VARSTVOSLOVJE
Journal of Criminal Justice and Security
year 24
no. 2
pp. 149–171

How does Educational Background Shape the Perception of Cybercrime? A Survey of Computer Science and Law Students on Selected Controversial Issues

Andrzej Uhl, Andrzej Porębski

Purpose:

The technical dimensions of cybercrime and its control have rendered it an inconvenient subject for many criminologists. Adopting either semantic (legal) or syntactic (technical) perspectives on cyber criminality, as theorised by McGuire, can lead to disparate conclusions. The aim of this paper is to examine how these perspectives and corresponding educational backgrounds shape opinions on cybercrime and cybercrime policy.

Design/Methods/Approach:

To address this research question, we first provide a non-exhaustive review of existing critical literature on a few selected controversial issues in the field, including cyber vigilantism, file sharing websites, and political hacking. Based on these areas, we developed an online survey that we then distributed among students of law and computer science, as well as to a 'non-cyber contrast group' including mainly students of philology and philosophy.

Findings:

Statistical analysis revealed differences in the way respondents approached most of the issues) to most of the issues, which were sometimes moderated by the year of studies and gender. In general, the respondents were highly supportive of internet vigilantism, prioritised the cybercrimes of the powerful, and encouraged open access to cybersecurity. The computer science students expressed a lower fear of cybercrime and approved of hacktivism more frequently, while the law students affirmed a conservative vision of copyrights and demonstrated higher punitiveness towards cyber offenders. Interestingly, the computer science students were least likely to translate their fear of cybercrime into punitive demands.

Research Limitations/Implications:

The findings support the distinction between various narratives about cybercrime by showing the impact of professional socialization on the expressed opinions. They call for a consciously interdisciplinary approach to the subject and could be complemented by a comprehensive qualitative inquiry in the perception of cyber threats.

Originality/Value:

The authors wish to contribute to the understanding of the construction of cybercrime on the border of criminal law and computer science. Additionally, we present original data which reveal different views on related issues held by potential future professionals in both areas.

Keywords: cybercrime, cyber victimisation, cyber punitiveness, internet crime

UDC: 343.3/.7 :004

Kako izobrazba oblikuje dojemanje kibernetske kriminalitete? Anketa med študenti računalništva in prava o izbranih spornih vprašanjih

Namen prispevka:

Zaradi tehničnih razsežnosti kibernetske kriminalitete in njenega nadzora je ta za mnoge kriminologe neprijetna tema. Sprejemanje semantičnega (pravnega) ali sintaktičnega (tehničnega) pogleda na kibernetsko kriminaliteto, kot ga je oblikoval McGuire, lahko privede do različnih zaključkov. Namen članka je preučiti, kako vidiki in ustrezna izobrazba oblikujejo mnenja o kibernetski kriminaliteti in politiki kibernetske kriminalitete.

Metode:

Da bi odgovorili na raziskovalno vprašanje, smo najprej pripravili neizčrpen pregled obstoječe kritične literature o nekaj izbranih spornih vprašanjih na tem področju, vključno s kibernetskim vigilantizmom, spletnimi stranmi za izmenjavo datotek in političnimi hekerskimi napadi. Na podlagi teh področij smo razvili spletno anketo, ki smo jo pozneje razdelili med študente prava in računalništva ter v "nekibernetsko kontrastno skupino", ki je vključevala predvsem študente filologije in filozofije.

Ugotovitve:

Statistična analiza je razkrila razlike v pristopu k večini vprašanj, ki so včasih odvisne od letnika študija in spola. Na splošno so anketiranci zelo podpirali internetno vigilanco, osredotočanje na kibernetske zločine močnih in odprt dostop do kibernetske varnosti. Študenti računalništva so izrazili manjši strah pred kibernetsko kriminaliteto in pogosteje odobravali hektivizem, medtem ko so študenti prava potrdili konservativno vizijo avtorskih pravic in pokazali večjo kaznovalnost do kibernetskih prestopnikov. Zanimivo je, da so študenti računalništva svoj strah pred kibernetsko kriminaliteto najredkeje prenesli v

kazenske zahteve.

Praktična uporabnost:

Ugotovitve podpirajo razlikovanje različnih pripovedi o kibernetski kriminaliteti, saj kažejo vpliv poklicne socializacije na izražena mnenja. Pozivajo k zavestnemu interdisciplinarnemu pristopu k tej temi in bi jih lahko dopolnili s celovito kvalitativno raziskavo dojemanja kibernetskih groženj.

Izvirnost/pomembnost prispevka:

Avtorji želijo prispevati k razumevanju konstrukcije kibernetske kriminalitete na meji kazenskega prava in računalništva. Poleg tega predstavljamo izvirne podatke, ki razkrivajo različne poglede prihodnjih strokovnjakov na obeh področjih na sorodna vprašanja.

Ključne besede: kibernetska kriminaliteta, kibernetska viktimizacija, kibernetska kaznovanost, internetna kriminaliteta

UDK: 343.3/.7:004

1 INTRODUCTION

The social construction of cybercrime takes place on the border between criminal law and computer science. Inevitably, interdisciplinarity lies at the heart of the newly established cyber criminological field of research. The nature of cybercrime as a technological problem, a crime problem, a business concern, and a social issue calls for its exploration from various academic perspectives (Payne & Hadzhidimova, 2020). As in the case of economic crime, the understanding of that complex phenomenon often requires consideration of technical nuances mostly unknown to criminal lawyers. McGuire (2018) has used the linguistic terms of syntax and semantics to illustrate that duality; the criminal justice is mainly concerned with the socially constructed (legal) meaning of online actions, whereas information technology delineates the conditions under which these actions are technically feasible within the digital setting. Existing discourses on cybercrime distinguished by Wall (2008) include legislative, expert, academic, and popular. While the law provides the normative structure that underpins the state's reaction to deviance in cyberspace, IT experts can offer a practical understanding of the domain wherein cybercrime and its control occurs (Holt, 2016).

Informed by those voices in scholarship, we conclude that the study of cybercrime cannot be complete without consideration of two different frames of reference: the normative and the technological view. It is still more important concerning controversial issues since the diversity of professional backgrounds could deliver valuable perspectives on e.g. cyber-surveillance, hacktivism, and other widely discussed topics. Crime control has, furthermore, long ceased to be an area of unconstrained professional discretion, and the sentiments of the general public ought to be reckoned with (Garland, 2002). The learned opinions of legislators and computer specialists should be at least compared against the background of the popular discourse, as mentioned by Wall (2008). To this end,

the study at hand draws upon themes from academic literature and consults representatives of popular, legal, and IT viewpoints.

