6

Putting the Cyber into Cybercrime Teaching

Ruth McAlister and Fabian Campbell-West

Introduction

Criminology is a broad subject area that intersects with numerous others in the social science arena including sociology, psychology, law, economics and political science. As a discipline, it is concerned with advancing knowledge on crime, deviance, its control, and prevention (Chan & Bennett Moses, 2015). Generally, the theoretical knowledge base of the subject reflects changes in society, for the purpose of this chapter we reflect specifically on technological changes. The subject is also responsive to how it adapts in terms of advancing knowledge, so that learning and teaching is contemporary and of an applied nature to

R. McAlister (✉)
Ulster University, Belfast, UK
e-mail: r.mcalister@ulster.ac.uk

F. Campbell-West
Queen's University Belfast, Belfast, UK

© The Author(s), under exclusive license to Springer Nature
Switzerland AG 2022

S. Young and K. Strudwick (eds.), *Teaching Criminology and Criminal Justice*,
https://doi.org/10.1007/978-3-031-14899-6_6

enhance the student learning experience, whilst also developing digital employability skills, such as being conversant in dealing with large-scale data sets, analysing and inferring from data and understanding the challenges in dealing with data.

Undoubtedly the expansion of the Internet and connected devices, particularly in the twenty-first century, has provided vast opportunities and benefits for education, business and for networking and socialising online, the significance of which has been heightened during the global COVID-19 pandemic in 2020–2021. Whilst this technology is arguably a force for good, it also offers unprecedented opportunities to cause harm. Those intent on causing harm are navigating the same online spaces searching for opportunities (Bossler & Berenblum, 2019; CEPOL, 2017). Abusing this technology has opened new avenues for cyber criminals to cause damage to individuals, businesses and governments remote to them. Given the impact of technology on our everyday lives, and on crime, it is clear to see why cybercrime is becoming increasingly integrated into the criminology curriculum at both undergraduate and postgraduate levels. The difficulty comes not with *including* cybercrime-related material, but how best to frame this for social science students, so that they can understand it and apply it, with the majority having a non-technical background. It is also important to consider the role of the educator and their background too when including technological elements in a social science subject. We propose here that by effectively integrating greater technological understanding to the criminology curriculum, is not only important for the study of crime, deviance and criminal justice processes today, but also for students in the future, who may consider a potential career into the burgeoning sphere of cyber security that previously would have been discounted due to a belief that they lack the requisite technical knowledge and skills.

This chapter explores a range of measures and teaching practices that can assist with how better to integrate technology in a truly interdisciplinary way to the criminology cybercrime curriculum. It will begin with a discussion around criminology and cybercrime, tracing the history and challenges of its inclusion within the broader subject area. Next, we embrace pedagogical issues regarding the delivery of interdisciplinary teaching, before considering a specific discussion around pedagogy and digital criminology and how integrating computer science expertise can add value to this approach. From this scene setting we then introduce the substantive element of the chapter where we outline how to integrate a socio-technical project into a cybercrime curriculum which considers the pedagogical issues previously outlined. The conclusion summarises key aspects of the discussion and proposes scholars continue to develop this socio-technical journey.

Criminology and Cybercrime

Attempting to provide a sound definition of what cybercrime is, and importantly what it is not, has plagued scholars for many years. The early days of cybercrime scholarship saw much debate about how best to define the governing of concepts in the field. As such, it was common to draw a distinction between cybercrime and computer crime (Furnell, 2003). Yar (2013) preferred to refer to cybercrime not as a single phenomenon, but rather a range of illicit activities where the common 'denominator' is the use of ICT networks in the commission of a crime. Later, in 2015 Wall provides a useful matrix identifying crime types and crime opportunities. Referring to the former this relates to crimes against machines (cyber trespass for example), crimes using the machine (cyber deception) and crimes in the machine (cyber violence and cyber obscenity). Today, there is still an absence of a consistent definition and whilst arguments regarding what is and what is not cybercrime have diminished a little, it is important to explore the complexities of this technological crime type.

Cybercrime now incorporates a multitude of different offences and offender profiles ranging from cyber-enabled crimes such as online fraud, the sharing of intimate abuse images, identity theft and child sexual exploitation; right through to cyber dependent crimes such as hacking and phishing. It is perpetrated by committed and motivated cyber criminals along with the aid of bots, viruses, phishing malware and ransomware that are designed to infect, and acquire information stored on personal computers (Yar & Steinmetz, 2019). Cybercrimes can be executed almost anywhere in the world with perpetrators not constrained by geographical borders like they are in the physical world.

How these criminals communicate, network and exchange knowledge can take place on hidden forums, they can also exchange stolen goods using cryptocurrencies. The range of threat actors can range from 'script kiddies' to organised criminal networks from different regions and with varying interests who use the Internet to propagandistically showcase and promote their activities (Patton et al., 2013).

