use.
Describes the ability to analyze data left or held on a device like a digital footprint in the same way a crime scene investigator can review a crime.	A topic cover of ways to protect yourself on digital devices to avoid social engineering or hacking.
I think of cleaning up your digital footprint like clearing cookies, ensuring your passwords are strong and looking at your Digital life in forensic detail to ensure that it is secure.	Anti-Virus, robust passwords, private & secure networks.
American TV series.	The Bank.
I hope the crimes are being watched.	I think of software.
Use of an incognito browser & Hide my laptop.	My laptop isn't up to scratch.
Tracking online activity.	Online steps taken to secure information.
Makes me think of a TV crime drama like Broadchurch or The Killing - but rather than being at a murder the detective is probably in an office or home computer.	A list of help or advice to keep you safe online? A protocol?
The checking of people's personal usage of the internet/searches/social media etc.	The protection of one's personal data.
Investigating cyber crime.	Protection for data kept or used on the internet.
Police investigation to online crime…hacking, tracing online activities etc... NCIS CYBER.	As above but the protection and prevention side.
Computer police.	Internet security.
No idea.	Protecting yourself online.
Forensic science within digital services.	A body designed to secure and protect computer-based systems.
Investigating digital crime.	Security surrounding anything deemed 'online'.
Investigating cyber security and devising methods of preventing it.	Securing internet connections to prevent breaches.

A man (and it is a man) analysing an attack to find out where it came from, block it for further attack and if possible pass information on for conviction.	Prevention of attacks.
Analysing the total memory and usage of a digital device and any programs associated to it.	Virus checkers and fire walls.
Analysing data.	Firewall's passwords secure networks.

Table 3: Small set of example responses to the terms digital forensics and cyber security

The 102 responses show that only a few participants hold, perhaps, a naive image of the roles within the two disciplines. Typically seen were one-word associations, unfamiliarity or inability to define their views; where those participants relate the terms and corresponding roles/activities to their true meaning. Although there were also images portrayed by few participants such as, "American TV series", for example "NCIS" and the characters which mimic and portray digital forensics investigators; coined the 'CSI Effect' (Overill, 2012; Baranowski *et al.*, 2017). Much has been written about the effect and its association with the image portrayed of a digital forensic practitioner due to the extensive dramatic licence applied in film and television. This study also identifies some participants recognise and relate digital forensics to one word or one activity; for example, "Banking"; "Crime"; "Forensics"; "Cyber crime". With one participant stating they are "Unsure". While others expressed more attitudinal responses such as "I hope the crimes are being watched", and "the checking of peoples personal usage of the internet/searches/social media etc." Some responses to the term cyber security were also vague, for instance: "cyber security?" and "computer security". A few respondents thought of the term as "complicated", or did not know or could not describe, with one respondent noting simply, "Worry". Other responses were intriguing and included more vision and creativity such as, "a robot standing at the door of a club waiting to check people's IDs". This disparate identity of cyber security could prove to outline the true perception of the discipline among members of the public where one respondent expresses cyber security as "buzzwords that few understand in any practical sense".

4. Limitations and Future Work

Limitations of this study are its relatively small number of UK-centric responses, of which there were 102. To capture the public's understanding of security further, a larger demographic and sample of participants should be captured and analysed for new and recurrent themes. Future works should focus on the public view of security and reflection of their own practices considering social desirability.

5. Conclusion

Results depicted the disparate thoughts the public have of the terms digital forensics and cyber security. This study found that there were very few respondents who were unsure on their own perception of the terms digital forensics or cyber security, and very few who exhibited portrayals based on roles of dramatic license seen in television scenarios. Essentially, answers to both terms found that people were aware of both fields in some manner be that a full description of the field or key terms which can relate to these fields. Participants showed awareness for the need for both fields in gathering and interpreting digital data and the idea of protection of data, systems and devices. Responses also show that awareness, education and training is required among the public to ensure cyber hygiene at home as well as the work environment.

6. References

Alharbi, S., Weber-Jahnke, J. and Traore, I. (2011) 'The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review', in Kim, T. et al. (eds) *Information Security and Assurance*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 87–100. doi: 10.1007/978-3-642-23141-4_9.

Aytes, K. and Connolly, T. (2004) 'Computer Security and Risky Computing Practices: A Rational Choice Perspective', *Journal of Organizational and End User Computing*, 16(3), pp. 22–40.

Aytes, K. and Conolly, T. (2003) 'A Research Model for Investigating Human Behavior Related to Computer Security', in *Proceedings of the 9th Americas Conference on Information Systems*. Tampa, FL: Association for Information Systems (AIS). Available at: https://aisel.aisnet.org/amcis2003/260 (Accessed: 22 February 2019).

Baranowski, A. M., Burkhardt, A., Czernik, E. and Hecht, H. (2017) 'The CSI-education effect: Do potential criminals benefit from forensic TV series?', *International Journal of Law, Crime and Justice*. doi: 10.1016/j.ijlcj.2017.10.001.