Most of the existing discourse on cybercrime is written in a highly practical tone, often amounting to the study of effective prevention. Many writings are produced by state agencies professionals who have rare cross-branch knowledge, but also a clear affiliation with the criminal justice system. On the contrary, remarkably little has been written on cybercrime from a critical perspective. Delinquency in cyberspace, as anywhere else, offers a subject for the study of state control, political conflict, and moral entrepreneurship (McCarthy & Steinmetz, 2020). The next section summarizes a few selected focal points of the critical literature on cybercrime. The list is by no means exhaustive but attempts to encompass the issues of high interest to academic scholarship as well as controversial topics present in the public debate on cyberspace and its offenders. Although the survey is not meant to side with any party to the outlined debates, the literature review is focused on critically oriented authors who raise these controversies by challenging the widespread beliefs and existing status quo. The opposite views could be partly inferred from their critical writings, but the entire disputes are not available for reasonable study in this single research article.

2 CONTROVERSIAL ISSUES IN CYBERCRIME

2.1 ‚Cyber' Terminology

The controversies over cybercrime began as early as the term was introduced. Cybercrime lacks a universally accepted definition (Gordon & Ford, 2006). Many authors challenge the idea that a category of crime can be distinguished by the sole virtue of being committed with the use of an electronic device. Grabosky (2001) has dubbed cybercrime "old wine in the new bottles"; meaning that it is, to all intents and purposes, the same as traditional criminality and different only in terms of the medium (but see: Yar, 2005). McGuire (2018) argues in a similar vein that internet criminality is ultimately the problem of underlying social interactions rather than how those interactions are mediated. The common root of crimes in cyberspace and physical environments has been exposed during recent lockdowns that led to crime displacement to online settings (Buil-Gil et al., 2021). Moreover, the claims about the prevalence of cybercrimes often lack clarification as to what is so particularly 'cyber' about them (Wall, 2008). According to various studies, 80% or more cybercrimes are performed due to the human factor (Kranenbarg & Leukfeldt, 2021). Even actions as technologically advanced as hacking, or the use of malware, show analogies with terrestrial sabotage, vandalism or, espionage (McGuire, 2018). As more and more areas of life go online, so do the related crime opportunities, whose diversity in cyberspace reaches the diversity of traditional crimes. Therefore, 'the relative equity in specialization relative to versatility, particularly in both on- and off-line activities, suggests that there may be limited value in treating cybercriminals as a distinct offender group' (Leukfeldt & Holt, 2022). Some authors have maintained that such 'cyber' framing constructs

internet crime as a unique threat calling for an extraordinary response, which in turn could only be given if crime control agencies were entrusted with extended powers (Palfrey, 2000; Rüther, 2001).

The 'cyber' prefix is also liberally used in reference to terror organizations, although it has been argued that few, if any, computer network attacks meet the criteria for terrorism (Denning, 2010). With critical infrastructure being isolated from the world wide web, terrorist use of the internet remains largely limited to propaganda, fundraising, and recruitment (Yar & Steinmetz, 2019). Holt (2016) classifies cyberterrorist activities comparable to real-life terror as 'social science fiction'. The apparent lack of genuine cyberterrorism provides space for the rhetorical use of the term on a political level (Romagna, 2020). Since the use of the terrorist label is a convenient way of delegitimizing a particular political project (Yar & Steinmetz, 2019), one man's cyberterrorist could as well be another man's hacktivist.

2.2 Fear of Crime

Once such a threat is constructed, it fuels what could be called the fear of cybercrime (Virtanen, 2017). Gradually, cyberspace is seen as pathologically unsafe and highly criminogenic (Wall, 2008). Massive and mostly uncritical media coverage contributes to that 'culture of fear' surrounding cybercrime (Jarvis et al., 2015; Prislan & Bernik, 2013) and does not adequately reflect the rather unspectacular experience of cyber criminality within the criminal justice system (Wall, 2008). While fear of cybercrime could be instilled instrumentally (Banks, 2015; Rüther, 2001), grassroots urban legends of e.g. the Blue Whale also depict the internet community as a deadly threat to children, who are supposedly incited to self-harm and suicide in the alleged online challenge (Puneßen, 2017). Although young people are certainly vulnerable on the internet, exaggerated claims and uninformed attempts to detach minors from cyberspace might hinder their socialization within the technologically savvy generation (Riek et al., 2016). For adults, fear of cybercrime is associated with avoidance behaviour, 'thereby impeding individuals' perceived online freedom and opportunities' (Brands & van Wilsem, 2021). We further link the growing fear of cybercrime to other phenomena: approval of expanded state surveillance or the excesses of online vigilantes.

2.3 Vigilantism

The rise of online vigilantes could be of interest to critical criminology as a challenge to power relations and exertion of control over the web. It could also be indicative of insufficient protection of the users by state agencies who have to fetch for themselves or resort to private security (Chang & Poon, 2017; Rosenbaum & Sederberg, 1974). As these topics are partly addressed below, this section pays special attention to the controversial phenomenon of online paedophile hunting. Some Internet users pass as juveniles under the age of consent and hold erotic conversations with interested adults. Then, they arrange a meeting, which provides the police with an opportunity to arrest the potential

abuser (Hadjimatheou, 2021). Often, chat logs are published before the police are informed and launch any investigation (Smallridge & Wagner, 2020). Online paedophile hunters, often acclaimed as popular heroes, have also received criticism for the use of entrapment, media exposure, and public humiliation prior to valid conviction (Campbell, 2016). Furthermore, such a conviction may prove impossible, e.g. in continental jurisdictions. Child grooming laws address a form of punishable preparation for an offence of child abuse (Albrecht, 2011). As the chat partner is actually an adult, the offence lacks its suitable object and could only be classified as an inept attempt (see Dubber & Hörnle, 2016). Therefore, a conviction for attempted preparatory offence would violate the very principle of the preparation-attempt-consummation sequence. While a criminal attempt to prepare an offence is hardly thinkable, misguided vigilantes could commit a number of infractions including libel, false accusation, or punishable provocation provided that their target person was not guilty.

2.4 Surveillance and (other) Cybercrimes of the Powerful

The moral panic over cybercrimes provides state agencies with arguments in favour of extended internet surveillance (Palfrey, 2000; Rüther, 2001). Scholars associated with critical surveillance studies wrote extensively on the monitoring of users' online behaviour. Some invoke the metaphor of the panopticon to draw a dystopic picture of cyberspace dominated by state and market forces and devoid of any anonymity (see Nussbaum & Udoh, 2020 for a review). Crime control agencies entrusted with overarching competences might face the temptation to employ them for new purposes (Ventura et al., 2005). Internet users are subject to surveillance, not only as state citizens, but also as customers and consumers; the constant analysis, monitoring, and manipulation are now argued to collectively constitute another surveillance regime (Nussbaum & Udoh, 2020).

The increased criminalisation of cybercrime is not necessarily accompanied by high standards of state and business ethics online. In their paper on critical cyber criminology, McCarthy and Steinmetz (2020) have applied the term of the crimes of the powerful to corporate control of internet access or the prosecution of online whistle-blowers. In recent years, big-tech algorithms have been considered a serious threat to democracy (Cho et al., 2020). Another adducible example is the total ban on Wikipedia in Turkey, under Erdogan's administration, instituted by the legal act bearing the telling title 'Law on Fighting Crimes Committed Through Internet Broadcasting'. The emergence of internet-related human rights sheds new light on such clear violations and calls for a better examination of that category of state crime (Szoszkiewicz, 2020).