As a subject, cybercrime has been described as something of a teenager, the study of the subject is no longer in its infancy, but it has not yet begun to assert its adult confidence and independence (Payne & Hadzhidimova, 2020). Jaishankar (2007), for example, observed that criminologists were almost late to the party in terms of researching cybercrime, yet counterparts in the field of computer science and engineering adapted quicker to change and created new fields such as information security and digital forensics. This may seem an unjust criticism given (for example) the influential work of David Wall who has been publishing scholarly research on cybercrime since the late 1990s. It is however fair to say that cybercrime has only recently become mainstream within the broader criminology curriculum. Now there is a healthy array of cybercrime research that has been undertaken by criminologists on the surface, or open web (the web we use every day with standard search engines), but also on the dark web, first introduced in 2000 where content is not available via standard search engines (Baravalle et al., 2017). Topics addressed by cybercrime scholars have remained fairly consistent over the last decade which includes crimes such as; hacking, financial theft and identity fraud, illicit online networks, child sexual exploitation, stalking and issues regarding surveillance and privacy (Alnabulsi & Islam, 2018; Bancroft, 2020; Cubitt et al., 2020; Etzioni & Rice, 2015; Levi & Soudijn, 2020; Martin, 2014; McAlister & Monaghan, 2020; Musotto & Wall, 2020; Pastrana et al., 2018; Wall, 2000, 2004, 2011; Yar, 2013). Whilst criminologists have developed expertise in these areas, it has been argued that others have remained largely neglected and outside of the criminological gaze. Stratton et al. (2016) for example, have drawn attention to how digital networks enable social harm has been under-researched, together with rapidly emerging issues such as 'digilantism' or digital vigilantism, open source policing, social network surveillance and the role and impact of social network movements. Smith et al. (2017) suggest that one explanation for what may be described as a 'siloed' cyber criminological focus lies in critiques of the discipline more broadly; namely, that criminology itself has become increasingly insular and self-referential, losing some of its fundamental and dynamic origins as the multidisciplinary study of crime, deviance and justice. This also echoes earlier criticism from Jaishankar (2010) where he described cyber criminology as compartmentalised and of no use. Evidence does suggest that true and meaningful engagement with computer science and cybercrime has been largely insular and lacking full interdisciplinary engagement which is according to Stratton et al. (2016) particularly detrimental to advancing a new generation of digital criminological scholarship concerned with technology, crime and deviance.

Interdisciplinary Cybercrime Pedagogy

Interdisciplinary study is described as an important teaching strategy that enables learners to make connections across disciplines and enables them to apply that knowledge in real-life situations (Casey, 2009; Nikita & Mansilla, 2003). It has been argued that learners can apply a broader theoretical and conceptual framework than that of a single discipline with integration of knowledge from differing perspectives beneficial to solve complex problems (Fortuin & Bush, 2010). That said, defining interdisciplinarity is a challenge in itself, partly due to inconsistency in the use of related terms such as multidisciplinary, and transdisciplinary (Lattuca et al., 2013). These terms are often used interchangeably in the literature indicating a lack of consensus on the differences. For those that distinguish among them, integration seems to be key (Hammons et al., 2020). One of the most widely quoted definitions of interdisciplinarity comes from Klein and Newell (1998: 393–394) who describe it as:

> *A process of answering a question, solving a problem, or addressing a topic that is too broad or complex to be dealt with adequately by a single discipline or profession … and draws upon disciplinary perspectives and integrates their insights through construction of a more comprehensive perspective.*

Whilst there is no evidence yet of a paradigmatic shift within criminology, there is evidence of greater interdisciplinarity with other subject areas such as computer science and software engineering. Indeed, it was noted in the introduction that criminology has historically been interdisciplinary as a subject, therefore it seems a natural shift to also integrate it with technical disciplines such as computer science, especially given the growing 'relationship' that crime has with technology. Chan and Bennett Moses (2016) also highlight some engagement with big data research with projects investigating social media data analysis; and an increasing uptake of computer modelling/algorithms as a predictive tool in police and criminal justice decision-making. Whilst this is welcoming, they suggest that 'criminologists and, indeed, social scientists more broadly must increasingly "share the podium" and collaborate with technical experts to further progress this field' (Chan & Bennett Moses, 2015: 25).

Of course, academic disciplines benefit from interdisciplinary work as many exciting advances in scholarship come from combining research efforts. However, Payne (2016) makes the important point that interdisciplinary approaches are not possible without having disciplinary approaches initially. Criminology as mentioned earlier has burgeoned out of a range of disciplines and grown stronger as a result of these other disciplines. The benefits of interdisciplinary research cannot be underplayed, not only for those in education, but all for society. Problems in society are better addressed through different approaches and considerations, whether this is regarding health and technology, city planning and technology, or indeed crime and technology as is the focus here. It can help to broaden perspectives (Oehlberg et al., 2012), interdisciplinary thinking (Lattuca et al., 2017), awareness and importance of team dynamics, communication and leadership (Coso et al., 2010).

Criminology as a discipline is well placed to respond to changes in criminal opportunities and crime prevention, but enhanced collaborations and greater interdisciplinary partnerships are urgently required to help ameliorate current epistemological and methodological gaps particularly around large-scale research and how we can work with such a plethora of data. In addition, a lot of crime sites are now termed to be in ‘cyberspace’ which requires alternative ways of conceptualising criminal motivations and impact on victims. An example, that is expanded on in this chapter, is the analysis of online forums to look for indicators of deviance. As the size of the forum increases it is intractable for traditional manual qualitative analysis by a criminologist. Using automated tools, the number of posts that need to be reviewed can be reduced from millions to hundreds. To ensure the study of cybercrime is truly interdisciplinary, criminology pedagogy needs to embrace and incorporate computational methods training and its students, educators and practitioners must become more digitally informed and algorithmically literate. Criminology educators working with other technical disciplines such as those from computer science or engineering could work more closely together ensuring that cybercrime is truly interdisciplinary. Research undertaken by Payne and Hadzhidimova (2020) examines whether cybercrime is treated as a disciplinary, or multidisciplinary subject, because exploring how cybercrime is studied by criminologists will provide guidance to advance the interdisciplinary and global scholarship of the subject. Their work identified that interdisciplinary cybercrime studies are rare, yet where there is increasing collaboration, it is between computer science and criminology scholars. To increase true interdisciplinary work, it is suggested that digital criminologists bridge the disciplinary and methodological divides in their future efforts (Payne & Hadzhidimova, 2020).

