Career Paper

Elizabeth Simpkins

4/8/25

Cyber Forensics: Its reliance on Social Science Research and Principles

What they do and how they connect to society?

Cyber forensics is a career meant to "restore, collect and examine the digital evidence of materials found in digital devices, in relation to cybercrimes." (Chaturvedi, 2019). This career deals with many sectors in society that affect whole populations of people including psychological understandings, legal work, and social media cybercrime investigations. A cyber forensics specialist has to be able to understand societal patterns to understand why cybercriminals will use different resources like social media or choose to target specific groups like a political group, for example. The legal system is something that everyone has to deal with in a society, and is a key aspect in cyber forensics. A cyber forensics specialist has to uncover sound evidence against the cybercriminal involved which can lead into the discussion of laws and ethics, therefore, affecting a society because anyone could be affected by the law. In an article by Sharma (2019), social media is explained to be a massive resource for a cyber forensic analyst, because it gives them access to all sorts of data like messages, videos, and specific platforms used by cybercriminals. Since social media is a platform that connects people in a society and how people are influenced by information online, this career is revolved around society's impact on cybercrime.

Social science research and principles required

A career in cyber forensics requires thought into the social science side of cybersecurity. Social science research helps these specialists be able to understand trends in the cyberspace world and track cybercriminal groups. The social science principles can be used throughout a cyber forensic specialist's research, starting with relativism. Relativism allows cyber forensic specialists to make these connections between society and cybercrime, such as an example listed in an article by Al-Khateeb (2019), between terrorist groups fulfilling their beliefs and social forum sites where they discuss. Objectivity is the next principle and this one is important for the legal part of cyber forensics. In this job, a cyber forensic specialists will be discovering and building evidence against a cybercriminal, and objectivity is mandatory for the research in order for it to be un-biased evidence and research. Parsimony is another principle important to this career field. Parsimony is the principle of explaining things as simple as possible, and while this can be a little difficult for in-depth research and evidence documents in cyber forensics, it is important for later researchers who review behind them to be able to understand it properly. Empiricism is the next principle and this can be seen in the physical "e-evidence" discussed in an article by Chaturvedi (2019), because it is something that the researchers can go off of because they can see it, rather than just believe it. This e-evidence can be messages between suspected cybercriminals, documents found in their possession, videos, or any sort of online information that can help a cyber forensic specialists provide evidence against the convicted cybercriminal. Ethical neutrality is a very tricky principle in this field because cyber forensic specialists are looking at personal, but public, even if restricted, messages and information. In the article by Chaturvedi (2019), this type of personal information can make investigations hard for cyber forensic specialists, because they have to remain ethically neutral by also protecting the rights of

the potential cybercriminal during investigation. Determinism is another principle in cyber forensics which can be seen in the fact that cyber forensic specialists don't just see the crime committed due to someone disliking a political party and then defacing their campaign site. They go to the root of the forum or chat that created a stir in this party and gather evidence from there. Skepticism is the last principle and it is very important in this day in age, due to AI. AI is ever-evolving and new cyberattacks are created all of the time. Skepticism is therefore valued over cyber forensic specialists just assuming past information is still relevant.

Cyber forensics, marginalized groups and other challenges

In cyber forensics, there can be many groups that are affected more than others. Cyber forensic specialists are in charge of tracking patterns in crime, finding evidence, and bringing the cybercriminal to justice. In this process, many different groups can be affected by the crime such as low-income individuals, older people, and other people with little knowledge about cyber awareness. Individuals who get attacked by a ransomware attack and lose a lot of money, or don't have the money to pay, can lose a lot of valuable information. It is important for a cyber forensic specialist not only to find the patterns and catch the criminal, but also to make sure the people affected are made aware of risky online behaviors to possibly prevent them in the future. Some challenges that can arise are the fact that not all cybercrimes are reported, which can make the collected patterns on cybercriminals and victims hard to track sometimes. Another challenge could be the use of AI in attacks nowadays, which can make older cyber awareness methods useless in new scamming attacks that are harder for individuals to identify. Another challenge for marginalized groups could be the groups specifically targeted by data breaches. In an article by Brown (2019), breaches can affect minorities and women more due to discrimination and

harassment. These groups have to be prioritized as well due to being easy targets for cybercriminals.

Applications to social science concepts

One application from class that connects to a career in cyber forensics would be the research method of archival research. Archival research collected can include the internet of things data, social media posts, “text messages, contact lists, photographs, geo-location data, demographic information [and] metadata.” (Sharma, 2019). Another social science concept that relates to this career is keeping society aware of cyber risks through training and the spread of information on how to prevent attacks. It is necessary for cyber forensics specialists to not only provide evidence against a cybercriminal but also understand the trends on who is affected and how they can be educated on the risk factors. As a society, each part of the cyber community should be making people aware of cybercrimes. Another concept would be the use of social media as a social collection of data for a cyber forensic specialist. Social media is a large collection of information and is where a lot of generated disinformation and harmful conversations are typically posted. Cyberbullying, disinformation spread, and terrorist conversations can be tracked and used as evidence when a cyber forensic specialist is conducting a search on a device. A cyber forensic specialist will typically use social media as a source for information along with typical information pulled from or gathered from a device, but this specific use has a name that can be applied from class, social cyber forensics. Social cyber forensics is specifically driven by the information found on online platforms like social media, chat forums, political group chats and so on. They use posts, messages, and different online content, like cyber forensic specialists, to use as evidence.

Conclusion

A career in cyber forensics will lead to a job involving the collection of information as evidence that can help catch a possible cybercriminal. Evidence can come in many forms and typically has to deal with social science frameworks. Social media is a great example of a resource that cyber forensic specialists use to pull messages, posts, images, and other public information from that may be identifiers to a cybercriminal. It is important to incorporate society into this career because people are a huge factor in why and how these specialists can do their jobs. Patterns of cybercriminals, victims, social media groups, and marginalized groups can help develop new mitigation techniques and widen the spread of cyber awareness.

References

Chaturvedi, A., Awasthi, A., & Shanker, S. (2019). Cyber Forensic- A Literature Review. *Trinity Journal of Management, IT & Media. 10*(1). https://www.researchgate.net/profile/Surabhi-Shanker/publication/358780840_Cyber_Forensic_-A_Literature_Review/links/6214f271eb735c508aea4cff/Cyber-Forensic-A-Literature-Review.pdf

Sharma, B.K., Joseph, M.A., Jacob, B., & Miranda, B. (2019). Emerging trends in Digital Forensic and Cyber Security-An Overview. *2019 sixth HCT Information Technology Trends (ITT).* https://doi.org/10.1109/ITT48889.2019.9075101

Al-Khateeb, S. & Agarwal, N. (2019). Social cyber forensics: leveraging open source information and social network analysis to advance cyber security informatics. *Comput Math Organ Theory 26.* https://doi.org/10.1007/s10588-019-09296-3

Brown, D. & Pytlak, A. (2019). Why gender matters in international cyber security. https://eu-iss.s3.eu-central-1.amazonaws.com/horizon/assets/wwqnKkoe/commissioned-research-brown-and-pytlak-1.pdf