2.5 Hacktivism

The rise of digital activists, also known as hacktivism, has been another controversial issue in the debate over cybercrimes and cyberliberties. Throughout its over 30-year-long history, its *modi operandi* have included defacement of public websites, distributed denial-of-service attacks, or publishing leaks from state agencies (Karagiannopoulos, 2021). Although many see political activism

in cyberspace as an emerging form of civil disobedience and social protest, unwelcome actions are sometimes given the cyberterrorist label by the security industry and government organizations (Romagna, 2020). The process aimed at constructing hacking as a criminal phenomenon, described by Yar and Steinmetz (2019), inevitably led to the association of politically motivated hackers with extremism and terror. Critical voices, however, have addressed hacktivism with approval of nonviolent methods, cultivation of free speech, and advocacy for human rights (Hampson, 2012; Vegh, 2003). The latter two are of special importance in countries where terrestrial forms of protests are still met with prosecution and state violence (Jordan & Taylor, 2004). Those attached to the narrow definition of terrorism may recognize the hacktivist campaign against the Islamic State as an indication of the qualitative difference between terror organizations and digital activism (Richards & Wood, 2018).

2.6 Digital Piracy

No single issue in internet crime control mirrors the assumptions of conflict criminology better than the fight over various forms of unofficial peer-to-peer file sharing. On the one side, the entertainment industry represented by actors such as RIAA introduces its own discourse of 'intellectual property theft' preying on 'starving artists' (Yar & Steinmetz, 2019). The opposing narration, here and there backed by entire Pirate Parties, embraces the open access to cultural goods and questions the role of corporate mediators between the creators and their audience – some pirates indeed see themselves as promoters of upcoming artists (Tade & Akinleye, 2012). Further dissident voices denounce antipiracy as an ideological endeavor aimed at preserving capital accumulation on the side of the entertainment industry, which seemingly orchestrated its 'version of the war on drugs: an expensive, protracted, apparently ineffective and seemingly misguided battle against a contraband that many suggest does little harm' (Mousley, 2003; Yar, 2008).

In this paper, we focus particularly on what critics call 'guesstimations'; an assessment of industry losses based on official prices multiplied by the number of unauthorised downloads. This methodology produced estimates of billions of dollars in losses incurred as a result of digital piracy (Drahos & Braithwaite, 2007; Yar & Steinmetz, 2019). In fact, overprized digital products are particularly likely to be accessed through unauthorised channels, as subjectively unfair prices were found to increase motivation to use pirate copies (Kukla-Gryz et al., 2021), which, in turn, increases the alleged losses. Remarkably, vast numbers of pirate files are downloaded in the countries of the Global South, where access to cultural goods is limited by inhibitive prices or even absent. Academic writing on that subject should not lack reference to online shadow libraries that make scholarly research on a broad scale possible in many nations, such as India (Liang, 2018). In western countries, many use pirate websites out of convenience despite having access to the media provided by their institutions (Bohannon, 2016). Moreover, the authors question the idea that intellectual property can be stolen or even challenge the idea that culture is subject to property rights. Yar and Steinmetz (2019) evoke

examples of cultures viewing art and knowledge as common goods that can and should be disseminated among the entire population.

2.7 Responsibilization of Cybersecurity

Once fear of crime in cyberspace has been instilled in the populace, the private industry of security products comes to rescue those ready to and capable of paying for its costly software. Symptomatic of the state's failure to protect ordinary users, the growth in sales of security services is additionally cultivated by the narration of fear (Banks, 2015). Yar and Steinmetz (2019) believe that privatization of internet security violates the principle of freedom from (cyber) criminal predation as a right of all citizens. The responsibilisation strategy in that area means that computer security is divisive and unevenly provided as a commodity (Yar, 2009), while societies most susceptible to cyber victimization cannot afford the market-dictated prices (Cassim, 2011). Thereby, the social disadvantage of some groups could be replicated or even exacerbated in cyberspace (Yar & Steinmetz, 2019). According to recent literature, private policing of the internet lacks oversight and accountability, but also suffers from the competing interests of various actors (McCarthy & Steinmetz, 2020; Renaud et al., 2018).

3 CURRENT STUDY

Following the review of selected academic literature on the topics discussed, the results were obtained among the representants of legal, technical, and popular perspectives on cybercrime. We thus intend to do justice to the classification of basic discourses on cybercrime put forward by Wall (2008). The surveyed sample consists of law and computer science students as well as a 'non-cyber contrast group' composed mainly of philology and philosophy students, i.e. individuals from a population assumedly unacquainted with either of the aforementioned area on a professional level. Both law and computer science students undergo a process of gradual socialization to their prospective professions. This process is accomplished through the adoption of certain jargon, ways of thinking, and professional ideologies (Guzman & Stanton, 2004; Mertz, 2007). Incorporating the 'year of study' variable allows for tracing the level of professional socialization in sampled students. Due to this socialization, we consider the opinions of the respondents to be indicative of the views held by practising lawyers and IT specialists. We employ gender, which is widely recognized to influence punitiveness and fear of crime (Armborst, 2017), as a control variable. The responses given to the set of ten questions constitute the dependent variables. These questions were informed by the issues discussed in the general public and the scholarly literature. In so doing, we do not present any comprehensive survey on cybercrime, but rather a snapshot of the opinions expressed on a few thought-provoking topics. In particular, interrelating these subjects in theoretical terms would require a study of an encyclopedic nature, which is beyond our capacities. Nevertheless, we believe that differences between three groups of students, if

observed, might demonstrate the significance of the distinction between the aforementioned modes of thinking about cybercrime.

4 METHODS

Having reviewed the relevant publications, we constructed an internet-based questionnaire with ten main items meant to test the attitude towards each of the aforementioned controversies (or selected aspects thereof) in a non-suggestive manner. The questionnaire was complemented with questions about gender and the current year of study. We did not employ variables on computer and Internet use, treating them as factors that differ inherently across the study groups. We thus do not wish to isolate their influence on the dependent variables from the influence of the field of study. The substantive questions took the form of short statements followed by a five-point (from 1 – *strongly disagree* or related to 5 – *strongly agree* or related) Likert scale[1], on which the subjects were asked to indicate their agreement or disagreement with a given statement. The survey was distributed among students from the nation's leading universities. Graduates of these institutions are most likely to successfully follow a career in their studied professions, e.g. become legal practitioners after obtaining a master's degree in law.

We sent an active link to the online form to the groups of the given courses on the social media platform Facebook, which is the most common form of peer communication among Polish students. To allow the research questions to be answered, respondents were additionally asked to specify their major at the end of the questionnaire. The survey was met with substantial interest, and nearly 400 raw responses were submitted. After cleaning the data set of unusable records, we obtained 370 observations, divided into three groups according to the major studied. The data set included 150 responses from computer science students, 103 responses from law students, and 117 responses from the contrast group.