Criminology scholars now have an incredible opportunity to really strengthen the discipline by incorporating greater technical education. Technology impacts on every facet of daily life for most people and almost every aspect of crime, so now more than ever the field ought to extend its disciplinary gaze. Therefore, rather than positioning technology as existing separately to society more broadly, we need to consider the ‘digital society’ as a concept that recognises such technologies are an embedded part of the larger social entity (Lupton, 2014). Criminology as a discipline is slowly transforming to take cognisance of this online crime ‘site’, not only through the foregrounding of digital technologies and data as key parts of everyday life, but also in terms of how they are being investigated and treated by wider agencies in the criminal justice process. The role of teaching what can be addressed as a ‘digital’ criminology which considers the potential impact of digital technologies across a broader range of criminal justice practices may provide a fruitful platform from which to expand the boundaries of contemporary criminological theory and research.

Pedagogy and Digital Criminology

In recent years debates around developing methodological and technical expertise in managing large-scale data sets, or 'big data', have emerged along with issues around Internet-based research and how crime is increasingly manifesting in online environments, or 'cybercrime' as mentioned in the introduction. It is therefore of paramount importance that we all adopt better digital hygiene and do our best to prevent cyber criminals from ruining lives. As explained in cyber security literature this is akin to washing our hands during the Covid-19 pandemic. Digital hygiene is our crucial first line of defence against new and evolving digital threats, such as malicious emails, social engineering, phishing, cyber harassment, hacking accounts and devices and stealing private data (Lewis, 2020). One of the most effective methods of prevention is through education, as mentioned above, with the integration of cybercrime modules into the discipline of criminology. However, technology and cybercrime evolve quickly therefore whilst it is important to include core concepts that are needed to understand the 'problem' of cybercrime, those teaching the subject should be aware of what feels like constant changes in the nature of the cybercrime landscape. This can be anything from threat actors, crime types and evolving threats, along with changes to legislation and policies that being created and revised to better deal with cybercrime.

Criminology pedagogy encourages students to think critically (Serrano et al., 2018). This encourages students to recognise, assess and counteract narratives relating to class, gender and race hierarchies, which influence social problems by promoting the marginalisation of voices (Barton et al., 2010). Critical thinking too should be applied to cybercrime, we need to better understand digital criminality for example. Criminological topics themselves may be theoretically focussed, taught in a traditional format of lectures, small group teaching, reading and policy reviews. It is important though that technology and technological skills are also integrated into the cybercrime curriculum. Conversely, Computer Science is a highly practical subject, so teachers must be proficient in both theory and practical application. Teaching typically requires a blend of presented material in a classroom environment, alongside a practical session where students complete assessed practical assignments (Giannakos et al., 2014). These can include not only computer programming, but also critical thinking and evaluation. As a taught subject Computer Science is highly integrated with technology and effective teaching requires the teacher to understand pedagogical approaches to best support learners (Tucker et al., 2011). The practical elements of which must be learned as much as taught, so engaging with students and encouraging self-learning are important. What we advocate is the 'integration' mentioned earlier. It is not necessary to abandon traditional criminological pedagogy, rather computer science elements can be integrated to ensure the teaching is truly interdisciplinary.

In terms of the learning and teaching experience, educators know that individuals will learn and retain information differently. It is therefore important that when cybercrime modules are developed that they are designed to incorporate various learning styles. Discussions about preferred learning styles have been around for many years and have continued to be revised. Pintrich et al. (1987) created a course to teach students how to learn, including several different teaching modes. Pintrich and De Groot (1990) researched different teaching modes regarding self-regulated learning. Pintrich et al. (1987), and Reed and Bolstad (1991) compared teaching modes of methods versus examples and research using video as a teaching method. VARK (visual, auditory, read/write and kinaesthetic) modalities were made popular by Fleming and Mills (1992) and have been applied to fields such as programming, nursing education, and online learning, and they have been used to investigate learners' levels of acceptance of different educational technologies, (Liew et al., 2015; Truong, 2016). However, opponents of VARK refer to the learning styles 'myth' which suggests that the learning style will only reaffirm individual preferences and should not be used as a learning preference (Kirschener & van Merrienboer, 2013).

In more recent times the technological pedagogical content knowledge (TPACK) framework, an extension of the pedagogical content knowledge framework proposed by Shulman (1986, 1987), has been developed as a method to incorporate modern technologies into the classroom. According to Sumba-Nacipucha et al. (2021) the TPACK model points to seven points of knowledge that an educator must possess, out of which three are called primary knowledge and the remaining four resulting from intersections of primary knowledge types. It is important to be aware that the TPACK may be accused of contributing to 'technostress' which can be referred to as the perceived overuse of technology when it is not necessary (Tarafdar et al., 2010), therefore, striking a balance is very much central.

It is suggested that 'doing' digital criminology requires a holistic approach when developing a cybercrime curriculum. As well as technical elements, including technological tools, there will be a blend of social science subjects and law. Blended academics who could act as a singular person to teach all aspects of the subject, who have an appreciation of both social science, technical skills and appreciation of technological applications, including software development are still quite rare, given that most criminology educators emanate from alternative disciplines. Therefore, incorporating technical expertise from the field of computer science can really add value to exploring cybercrime, or wider digital criminology. Computer science researchers are experienced in applying structured rigorous analysis methodologies to large data sets. They can also help with all stages of a project, adding automation to repetitive jobs and creating scripts to conduct reliable and consistent processing of data. Undoubtedly, failure to adapt the discipline to the digital environments will impinge on the quality of contribution that criminology can offer to crime, deviance and justice processes in the digital age. The assessment recommended in the next section blends technical methods with traditional criminological analysis to highlight the need and use for interdisciplinary skills.