Cabinet Office (2016) *National Cyber Security Strategy 2016-2021*. London: HM Government, p. 80. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (Accessed: 8 August 2018).

Dlamini, M. T., Eloff, J. H. P. and Eloff, M. M. (2009) 'Information security: The moving target', *Computers & Security*, 28(3–4), pp. 189–198. doi: 10.1016/j.cose.2008.11.007.

Grobler, C. and Louwrens, B. (2006) 'Digital forensics: a multi-dimensional discipline', in *Proceedings of the ISSA 2006. Insight to Foresight Conference*, Pretoria: University of Pretoria.

Grobler, M. and Dlamini, I. (2010) 'Managing digital evidence-the governance of digital forensic', *Journal of Contemporary Management*, 7(1), pp. 1–21.

Irons, A. D., Stephens, P. and Ferguson, R. I. (2009) 'Digital Investigation as a distinct discipline: A pedagogic perspective', *Digital Investigation*, 6(1–2), pp. 82–90. doi: 10.1016/j.diin.2009.05.002.

Joint Task Force on Cybersecurity Education (2017) ‘Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity’, in. (Computing Curricula Series). doi: 10.1145/3184594.

Krakoff, S. (no date) ‘What’s the Difference Between Cybersecurity and Computer Forensics?’, *Champlain College Online*. Available at: https://4a2fd7f23d864318bc3a28e8a2b1590e.pages.ubembed.com/3c4f074e-b8d9-4721-a5e2-c2b2e3945e6f/c.html?closedAt=0 (Accessed: 30 December 2018).

Luiijf, E., Besseling, K. and De Graaf, P. (2013) ‘Nineteen national cyber security strategies’, *International Journal of Critical Infrastructures*, 9(1–2), pp. 3–31. doi: 10.1504/IJCIS.2013.051608.

Merdenyan, B. and Petrie, H. (2018) ‘Generational differences in password management behaviour’, in *Proceedings of 32nd British HCI Conference 2018*. *British HCI 2018*, Belfast, Northern Ireland: BCS Learning and Development Ltd., pp. 1–10. doi: 10.14236/ewic/HCI2018.60.

NCSC (2017) *Certification of Bachelor’s Degrees in Computer Science and Digital Forensics*. Standards 2.0. United Kingdom: National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/content/files/protected_files/article_files/Certification-Bachelors-2_0-20171214.pdf (Accessed: 1 January 2018).

Newhouse, W., Keith, S., Scribner, B. and Witte, G. (2017) *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. NIST SP 800-181. Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.SP.800-181.

Omar, T., Venkatesan, S. and Amamra, A. (2018) ‘Development of Undergraduate Interdisciplinary Cybersecurity Program: A Literature Survey’, in. *2018 ASEE Annual Conference & Exposition*, Salt Lake City, UT: American Society for Engineering Education. Available at: https://www.asee.org/public/conferences/106/papers/22996/view (Accessed: 9 February 2019).

Overill, R. (2012) ‘The “Inverse CSI Effect”: Evidence from e-Crime Data’, in *Proceedings of the 2nd International Conference on Cybercrime, Security and Digital Forensics*. London, UK. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.306.4279&rep=rep1&type=pdf (Accessed: 22 February 2019).

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017) ‘The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies’, *Computers & Security*, 66, pp. 40–51. doi: 10.1016/j.cose.2017.01.004.

Ramirez, R. B. (2017) *Making Cyber Security Interdisciplinary: Recommendations for a Novel Curriculum and Terminology Harmonization*. Master of Science in Technology and Society. Columbia University. Available at: https://dspace.mit.edu/bitstream/handle/1721.1/111232/1003284196-MIT.pdf?sequence=1.

Reith, M., Carr, C. and Gunsch, G. H. (2002) ‘An Examination of Digital Forensic Models’, *International Journal of Digital Evidence (IJDE)*, 1(3), pp. 1–12.

Rowe, B. R. and Gallaher, M. P. (2006) ‘Private Sector Cyber Security Investment: An Empirical Analysis’, in *the fifth workshop on the economics of information security*. *WEIS06*, University of Cambridge, England. Available at: https://www.econinfosec.org/archive/weis2006/docs/18.pdf (Accessed: 15 April 2019).

Schatz, D., Bashroush, R. and Wall, J. (2017) ‘Towards a More Representative Definition of Cyber Security’, *The Journal of Digital Forensics, Security and Law*, 12(2), pp. 53–74. doi: 10.15394/jdfsl.2017.1476.

Shinder, D. L. and Cross, M. (2008) *Scene of the Cybercrime*. 2nd edn. Burlington, MA: Elsevier.

Vidalis, S., Llewellyn, E. and Angelopoulou, O. (2010) ‘Educating Digital Forensic Investigators at Newport’, in *the 4th International Conference on Cybercrime Forensics Education & Training*. Canterbury, UK.