Statistical analysis was performed using the R v. 3.63 language (R Core Team, 2020), RStudio IDE (RStudio Team, 2020) and packages: *ordinal* (Christensen, 2019a), *dplyr* (Wickham et al., 2020), *brant* (Schlegel & Steenbergen, 2020), *MASS* (Venables & Ripley, 2002), and *readr* (Wickham et al., 2018). Since the surveys used a Likert scale, which is an ordinal scale, it made the most sense to utilise modelling techniques constructed for the ordinal dependent variables. Although it is possible to treat the Likert scale as an interval scale (Norman, 2010), such an approximation would be less accurate the fewer points the scale includes (Wu & Leung, 2017). Therefore, we decided to use cumulative link modeling to create ordinal regression models (Christensen, 2019b). Nevertheless, to illustrate the general characteristics of the responses in the subgroups, the mean values were calculated, treating the Likert scale as an interval scale.

The backward stepwise regression with optimization relative to the Akaike information criterion (AIC) was used for the modelling process. The *Course* variable was binarized so that the reference was the contrast group: binary variables *CS* (1, for *Course* = "CS"; 0 in other cases) and *Law* (1, for *Course* = "Law"; 0 in other cases)

1 *Except for question 6 where we employed six-point scale (from 0 – agree with the contrary opinion to 5 – strongly agree).*

were created. The *Year* variable was transformed to take values from 0 to 4 so that the coefficients and threshold coefficients of the model would offer a meaningful interpretation. After this transformation, *Year* can be interpreted as 'completed year of studies' instead of 'current year of studies'.

Then, for each question, all potential independent variables (*Gender*, *CS*, *Law*, and *Year*) and interactions between *Year* and *CS*, and *Year* and *Law* were included in the input of the backward stepwise method. To test whether fear of cybercrime increases punitiveness, the same procedure was used to create an additional model for question 9 (Q9; *Punitiveness towards cyber-criminals*), but in this case, the responses to Q1 (*Fear of cybercrime*) were included as an additional (numerical – with an assumption of interval character of the Likert scale) potential explanatory variable.

The final models were selected by comparison based on the AIC, log-likelihood, and significance testing of model coefficients. We did not assume a specific significance level for the variables, such as 0.05, since the use of this type of heuristic cannot be considered valid (Goodman, 2008; Wasserstein et al., 2019; Wasserstein & Lazar, 2016). Instead, we recognised the basis for considering a given relationship to be stronger the lower the *p*-value, and weaker, but not nonexistent, when the *p*-value is high, e.g. 0.1.

5 SURVEY FINDINGS

As shown in Table 1, there are noticeable differences between the means in at least two subgroups for most of the questions. The most noticeable differences in the means are for Q8 (*Free access to cybersecurity*) and Q4 (*Focus on the crimes of the powerful*). In some cases, one group differentiates itself relative to the similarity of the other two, such as in Q3 (*Approval of hacktivism*) or Q1. It is noteworthy that the attitude towards copyrights and free access to cybersecurity held by students of computer science is unenthusiastic, and they were more supportive of hacktivism. Law students are the least likely to place a higher value on cybercrimes by states and large corporations and to consider internet control excessive.

The coefficients and their *p*-values for each of the 10 final ordinal regression models are included in Table 2. Each model was tested for proportional odds assumption using the omnibus Brant test. In no case were there strong reasons for rejecting the assumption, as the lowest *p*-values were 0.10 (for Q4) and 0.12 (for Q3), and in the remaining cases p-values ≥ 0.15. The most interesting finding of the study is that at least a variable related to the field of study appears directly, or as an interaction item, in each of the constructed models. The strength, direction and significance of the influence of studying computer science or law majors vary considerably depending on the question being modelled. However, the mere presence of the aforementioned variables in the considered models provides a rationale for acknowledging the influence of the field of study on attitudes towards cybersecurity.

Law as a stand-alone variable (apart from interaction) was included in as many as eight models, with *p*-values lower than 0.13 in each, lower than 0.05 in six, and lower than 0.02 in five. Its strongest positive effect appeared to occur in

the model for Q2 (*Guesstimations*; in the model for Q9 its positive effect is offset by the interaction with the year of study), while the strongest negative effect of this variable occurs in the model for Q4 [in the Q6 (*Cyberterrorism less dangerous*) and Q8 models the mentioned interaction phenomenon occurs]. Less frequently included is the impact of the variable *IT*, which as a stand-alone variable occurred in four models, with *p*-values each time less than 0.08, and in two cases less than 0.02. The strongest positive impact of this variable can be seen in Q3 and the strongest negative impact in Q8. The variable *Year* as a stand-alone was included in four models (*p*-values less than 0.13 in each case and less than 0.04 in three cases) and as an interaction component in five models (six coefficients in total; *p*-values less than 0.08 in each case and less than 0.05 for four coefficients). This indicates that attitudes towards some cyber security issues are shaped throughout the studies, but in different ways from different majors.

Table 1: Responses by major – mean scores

Statement		Contrast	CS	Law
1.	The internet is not a safe place for children and youth.	3.53	3.18	3.54
2.	Each download of an unauthorized copy of a movie incurs a loss on the side of the film producer as high as the price for legal access.	3.43	2.65	3.45
3.	Hacking could pursue legitimate goals and be justified.	3.74	4.22	3.69
4.	Combating internet crime should focus on personal data abuse by huge corporations and illegal activities of the states rather than concentrate on hacker groups and pirate websites.	3.96	3.63	3.27
5.	In the name of combating cyberterrorism, those at power excessively monitor users' activities.	3.59	3.73	3.29
6.	Cyberterrorism is not as dangerous as traditional terrorism.	2.26	2.30	2.00
7.	Some internet users pose as juveniles under the age of consent and hold erotic conversations with interested adults. Then, they arrange a meeting together, which provides the police with an opportunity to arrest the potential paedophile. What is your opinion about the actions of such "paedophile hunters"?2	4.02	3.82	3.75
8.	Cybersecurity including antivirus software should be available for free to all internet users.	4.48	3.27	3.75
9.	Cybercriminals should be prosecuted more efficiently and deserve harsher penalties.	3.86	3.50	3.77
10.	While the internet pervades all areas of life, 'cybercrime' as a separate term becomes meaningless in modern society.	2.92	2.77	2.36

2 *For this question, the possible answers were respectively strongly disapprove (1), disapprove (2), etc.*

Table 2: Ordinal regression models

	Threshold coefficients	CS	Law	Year	Male	Interaction terms
Q1. Fear of cybercrime	1|2 - 3.37 2|3 - 1.48 3|4 - 0.56 4|5 1.55	- 0,40 ° (0.071)	-	-	- 0.32 (0.149)	-
Q2. Guess-timations	1|2 - 2.63 2|3 - 1.54 3|4 - 0.86 4|5 0.82	-	0.61 ** (0.008)	- 0.15 * (0.039)	- 1.37 *** (< 0.001)	-
Q3. Approval of hacktivism	1|2 - 2.60 2|3 - 1.10 3|4 - 0.21 4|5 1.32	0.52 ° (0.053)	- 0.41 (0.124)	0.16 * (0.026)	0.54 * (0.017)	-
Q4. Focus on the crimes of the powerful	1|2 - 3.98 2|3 - 2.01 3|4 - 0.87 4|5 0.49	-	- 1.11 *** (< 0.001)	-	-	CS:Year -0.22 ** (0.003)
Q5. Worries over surveillance	1|2 - 3.22 2|3 - 1.31 3|4 0.12 4|5 1.43	-	-0.54 * (0.016)	-	0.81 *** (< 0.001)	-
Q6. Cyber-terrorism less dangerous	0|1 - 2.55 1|2 - 0.66 2|3 0.46 3|4 1.19 4|5 2.55	-	-1.07 * (0.012)	-	-	Law:Year 0.23 * (0.048)
Q7. Support for paedophile hunting	1|2 - 3.68 2|3 - 2.50 3|4 - 1.23 4|5 0.45	-	- 0.35 (0.113)	-	- 0.53 ** (0.007)	-