Applied Socio-Technical Project

A practical application of the ideas suggested in this chapter can be combined into a project designed and tailored around a real-world cybercrime investigation. The following is a description of a project that is flexible and extensible, designed to be used for a range of class sizes, experience levels and technical ability. The project is structured as an intelligence gathering and analysis task on a website forum related to hacking. It is split into a series of phases based on how a multidisciplinary team would tackle such a problem in the real world. Each phase can be tuned independently, giving the lecturer scope to tailor the work for the topic and class.

For a criminology student the main benefits of this approach are:

- Demystifying data analysis and removing psychological barriers to entry.
- Broaden awareness of what's involved in practical cybercrime work, including where the challenges are.
- Provide multiple ways for engagement between the technology and social elements.
- Encourage students to develop skills themselves and be self-sufficient.
- Upskill of the discipline and increased employability.

For the lecturer the main benefits of this approach are:

- Standardised assessment with adjustable difficulty based on the student ability
- Can be used for any size of class by adjusting the scope with group size
- Can be modified every time the course is run to minimise plagiarism
- Teaching modern best practice in data analysis along with modern criminology.

Pastrana et al. (2018) noted that only a few members of the thousands frequenting cybercrime forums commit serious crime. However, the role of forums is significant in terms of exposure and dissemination. Forums are a useful target for digital criminology research but require some technical skills to make analysis feasible. For these reasons using a cybercrime forum as the subject for a practical assignment gives students an opportunity to learn valuable transferrable skills. Computer science methods for automated analysis, such as natural language processing, can be directed towards these sights to help identify data for review and reduce the overall manual effort required for a criminologist.

A web forum is a structured collection of conversations between named users. There is a hierarchy of topics, often referred to as subforums, with conversation threads containing posts by individual authors. Examples are shown in Figs. 6.1, 6.2 and 6.3.

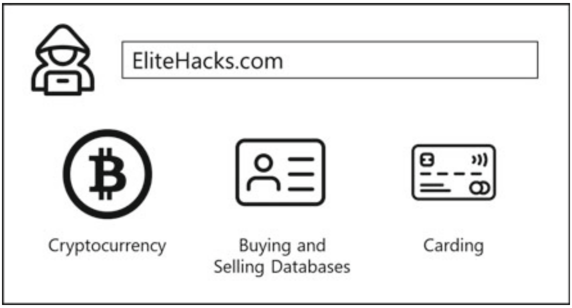


Fig. 6.1 Mock-up of a replica forum called "Elite Hacks" with three subforums: cryptocurrency, buying and selling databases and carding

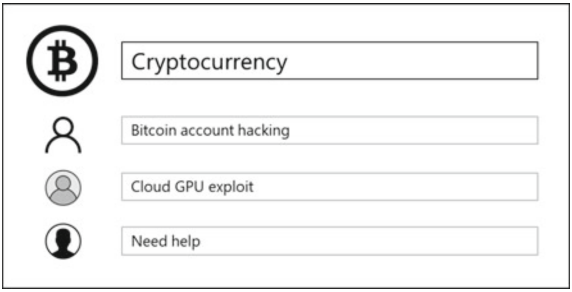
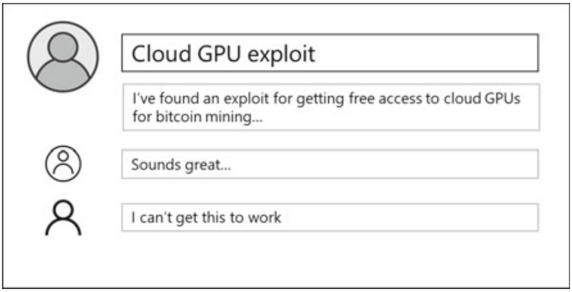


Fig. 6.2 Mock-up of the cryptocurrency subforum with three threads



Cloud GPU exploit

I've found an exploit for getting free access to cloud GPUs for bitcoin mining...

Sounds great...

I can't get this to work

Fig. 6.3 Mock-up of a thread with two other posts from different authors

The replica site is controlled by the lecturer and it is not accessible outside of the student cohort. The lecturer can embed target information in the forum and the project task is for the students to recover this information and reach the correct conclusion. The replica forum is populated with threads and posts based on a real-world hacking forum, making the project task highly realistic. This can be direct and quantitative or open-ended and qualitative with customisable difficulty. Examples are:

- 'How many users are on the forum?'
- 'Who is the most influential user?'
- 'How would you characterise the engagement on the forum?'
- 'Is there any evidence of illegal activity?'

The forum is populated with several thousand or more posts to discourage manual analysis and demonstrate the practical reason for the project phases. To create the replica forum a publicly available dump of an existing forum can be used as a seed, for example AZSecure (https://www.azsecure-data.org). A criminology lecturer may need assistance from computer science colleagues in setting up the replica site in the first instance, but later modifications and management should be straightforward. Working closely in this way in the initial stages helps to foster the interdisciplinary relationship.

The schematic in Fig. 6.4 illustrates the key components of the project. The lecturer uses their domain knowledge to modify the Master Site Record, which is the database behind the forum that contains the information the students must work with. The students can browse the forum through a web browser like a regular forum. Students may be provided with a pre-prepared copy of the web forum in an unstructured or structured format. An example of an unstructured format in this example would be a copy of every thread in the forum in an individual file. An example of a structured format would be a spreadsheet containing a row for every post with columns containing metadata such as date, author, post text, etc. The student uses this information to work through the project and presents their results in an oral or written format.

The project work phases, in Table 6.1, are based on an authentic workflow a criminologist would use in the real world to do this type of analysis work. Each phase has suggested levels and learning outcomes. Level 1 is the simplest version of the project, aimed at students with limited experience. Level 3 represents the tasks required of a professional criminologist conducting this project in academia, industry and government. It is common for subject experts to work in teams and highly skilled criminologists will add more value and find communication and teamwork easier. Each phase can be adjusted independently, for example if the subject matter lends itself more to a particular phase the others can be simplified.