Q8. Free access to cybersecurity	1|2 - 4.40 2|3 - 3.16 3|4 - 2.50 4|5 - 1.27	- 1.02 *** (< 0.001)	- 1.53 ** (0.004)	- 0.15 (0.129)	- 1.36 *** (< 0.001)	Law:Year 0.30 ° (0.069)
Q9. Punitiveness towards cyber-criminals	1|2 - 3.82 2|3 - 2.67 3|4 - 0.74 4|5 0.78	- 1.01 * (0.016)	0.99 * (0.040)	-	- 0.46 * (0.048)	CS:Year 0.24 ° (0.071) Law:Year - 0.31 * (0.013)
Q10. Term "cybercrime" meaningless	1|2 - 1.27 2|3 0.27 3|4 1.07 4|5 2.63	-	-	0.19 * (0.024)	-	Law:Year - 0.27 *** (< 0.001)

*° p < 0.1; * p < 0.05; ** p < 0.01; *** p < 0.001; precise p-values are reported in brackets.*

Taking the issue of interactions between the year and the major further, they indicate a different relationship between responses to a given question and the year of study for specific majors. The interaction terms provided interesting conclusions. In the model for Q10 (*Term "cybercrime" meaningless*), the variable *Year* has a positive effect for both the contrast group and the computer science students, while for the law students this effect is negative and weaker, or absent. This model indicates a greater tolerance for the concept of cybercrime among law students than in the other two groups, perhaps increasing over years of study. In the model for Q9, in turn, interactions indicate that with the progress of study, the initially lower punitiveness of computer science students and the higher punitiveness of law students gradually gravitate towards the punitiveness of the contrast group, which is constant over time. In the case of law students, it even turns out to be lower than that of the contrast group near graduation. The phenomenon of levelling the initial attitude during law studies is also indicated by the models for Q6 and Q8. This leads to the conclusion about the influence of the study period on the formation of some views on cybersecurity. In the model for Q4, the effect of the *Law* variable is negative and constant, while the negative effect of the *Year* variable is present only for computer science studies.

Table 3: Ordinal regression model – fear and punitiveness

	Threshold coefficients	Q1. Fear of cybercrime	Law	Male	Fear:IT	CS:Year	Law:Year
Q9. Punitiveness towards cyber-criminals	1|2 - 2.09 2|3 - 0.86 3|4 1.14 4|5 2.73	0.54 *** (< 0.001)	0.92 ° (0.057)	- 0.34 (0.140)	- 0.35 *** (< 0.001)	0.30 * (0.013)	- 0.32 * (0.010)

*° p < 0.1; * p < 0.05; ** p < 0.01; *** p < 0.001; precise p-values are reported in brackets.*

Table 3 presents an additional model for Q9 with the responses given to Question Q1 as the numerical explanatory variable. Proportional odds assumption could be held (*p*-value of the omnibus Brant test = 0.27). As can be seen, the fear of cybercrime has a very significant and powerful effect on cyber-punitiveness. Each additional point in the responses to the fear question shifts the distribution of the dependent variable by +0.54. This effect is much weaker (+0.19) for computer science students. Importantly, an *ANOVA* of the two optimal models for Q9 (including Q1 as the independent variable and lacking it) indicates a strong preference for the extended model (*p*-value < 0.001). This implies that the fear of cybercrime variable carries important information related to cyber-punitiveness.

6 DISCUSSION

The purpose of this research was to investigate how the perception of some controversial issues varies across perspectives of law and information technology. The results have indicated that in several instances the study major differentiated student's attitudes towards cybercrime. Distinct normative (law students) and expert (computer science students) approaches to cybercrime are manifested with high significance as far as piracy, hacking, and internet safety are concerned. Wall's

(2008) four narratives or syntactic and semantic approaches distinguished by McGuire (2018) do not only constitute disparate frames of reference in the debate on cybercrime, but also effectively generate different attitudes towards various controversial issues. The accounts of cybercrime by these groups are not merely two ways of telling the same story. They involve different moral judgements and vary in the appraisal of the facts and the assessment of risks.

All in all, the computer science students expressed a less dramatic view on internet security and hacking. This observation should be read together with the findings by Virtanen (2017) and De Kimpe et al. (2021) that confidence in one's computer skills or perceived knowledge of online safety lowers their fear of cybercrime. Self-selection processes may be involved. Technology-savvy students see the internet as a domesticated place and rarely define it through the lens of urban legends and media scares. By virtue of their computer skills alone, those respondents stood closer to the perpetrators of technologically advanced cybercrimes and were more likely to challenge the negative presentations of hackers or hacktivists. Both could be an object of admiration, if not for political reasons, then at least in acknowledgement of their technical finesse (Wall, 2008). For each group, the support for hacktivism was much higher than in any previous studies (Yar & Steinmetz, 2019: 55–58).

Since the surveillance and data misuse by the corporate and state actors take non-obvious and intangible forms, the computer science students were expected to appreciate these problems to a fuller extent than their peers from other courses. However, only the group of future lawyers differed in their attitudes toward surveillance, which they were more likely to accept. At the same time, they were most focused on the crimes of less powerful actors, while that focus grew over time in computer science students. Considering Dinev (2008), who linked internet literacy with increased government intrusion concern and lowered perceived need for surveillance, one has to conclude that the effects noted to indicate the existence of factors exerting a countervailing influence.

Legal education focuses on procedural safeguards, and, perhaps as a result, future lawyers were more likely than other respondents to express concerns about paedophile hunting (although this effect is not highly significant). At the same time, they were less likely to be concerned about cyber-surveillance. Law students were far less concerned about cybercrimes of the powerful, which was surprising, even though the white-collar criminality remains largely underrepresented in law school curriculums (Friedrichs, 2009). Those entering law school are characterized by significantly higher cyber-punitiveness, which declines rapidly over the course of their studies to reach levels lower than the humanities students at the end of their studies. The conservative vision of intellectual property embraced by the existing regulation might explain relatively high support of 'guesstimations' by law students and their reluctance towards 'socialized' cybersecurity (Mückenberger, 1971). The findings should be read together with the relatively lower actual use of pirate access reported by other Polish law students in a self-report study by Filiciak and Tarkowski (2018). As for other forms of deviation, those who download pirate files are also more likely to employ neutralization techniques, including denial of injury (Sykes & Matza, 1957). Given the doubts about exaggerated industry losses,

that excuse proves popular and convenient. Computer science students could, in turn, identify with the IT industry that develops antivirus software and appreciate its complexity. Conversely, the widespread demands for free cybersecurity in the contrast group correspond to students' low satisfaction with the protection of the public in cyberspace by state agencies observed by Conway and Hadlington (2018).

Generally, fear of cybercrime, as exemplified in the first question, was positively correlated with the punitive stance toward cybercriminals. In one case, that effect was significantly mediated by the study subject. Not only did the computer science students give a lower estimate of the risk of cybercrime, but they were also less likely to translate such worries into punitive demands. The accumulated knowledge of cyberspace might have encouraged them to support other, more cost-effective solutions. Once again, the calls for harsher punishments and more consequential enforcement appear to be a reaction less popular with those more familiar with the actual nature of the issue. It is an original finding since the impact of fear of crime on punitiveness is explored in the specific context of cyber criminology (see Armborst, 2017 and Meško et al., 2012 for a general overview). However, the model does not employ certain control variables, most notably the victimization experience, involved in the broader research into that relationship (Virtanen, 2017). Furthermore, the survey lacks international comparison (Dimc & Dobovsek, 2014).

Finally, most of the students, regardless of their stated major, approved the use of the term 'cybercrime'. Cyberterrorism was also considered a threat at least equal to terrestrial terrorism, with no differences established between the groups. We expected lawyers to question the novelty of cybercrime more frequently than both other groups. This assumption was based on McGuire's (2018) comparison of syntactic and semantic perspectives on cybercrime. In spite of law's focus on the socially constructed meaning attributed to the actions of cybercriminals rather than their instruments, the future lawyers mostly considered the term useful and, contrary to the other groups, they increasingly recognized its importance over the course of the study. Perhaps, lawyers, because of the nature of their educational process, which revolves around learning terms, may have a particular tendency to create concepts and feel compelled to use them. Although academic literature may question its terminological value (see: Grabosky, 2001; Palfrey, 2000), the concept of cybercrime remains popular with both laypeople and professionals.

7 CONCLUSIONS AND LIMITATIONS

We have surveyed students of various majors on the controversial issues in cybercrime and its control. Such a design seems appropriate to examine the relationship between the professional background and the views held on the number of relevant subjects. Moreover, the gathered data has provided insight into the link between the fear of cybercrime and punitiveness, offering a unique opportunity to take account of both the major and the year of study.

These results suggest the following warning: professionals who are to regulate, prosecute, and judge cybercrime hold far more traditional views on it than

individuals with a deeper knowledge of cyberspace, in which this crime occurs. Depending on the professional roles later adopted by lawyers and IT specialists, this could have unexpected consequences and lead to disagreements. Since computer science knowledge is instrumental to the prevention and investigation of cybercrime, the reconciliation of the two perspectives appears necessary. On practical grounds, introductory courses of law for computer science students, and vice versa, could increase mutual understanding between the representatives of both perspectives. Moreover, the disparate results in the contrast group call public support for at least some rules and policies into question. Demands for unrestricted access to internet security, punitiveness towards powerful cybercriminals, and approval of paedophile hunting were higher among students familiar with neither law nor computer science. Regardless of whether the future policy will aim to meet the expectations of the general public or follow the voices of experts, some levels of discontent are expected on either side.

There are some important limitations of the presented study. The most significant issue is the sample, which cannot be considered random. Therefore, the results of the study, though valid for students who use social media, cannot be extrapolated to the entire population. Furthermore, one has to bear in mind the simplified construction of the questionnaire, which is based on single-item unidimensional scaling. Most complex theoretical constructs cannot be represented by a one-item scale in a comprehensive way (McIver & Carmines, 1981). It should be noted, however, that in some cases single-item scales suffice to measure some constructs (Bergkgkvist & Rossiter, 2007; Cunny & Perri, 1991) and, in such cases, multiple-item design can even be a worse option and could cause an increase of random error (Drolet & Morrison, 2001). Secondly, statistical validation of the one-item instrument is not possible without reference to data on the corresponding scale. In particular, it is not possible to determine a measure of the validity of the single-item scale (e.g. the calculation of Cronbach's alpha requires at least two items). Accordingly, no validation of the research tool was performed during the study. Moreover, the questionnaire featured fairly general statements, which included numerous terms that could be considered vague. The understanding of the same terms may have varied to some extent, depending on characteristics of the respondent. This possibly different interpretation of some of the terms used is an additional source of noise in the data and, in conjunction with the single-item nature of the questionnaire, suggests that the conclusions of the study should be interpreted with caution.

One further limitation is the limited set of control variables. The study would highly benefit from including controls for additional variables such as age or general worldview orientation. The study presented here does not account for the possible correlation between study programme and worldview identification, which were found to be an important factor in views on technology (Han et al., 2021). The omission of computer and internet use variables, which we mentioned in the description of the methodology, leads to the impossibility of statistically verifying whether, after isolating their influence, group membership remains a significant predictor of the views studied. The same applies to the extent to which these variables constitute the differentiating factor between the groups studied. In

this sense, the absence of these variables can be considered another limitation of the present study.

Finally, the use of a quantitative methodology can also be treated as a limitation. It is hence impossible to recreate the complete attitudes, including motivations and beliefs underlying the given responses. We use the independent variables (major and year of study) as a proxy for a much more complex process of professional socialization. This study does not take account of the ingroup differences that could be large between, e.g., the lawyers specializing in intellectual property or criminal law. We acknowledge that further, perhaps qualitative, research is needed to grant full insight into the perception of cybercrime including the four main narratives proposed by Wall (2008). It is also beyond the scope of this study to assess participants' awareness of the problems addressed. Along with the depth of the investigation, its thematical scope is by no means complete and covers only a thin selection of issues. The possible cross-country differences also deserve mention; Lawyers' opinions may vary across jurisdictions according to regulations in force. Computer scientists from developing countries could react to lower internet security, but also show higher approval of illicit practices due to the economical constraints of full legal use of the internet.