Phases 1, 7 and 9 are common to any criminology study. The other phases are an opportunity to bring in techniques common to computer science. There are a growing number of programmes in Criminology and Criminal Justice that have a statistical focus, and students in these programmes will be comfortable. For others, the rigorous and methodical analysis may seem too technical, but the exposure will help normalise and demystify the concepts. Each of the phases can be simplified or made more challenging to suit the exact requirements of the module. It is recommended to keep the phase structure to ensure students appreciate all the phases involved in a real-world project. In particular, Phase 4: Data Cleaning is often overlooked in this type of project work, but it is an extremely important part of data analysis. In real-world projects data is often incomplete and contains awkward sections that need to be handled. By dedicating a phase of the project to this task reinforces in the students' minds that it is an opportunity to really understand the data and learn more about the problem. Some taught programmes include

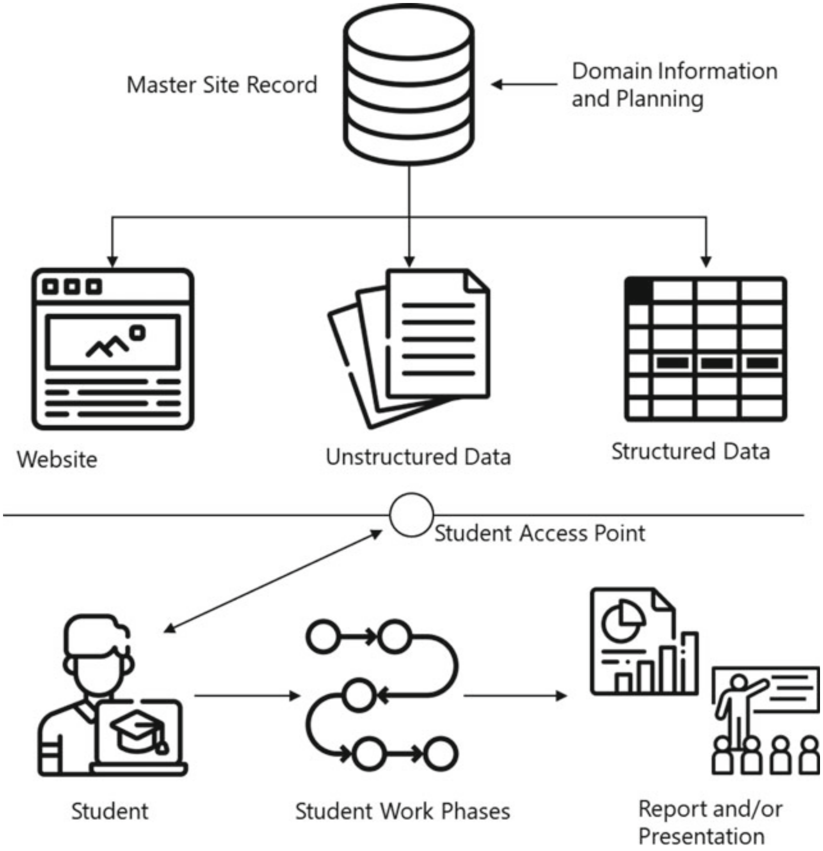


Fig. 6.4 Project schematic illustrating different levels of information the students can access

qualitative research modules, but this is dependent on the availability of appropriate lecturers.

This project structure encourages a practical application of material learned through the course. It promotes communication and interdisciplinary work. It demystifies some technical aspects and promotes a reflective approach suitable for work post-study. It is based on a recent real-world study conducted by the authors, and as such is highly relevant to modern criminology. In the context of TPACK this project covers

Table 6.1 Project work phases

Phase	Tasks and suggested levels	Learning outcomes
1 Project Planning Enable students to consider why tasks are important	Read the project brief and identify the key tasks involved Determine success criteria 1.Project plan is already provided by the lecturer, with clear qualitative/quantitative questions to answer 2.Some guidance is given but students are still given choices in the process 3.Students are given autonomy to design the process with guidance available if needed	Planning, organising and scheduling tasks. Designing Phases of work with potentially incomplete information. Assess the feasibility of the project goal with the information available and the given timescales
2. Identify Data Sources A criminologist must critically evaluate where the information is coming from, if it is authentic and if it potentially satisfies the overall project requirements	Identify suitable sources to gather data from Check access to the data Is the data sufficient? 1.Data sources are explicitly provided and the student is directed 2.Data sources are provided but the student must choose between them, evaluating pros and cons 3.Student must correctly identify the data sources and evaluate their relative value	Critical evaluation of information in the context of a larger goal. Consideration of practical, ethical and legal constraints regarding data access

Phase	Tasks and suggested levels	Learning outcomes
3. Data Gathering Creating a safe place for student to learn about different data gathering tools, such as web scrapers, the project can introduce layers of complexity. This Phase also gives the student an appreciation and awareness of the effort and time required to acquire data for analysis. This is a practical complement of Phase 2	Manually or otherwise obtain the data and store it in a suitable format 1.Data is provided in the format required for analysis, e.g. a spreadsheet 2.Data is provided in one or more formats, but students must manipulate it for analysis, e.g. structured and unstructured files 3.Data must be gathered by the student themselves, e.g. they have access to the replica website and nothing more	Increased awareness of data volume and the consequences of having large data sets, including transmission, storage, sorting and reviewing. Exposure to different data storage formats (file formats, databases)
4. Data Cleaning Data cleaning is often overlooked and is often seen as a less glamorous side of data analysis. Common examples when processing web forums are date and time formats, unusual characters in usernames, and dealing with long posts	Review the data and determine its quality. Is there data missing? Is any data badly formatted or corrupted? 1.Data is already cleaned and ready for analysis 2.Data is partially cleaned, perhaps some is missing or corrupted; or some invalid or irrelevant data is present 3.Data is unmodified from its original source	Understanding that good outputs require good inputs. The need to reduce the amount of data for manual review by removing bad samples and preparing good samples for filtering