REFERENCES

Albrecht, H.-J. (2011). Editorial: Grooming, das Internet und die Schließung von Sicherheits- und Strafbarkeitslücken. *Monatsschrift für Kriminologie und Strafrechtsreform*, *94*(2), iii–vi. https://doi.org/10.1515/mks-2011-940201

Armborst, A. (2017). How fear of crime affects punitive attitudes. *European Journal on Criminal Policy and Research*, *23*(3), 461–481. https://doi.org/10.1007/s10610-017-9342-5

Banks, J. (2015). The heartbleed bug: Insecurity repackaged, rebranded and resold. *Crime, Media, Culture*, *11*(3), 259–279. https://doi.org/10.1177/1741659015592792

Bergkvist, L. I., & Rossiter, J. (2007). The predictive validity of multiple-item versus single-item measures of the same constructs. *Journal of Marketing Research, 44*(2), 175–184. https://doi.org/10.1509/jmkr.44.2.175

Bohannon, J. (28. 4. 2016). Who's downloading pirated papers? Everyone. *Science, 352*(6285), *508*–512. https://doi.org/10.1126/science.352.6285.508

Brands, J., & van Wilsem, J. (2021). Connected and fearful? Exploring fear of online financial crime, internet behaviour and their relationship. *European Journal of Criminology 18*(2), 213–234. https://doi.org/10.1177/1477370819839619

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*, *23*(1), 47–59. https://doi.org/10.1080/14616696.2020.1804973

Campbell, E. (2016). Policing paedophilia: Assembling bodies, spaces and things. *Crime, Media, Culture*, *12*(3), 345–365. https://doi.org/10.1177/1741659015623598

Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: Evaluating measures adopted by South Africa and other regional role players. *Comparative and International Law Journal of Southern Africa*, *44*(1), 123–138.

https://unisapressjournals.co.za/index.php/CILSA/article/view/11525
Chang, L. Y. C., & Poon, R. (2017). Internet vigilantism: Attitudes and experiences of university students toward cyber crowdsourcing in Hong Kong. *International Journal of Offender Therapy and Comparative Criminology*, *61*(16), 1912–1932. https://doi.org/10.1177/0306624X16639037
Cho, J., Ahmed, S., Hilbert, M., Liu, B., & Luu, J. (2020). Do search algorithms endanger democracy? An experimental investigation of algorithm effects on political polarization. *Journal of Broadcasting & Electronic Media*, *64*(2), 150–172. https://doi.org/10.1080/08838151.2020.1757365
Christensen, R. H. B. (2019a). Ordinal - Regression models for ordinal data: R package version 2019.12-10. *The Comprehensive R Archive Network*. https://CRAN.R-project.org/package=ordinal
Christensen, R. H. B. (2019b). Cumulative link models for ordinal regression with the R package ordinal. *The Comprehensive R Archive Network.* https://cran.r-project.org/web/packages/ordinal/vignettes/clm_article.pdf
Conway, G., & Hadlington, L. (2018). How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization. *Policing: A Journal of Policy and Practice*, *15*(1), 119–129. https://doi.org/10.1093/police/pay098
Cunny, K. A., & Perri, M. (1991). Single-item vs multiple-item measures of health-related quality of life. *Psychological Reports*, *69*(1), 127–130. https://doi.org/10.2466/pr0.1991.69.1.127
De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, *41*(8), 1796–1808. https://doi.org/10.1080/0144929X.2021.1905066
Denning, D. (2010). Terror's web: How the internet is transforming terrorism. In Y. Jewkes, & M. Yar (Eds.), *Handbook of internet crime.* Willan. https://doi.org/10.4324/9781843929338
Dimc, M., & Dobovšek, B. (2013). Perception of cybercrime by selected internet users in Slovenia and USA. *Journal of Criminal Justice and Security*, *15*(3), 338–356. https://www.fvv.um.si/rv/arhiv/2013-3/03_PerceptionOfCybercrime_2013_3-E.html
Dinev, T. (2008). Internet users' beliefs about government surveillance the role of social awareness and internet literacy. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences* (pp. 275–275). HICSS. https://doi.ieeecomputersociety.org/10.1109/HICSS.2008.357
Drahos, P., & Braithwaite, J. (2007). *Information feudalism: Who owns the knowledge economy?* (Paperback edition). The New Press.
Drolet, A. L., & Morrison, D. G. (2001). Do we really need multiple-item measures in service research? *Journal of Service Research, 3*(3), 196–204. https://doi.org/10.1177/109467050133001
Dubber, M., & Hörnle, T. (2016). *Criminal law: A comparative approach*. Oxford University Press.
Filiciak, M., & Tarkowski, A. (2018). Poland: Where the state ends, the hamster

begins. In J. Karganis (Ed.), *Shadow libraries: Access to knowledge in global higher education* (pp. 159–183). MIT Press.

Friedrichs, D. (2009). *Trusted criminals. White-collar crime in the contemporary society* (4th edition). Cengage Learning.

Garland, D. (2002). *The culture of control: Crime and social order in contemporary society*. University of Chicago Press.

Goodman, S. (2008). A dirty dozen: Twelve P-value misconceptions. *Seminars in Hematology*, *45*(3), 135–140. https://doi.org/10.1053/j.seminhematol.2008.04.003

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*, 13–20. https://doi.org/10.1007/s11416-006-0015-z

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social and Legal Studies*, *10*(2), 243–249. https://doi.org/10.1177/a017

Guzman, I., & Stanton, J. (2004). Culture clash! The adverse effects of IT occupational subculture on formative work experiences of IT students. In *AMCIS Proceedings* (pp. 3623–3629). Americas Conference on Information Systems. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=2033&context=amcis2004

Hadjimatheou, K. (2021). Citizen-led digital policing and democratic norms: The case of self-styled paedophile hunters. *Criminology & Criminal Justice, 21*(4), 547–565. https://doi.org/10.1177/17488958198809

Hampson, N. C. N. (2012). Hacktivism: A new breed of protest in a networked world. *Boston College International and Comparative Law Review*, *35*(2), 511–542. https://heinonline.org/HOL/P?h=hein.journals/bcic35&i=515

Han, H., Park, S., & Lee, K. (2021). Does political orientation affect the evaluation of artificial intelligence?. *Asia Marketing Journal, 23*(2), 50–67. https://doi.org/10.53728/2765-6500.1180

Holt, T. J. (2016). Situating the problem of cybercrime in a multidisciplinary context. In T. J. Holt (Ed.), *Cybercrime through an interdisciplinary lens* (pp. 1–14). Routledge. https://doi.org/10.4324/9781315618456

Jarvis, L., Macdonald, S., & Whiting, A. (2015). Constructing cyberterrorism as a security threat. *Perspectives on Terrorism*, *9*(1), 60–75. https://www.jstor.org/stable/26297327

Jordan, T., & Taylor, P. A. (2004). *Hacktivism and cyberwars: Rebels with a cause?* Routledge.

Karagiannopoulos, V. (2021). A short history of hacktivism: Its past and present and what can we learn from it. In T. Owen, & J. Marshall (Eds.), *Rethinking cybercrime critical debates* (pp. 63–86). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-55841-3_4

Kranenbarg, M. W., & Leukfeldt, R. (2021). *Cybercrime in Context. The human factor in victimization, offending, and policing*. Springer.

Kukla-Gryz, A., Tyrowicz, J., & Krawczyk, M. (2021). Digital piracy and the perception of price fairness: Evidence from a field experiment. *Journal of Cultural Economics, 45*, 105–131. https://doi.org/10.1007/s10824-020-09390-4

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, *126*(106979). https://doi.org/10.1016/j.chb.2021.106979

Liang, L. (2018). India: The knowledge thief. In J. Karaganis (Ed.), *Shadow libraries: Access to knowledge in global higher education* (pp. 183–222). The MIT Press.

McCarthy, A. L., & Steinmetz, K. F. (2020). Critical criminology and cybercrime. In T. J. Holt, & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 601–621). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3

McGuire, M. (2018). Cons, constructions, and misconceptions of computer related crime: From a digital syntax to a social semantics. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 137–156. https://doi.org/10.21428/88de04a1.505d151e

McIver, J. P., & Carmines, E. G. (1981). *Unidimensional scaling*. SAGE.

Meško, G., Šifrer, J., & Vošnjak, L. (2012). Punitiveness, victimization and fear of crime of criminal justice students – Results from a web survey. *Journal of Criminal Justice and Security*, *14*(1), 75–96. https://www.fvv.um.si/rV/arhiv/2012-1/05_Mesko_Sifrer_Vosnjak.pdf

Mertz, E. (2007). *The language of law school: Learning to "think like a lawyer"*. Oxford University Press.

Mousley, M. C. (2003). Peer-to-peer combat: The entertainment industry's arsenal in its war on digital piracy. *Villanova Law Review*, *48*(2), 667–696. https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1329&context=vlr&httpsredir=1&referer=

Mückenberger, U. (1971). Legitimation durch Realitätsverleugnung: Am Beispiel Privatautonomie. *Kritische Justiz*, *4*(3), 248–268.

Nussbaum, B., & Udoh, E. S. (2020). Surveillance, surveillance studies, and cyber criminality. In T. J. Holt, & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 155–182). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3

Norman, G. (2010). Likert scales, levels of measurement and the "laws" of statistics. *Advances in Health Sciences Education*, *15*(5), 625–632. https://doi.org/10.1007/s10459-010-9222-y

Palfrey, T. (2000). Surveillance as a response to crime in cyberspace. *Information & Communications Technology Law*, *9*(3), 173–193. https://doi.org/10.1080/713670494

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

Prislan, K., & Bernik, I. (2013). Socio-psychological implications of cyberterrorism. *Journal of Criminal Justice and Security*, *15*(3), 357–369. https://www.fvv.um.si/rv/arhiv/2013-3/04_SocipsychologicalImplicationsOfCyberterrorism_2013_3.pdf

Puneßen, A. (2017). Blue Whale – Mythos oder Realität?. *Kinder- und Jugendschutz in Wissenschaft und Praxis*, *62*(4), 162–167.

R Core Team (2020). *R: A language and environment for statistical computing*. R Foundation for Statistical Computing, Vienna, Austria. https://www.R-project.org/

Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018).

Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security*, *78*, 198–211. https://doi.org/10.1016/j.cose.2018.06.006

Richards, I., & Wood, M. A. (2018). Hacktivists against terrorism: A cultural criminological analysis of anonymous' anti-IS campaigns. *International Journal of Cyber Criminology*, *12*(1), 187–205. https://doi.org/10.5281/ZENODO.1467895

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261–273. https://doi.org/10.1109/TDSC.2015.2410795

Romagna, M. (2020). Hacktivism: Conceptualization, techniques, and historical view. In T. J. Holt, & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 743–769). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3

Rosenbaum, H. J., & Sederberg, P. C. (1974). Vigilantism: An analysis of establishment violence. *Comparative Politics*, *6*(4), 541–570. https://doi.org/10.2307/421337

RStudio Team (2020). RStudio: Integrated Development for R. RStudio. PBC. http://www.rstudio.com/

Rüther, W. (2001). Cyber-crime: Neue Bedrohungs-Szenarien in der Kriminalpolitik. *Neue Kriminalpolitik*, *13*(3), 4–5.

Schlegel, B., & Steenbergen, M. (2020). brant: Test for parallel regression assumption. R package version 0.3.0. *The Comprehensive R Archive Network*. https://CRAN.R-project.org/package=brant

Smallridge, J., & Wagner, P. (2020). The rise of online vigilantism. In T. J. Holt, & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 1307–1331). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664–671. https://doi.org/10.2307/2089195

Szoszkiewicz, Ł. (2020). Internet access as a new human right? State of the art on the threshold of 2020. *Adam Mickiewicz University Law Review*, *8*. https://doi.org/10.14746/ppuam.2018.8.03

Tade, O., & Akinleye, B. (2012). 'We are promoters not pirates': A qualitative analysis of artistes and pirates on music piracy in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1014–1029. https://www.cybercrimejournal.com/pdf/Tade&Akenliye2012julyijcc.pdf

Vegh, S. (2003). *Hacking for democracy: A study of the Internet as a political force and its representation in the mainstream media* [Doctoral Dissertation]. University of Maryland. https://www.proquest.com/dissertations-theses/hacking-democracy-study-internet-as-political/docview/305325037/se-2

Venables, W. N., & Ripley, B. D. (2002). *Modern Applied Statistics with S* (4th edition). Springer.

Ventura, H., Miller, M., & Deflem, M. (2005). Governmentality and the war on terror: FBI project carnivore and the diffusion of disciplinary power. *Critical Criminology*, *13*, 55–70. https://doi.org/10.1007/s10612-004-6167-6

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology, and Law: An Interdisciplinary Journal of the Australian and New Zealand Association of Psychiatry, Psychology and Law*, *24*(3), 323–338. https://doi.org/10.1080/13218719.2017.1315785

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, *22*(1), 45–63. https://doi.org/10.1080/13600860801924907

Wasserstein, R., & Lazar, N. (2016). The ASA's statement on p-values: Context, process, and purpose. *The American Statistician*, *70*(2), 129–133. https://doi.org/10.1080/00031305.2016.1154108

Wasserstein, R., Schirm, A., & Lazar, N. (2019). Moving to a world beyond "$p < 0.05$". In *The American Statistician*, *73*(1), 1–19. https://doi.org/10.1080/00031305.2019.1583913

Wickham, H., François, R., Henry, L., & Müller, K. (2020). dplyr: A grammar of data manipulation. R package version 1.0.2. *The Comprehensive R Archive Network.* https://CRAN.R-project.org/package=dplyr

Wickham, H., Hester, J., & François, R. (2018). readr: Read rectangular text data. R package version 1.3.1. *The Comprehensive R Archive Network*. https://CRAN.R-project.org/package=readr

Wu, H., & Leung, S-O. (2017). Can Likert scales be treated as interval scales? — A simulation study. *Journal of Social Service Research*, *43*(4), 527–532. https://doi.org/10.1080/01488376.2017.1329775

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Yar, M. (2008). The rhetorics and myths of anti-piracy campaigns: Criminalization, moral pedagogy and capitalist property relations in the classroom. *New Media & Society*, *10*(4), 605–623. https://doi.org/10.1177/1461444807087911

Yar, M. (2009). Computer crime control as industry: Virtual insecurity and the market for private policing. In K. F. Aas, H. O. Gundhus, & H. M. Lomell (Eds.), *Technologies of insecurity: The surveillance of everyday life.* Routledge-Cavendish.

Yar, M., & Steinmetz, K. (2019). *Cybercrime and Society* (3rd edition). SAGE.

About the authors:

Andrzej Uhl is a postgraduate student in Criminological Research at the University of Cambridge. E-mail: andrzejuhl44@gmail.com

Andrzej Porębski is a PhD candidate in Law at the Jagiellonian University, Doctoral School of Social Sciences. E-mail: poreand@gmail.com