(continued)

Table 6.1 (continued)

Phase	Tasks and suggested levels	Learning outcomes
5. Exploratory Data Analysis A traditional data analytical approach can reduce and filter data, but the quantitative view will help understand what data is relevant. In other words, one can use quantitative analysis to filter and sort data, but it is often the qualitative analysis that indicates what good data looks like	Use a mixture of statistical and analytical methods to find patterns and structure in the data Identify metrics for extracting key information Identify methods for filtering to reduce the data volume Begin to gauge if the data is suitable for answering the project questions 1.Explicit instructions are given on what analysis to apply and how 2.Some guidance is given as to good and bad ideas 3.Student is expected to analyse the data independently	Review of basic quantitative analysis techniques and application to a real-world problem. Demonstrating ability to judge data based on measurements and take appropriate conclusions. Critical analysis and adjustment of the approach based on incremental experimentation

Phase	Tasks and suggested levels	Learning outcomes
6. Design, develop and test processes This Phase is an excellent opportunity for criminology students to learn more complex data management skills. From basic analysis, e.g. using Pivot tables in a spreadsheet, to more complex forms. Increased awareness of methods helps communication in an interdisciplinary team	Use findings from Phase 5 to develop automated analysis tools Demonstrate correct operation and usage 1.Use of general-purpose software such as Microsoft Excel to filter, sort and analyse data 2.Bespoke analysis in any available tools 3.Student is encouraged to find and use tools for advanced analysis. Some programming may be used to provide specific analysis function	Familiarity and advanced use of general-purpose software such as spreadsheet and other statistical software packages. For more advanced students programming languages, such as Python, can be used to filter complex data sets
7. Review and analysis This Phase brings together all the data and seeks to address how well the overall objective has been met. In a team environment the criminologist, as the domain expert, will be relied upon to give insight into whether the data is sufficiently detailed and reliable	Core critical thinking component and application of criminology experience Use theoretical and practical domain knowledge to link facts and inform next steps 1.Basic analysis and commentary on the process. Critical analysis of results and drawing basic conclusions 2.Critical analysis of the process and the results. Conclusions and future work planned 3.Full analysis and critique of all stages	Ability to interpolate and extrapolate, where appropriate, to make decisions. Use of knowledge gained during the course and application to an unfamiliar context. Demonstration of mastery of the subject matter
8. Retrospective and repeat This Phase teaches students that retrospective analysis of the process and modification is both "okay" and necessary. This Phase may involve returning to any of the previous phases to modify the process and repeat the work	Critically evaluate the process, identify missing information or flaws in work Return to any prior Phase to update and continue work 1.Commentary on the process, what worked well and what could be done better 2.Evidence of modification of the process based on retrospective analysis 3.Demonstrated learning from the process with evidence of repeated analysis and updated conclusions	Reflection on the performance of the process and separation of results from effort. Ability to identify weaknesses and problems and implement remedial actions. Resilience to negative results and/or feedback and demonstrated perseverance

(continued)

Table 6.1 (continued)

Phase	Tasks and suggested levels	Learning outcomes
9. Conclusion and reporting Reflective analysis of all stages, what worked well, challenges. How things could be improved. What would be done differently next time? What extra training is required? Where should the student focus additional effort?	Draw final conclusions with supporting evidence Present answers to questions in written and/or presentation formats 1.Group discussion and feedback chaired by the lecturer 2.Students present their methods and findings to the class 3.Written project report	Demonstrated ability to present complex information in oral and written formats. Where appropriate the ability to work as a team and play an appropriate role

many different learning activity types including role-playing, interpretation, application and evaluation (Doukakis & Papalaskari, 2019).

Conclusion

This chapter has outlined the importance of interdisciplinary teaching to advance the study of cybercrime or digital criminology. We argue that such integrative strategies enable learners to make connections across disciplines which allows them to see how such knowledge can be applied in real-world situations. With online spaces becoming almost ubiquitous crime sites, a digital criminology approach allows criminologists to refine pedagogical, methodological and theoretical approaches. Learning and adopting rigorous and methodical techniques from computer science allows criminologists to experiment with new ideas for obtaining insights into online offending behaviour and how best the criminal justice agencies can best respond. Consequently, students benefit from learning from how relevant elements of what might seem a far-off subject area can be applied to their field of study. Essentially, we believe that exploiting the innovative capabilities of digital technology for generating new forms of knowledge is essential to advance the cybercrime curriculum, in order it can shed its 'teenage' image and embrace a new stage of development deemed more confident and mature. Whilst we acknowledge that this chapter offers a small contribution in this process, it nevertheless provides an illustration of how integrating computer science techniques to cybercrime is valuable and important. Our intention is to foster a conversation within criminology to further embrace this interdisciplinary socio-technical scholarship. Embracing this journey will inspire new pedagogical dimensions, advance scholarship and enhance digital skills for criminology students.

Top Tips: Teaching Cybercrime

- To raise awareness. Cybercrime as a subject area is growing with multiple crime sites online. Effective cybercrime research is required that is intertwined with computer science and related fields, such as artificial intelligence.
- To promote relevance. Practical applications of combatting cybercrime require a combination of social science and technical skills. Teaching students interdisciplinary material during their degree programme empowers them in their future career.
- Encourage collaborative work. Computer science researchers are increasingly using cybercrime domains for their research but would benefit from a socio-technical perspective that professional criminologists can provide.
- Be hands-on. By using applied practical coursework with perspectives from computer science, criminology students can take a hands-on approach to a real-world problem. The coursework can be tailored to the ability of the group or the scope of the project, with most elements able to be simplified independently.
- Reuse and expand over time. Once the curriculum and module design has been setup initially it can be re-used with little effort on the part of the lecturer and can be efficiently assessed.

References

Alnabulsi, H., & Islam, R. (2018). Identification of illegal forum activities inside the dark net. *International Conference on Machine Learning and Data Engineering (iCMLDE)* (pp. 22–29). https://doi.org/10.1109/iCMLDE.2018.00015

Bancroft, A. (2020). *The darknet and smarter crime*. Palgrave.

Baravalle, A., Sanchez Lopez, M., & Wee Lee, S. (2017). Mining the dark web: Drugs and fake IDs. *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW) Institute of Electrical and Electronics Engineers (IEEE).* https://doi.org/10.1109/ICDMW.2016.0056

Barton, A., Corteen, K., Davies, J., & Hobson, A. (2010). Reading the word and reading the world: The impact of a critical pedagogical approach to the teaching of criminology in higher education. *Journal of Criminal Justice Education, 21*(1), 24–41.

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Criminal Justice, 42*(5), 495–499. https://doi.org/10.1080/0735648X.2019.1692426

Casey, J. (2009). Interdisciplinary approach—advantages, disadvantages, and the future benefits of interdisciplinary studies. *ESSAI, 7*, 26.

CEPOL. (2017). Crime in the age of technology. https://www.cepol.europa.eu/sites/default/files/924156-v7-Crime_in_the_age_of_technology_.pdf. Accessed 24 September 2021.

Chan, J., & Bennet Moses, L. (2015). Is big data challenging criminology. *Theoretical Criminology, 20*(1), 21–39. https://doi.org/10.1177/1362480615586614

Coso, A. E., Bailey, R. R., & Minzenmayer, E. (2010). How to approach an interdisciplinary engineering problem: Characterizing undergraduate engineering students' perceptions. 2010 IEEE Frontiers in Education Conference (FIE) Washington, DC: F2G-1-F2G-6.

Cubitt, T. I. C., Wooden, K. R., & Roberts, K. A. (2020). A machine learning analysis of serious misconduct among Australian police. *Crime Science, 9*(22), 1–13. https://doi.org/10.1186/s40163-020-00133-6

Doukakis, S., & Papalaskari, M. A. (2019). Scaffolding Technological Pedagogical Content Knowledge (TPACK) in Computer Science Education through Learning Activity Creation. Conference: 2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). https://doi.org/10.1109/SEEDA-CECNSM.2019.8908467

Etzoni, A., & Rice, C. J. (2015). *Privacy in a cyber age*. Palgrave.

Fleming, N. D., & Mills, C. (1992). Helping students understand how they learn. *The teaching professor* (Vol. 7, No. 4). Magma Publications.

Fortuin, K. P., & Bush, S. R. (2010). Educating students to cross boundaries between disciplines and cultures and between theory and practice. *International Journal of Sustainability in Higher Education, 11*(1), 19–35.

Furnell, S. (2003). Cybercrime: Vandalizing the Information Society. In: Lovelle, J.M.C., Rodríguez, B.M.G., Gayo, J.E.L., del Puerto Paule Ruiz, M., Aguilar, L.J. (eds) Web Engineering. ICWE 2003. *Lecture Notes in Computer Science,* vol 2722. https://doi.org/10.1007/3-540-45068-8_2

Giannakos, M. N., Doukakis, S., Crompton, H., Chrisochoides, N. Adamopoulos, N., & Giannopoulou, P. (2014). Examining and mapping CS teachers' technological, pedagogical and content knowledge (TPACK)min K-12 schools, in 2014 IEEE Frontiers in Education Conference(FIE) Proceedings (pp. 1–7).

Hammons, A. J., Fiese, B., Koester, B., Garcia, G. L., Parker, L., & Teegarden, D. (2020). Increasing undergraduate interdisciplinary exposure through an interdisciplinary web-based video series. *Innovations in Education and Teaching International, 57*(3), 317–327. https://doi.org/10.1080/14703297.2019.1635902

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology, 1*(1), 1–6.

Jaishankar, K. (2010). The future of cyber criminology: Challenges and opportunities. *International Journal of Cyber Criminology, 4*(1 and 2), 26–31.

Kirschner, P. A., & van Merrienboer, J. J. G. (2013). Do learners really know best? *Urban Legends in Education, 48*(3), 169–183. https://doi.org/10.1080/00461520.2013.804395

Klein, J., & Newell, W. (1998). Advancing interdisciplinary studies. In W. Newell (Ed.), *Interdisciplinarity: Essays from the Literature* New York: College Entrance. Examination Board (pp. 393–394).

Lattuca, L. R., Knight, D. B., & Bergom, I. (2013). Developing a measure of interdisciplinary competence. *International Journal of Engineering Education, 29*(3), 726–739.

Lattuca, L. R., Knight, D. B., Ro, H. K., & Novoselich, B. J. (2017). Supporting the development of engineers' interdisciplinary competence. *Journal of Engineering Education, 10*(6), 71–97.

Lewis, J. (2020). *Five digital hygiene tips to start fresh in the new year*. https://www.cira.ca/blog/cybersecurity/5-digital-hygiene-tips

Levi, M., & Soudijn, M. (2020). Understanding the laundering of organized crime money. *Crime and Justice, 49*, 579–631.

Liew, S. C., Sidhu, J., & Baura, A. (2015). The relationship between learning preferences (styles and approaches) and learning outcomes among pre-clinical undergraduate medical students. *BMC Medical Education, 15*(4). https://bmcmededuc.biomedcentral.com/articles/10.1186/s12909-015-0327-0. Accessed 20 September 2021.

Lupton, D. (2014). *Digital sociology*. Routledge.

Martin, J. (2014). Lost on silk road. Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice, 14*(3), 351–367. https://doi.org/10.1177/1748895813505234

McAlister, R., & Monaghan, R. (2020). Digital extremisms: Readings. In M. Littler, & B. Lee (Eds.), *Violence, radicalisation and extremism in the online space* (pp. 133–156). Macmillan.

Musotto, R., & Wall, D. S. (2020). More Amazon than Mafia: Analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime, 25*, 173–191. https://doi.org/10.1007/s12117-020-09397-5

Nikitina, S., & Mansilla, V. B. (2003). *Interdisciplinary studies project, project zero. Harvard Graduate School of Education Three Strategies for Interdisciplinary Math and Science Teaching: A Case of the Illinois Mathematics and Science Academy*.

Oehlberg, L., Leighton, I., Agogino, A., & Hartmann, B. (2012). Teaching human-centered design innovation across engineering, humanities and social sciences. *International Journal of Engineering Education, 28*(2), 484–491.

Patton, D. U., Eschmann, R. D., & Butler, D. A. (2013). Internet banging: New trends in social media, gang violence, masculinity and hip hop. *Computers in Human Behavior, 29*, A54–A59.

Payne, B. K. (2016). Expanding the Boundaries of Criminal Justice: Emphasizing the "s" in the criminal justice sciences through Interdisciplinary efforts. *Justice Quarterly, 33*(1), 1–20. https://doi.org/10.1080/07418825.2015.1068837

Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research. *International Journal of Cyber Criminology, 14*(1), 81–105. https://doi.org/10.5281/zenodo.3741131

Pastrana, S., Hutchings, A., Caines, A., & Buttery, P. (2018). Characterizing eve: Analysing cybercrime actors in a large underground forum. *Research in Attacks, Intrusions, and Defences*, (RAID) (pp. 207–277).

Pintrich, P. R., Mckeachie, N. J., & Lin, Y. G. (1987). Teaching a course in learning to learn. *Teaching of Psychology, 14*(2), 81–86.

Pintrich, P. R., & de Groot, E. V. (1990). Motivational and self-regulated learning components of classroom academic performance. *Journal of Educational Psychology, 82*(1), 33–40.

Reed, S. K., & Bolstad, C. A. (1991). Use of examples and procedures in problem solving. *Journal of Experimental Psychology: Learning, Memory, and Cognition, 17*(4), 753–766. https://doi.org/10.1037/0278-7393.17.4.753

Shulman, L. S. (1986). Those who understand: Knowledge growth in teaching. *Educational Researcher, 15*(2), 4–14. https://doi.org/10.3102/0013189X015002004

Shulman, L. S. (1987). Knowledge and teaching: Foundations of the new reform. *Harvard Educational Review, 57*(1), 1–22. https://doi.org/10.17763/haer.57.1.j463w79r56455411

Smith, G. J. D., Bennett Moses, L., & Chan, J. (2017). The challenges of doing criminology in the big data era: towards a digital and data driven approach. *British Journal of Criminology, 57*(2), 259–274. https://doi.org/10.1093/bjc/azw096

Serrano, M., O'Brien, M., Roberts, K., & Whyte, D. (2018). Critical pedagogy and assessment in higher education: The ideal of 'authenticity' in learning. *Active Learning in Higher Education, 19*(1), 9–21.

Stratton, G., Powell, A., & Cameron, R. (2016). Crime and justice in digital society: Towards a digital criminology. *International Journal for Crime, Justice and Social Democracy, 6*(2), 17–33. https://doi.org/10.5204/ijcjsd.v6i2.355

Sumba-Nacipucha, N., Estrada-Cueva, J., Lorenzo-Conde, E. (2021). *Reflections on the role of the professor from the TPACK model perspective during covid-19*. IEEE World Conference on Engineering and Education. https://ieeexplore.ieee.org/document/9429097. Accessed 20 September 2021.

Tarafdar, M., Tu, Q., & Ragu-Nathan, T. S. (2010). Impact of technostress on end-user satisfaction and performance. *Journal of Management Information Systems, 27*(3), 303–334. https://doi.org/10.2753/mis0742-1222270311

Tucker, A., Seehorn, D., Carey, S., Moix, D., Fuschetto, B., Lee, I., O'Grady-Cuniff, D., Stephenson, C., Verno, A. (2011). CSTA K-12 computer science standards. CSTA Standards Task Force (revised). http://csta.acm.org/Curriculum/sub/CurrFiles/CSTA_K-12_CSS.pdf

Truong, H. M. (2016). Integrating learning styles and adaptive e-learning system: Current developments, problems and opportunities. *Computers in Human Behaviour*, *55*(Part B), 1185–1193. https://doi.org/10.1016/j.chb.2015.02.014

Wall, D. S. (2000). Introduction cybercrimes, cyberspeech and cyberliberties. *International Review of Law, Computers and Technology, 14*(1), 5–9.

Wall, D. S. (2004). Digital realism and the governance of spam as cybercrime. *European Journal on Criminal Policy and Research, 10*(4), 309–335.

Wall, D. S. (2011). Cyber criminology exploring internet crimes and criminal behaviour foreword. *Cyber Criminology: Exploring Internet crimes and human behaviour* (pp. XI–XI).

Yar, M., & Ste, K. F. (2019). *Cybercrime and society*. Sage.

Yar, M. (2013). *Cybercrime and Society*. Sage