ALI, R., MCALANEY, J., FAILY, S., PHALP, K. and KATOS, V. 2015. Mitigating circumstances in cybercrime: a position paper. In Wu, Y., Min, G., Georgalas, N., Hu, J., Atzori, L., Jin, X., Jarvis, S., Liu, L. and Agüero Calvo, R. (eds.) *CIT/IUCC/DASC/PICom 2015*: proceedings of the 3rd International workshop on cybercrimes and emerging web environments (CEWE 2015), part of the 13th IEEE international conference on dependable, autonomic and secure computing (DASC 2015), co-located with the 15th IEEE international conference on computer and information technology (CIT 2015), the 14th IEEE international conference on ubiquitous computing and communications (IUCC 2015), and the 13th IEEE international conference on pervasive intelligence and computing (PICom 2015), 26-28 October 2015, Liverpool, UK. Los Alamitos: IEEE Computer Society [online], pages 1972-1976. Available from: https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.292

Mitigating circumstances in cybercrime: a position paper.

ALI, R., MCALANEY, J., FAILY, S., PHALP, K. and KATOS, V.

2015

Mitigating Circumstances in Cybercrime: a Position Paper

Raian Ali, John McAlaney, Shamal Faily, Keith Phalp, Vasilios Katos
Faculty of Science and Technology, Bournemouth University, UK
{rali, jmcalaney, sfaily, kphalp, vkatos}@bournemouth.ac.uk

***Abstract*— This paper argues the need for considering mitigating circumstances in cybercrime. Mitigating circumstances are conditions which moderate the culpability of an offender of a committed offence. Our argument is based on several observations. The cyberspace introduces a new family of communication and interaction styles and designs which could facilitate, make available, deceive, and in some cases persuade, a user to commit an offence. User's lack of awareness could be a valid mitigation when using software features introduced without a proper management of change and enough precautionary mechanisms, e.g. warning messages. The cyber behaviour of users may not be necessarily a reflection of their real character and intention. Their irrational and unconscious actions may result from their immersed and prolonged presence in a particular cyber context. Hence, the consideration of the cyberspace design, the "cyber psychological" status of an offender and their inter-relation could form a new family of mitigating circumstances inherent and unique to cybercrime. This paper elaborates on this initial argument from different perspectives including software engineering, cyber psychology, digital forensics, social responsibility and law.**

Keywords—mitigating circumstances; cybercrime; cyberspace.

I. INTRODUCTION

Mitigating circumstances in criminal law are conditions which lessen the degree of responsibility of an offender. Adapted from the UK Criminal Justice Act, this includes cases such as an intention to cause less harm than the harm actually caused, lack of premeditation, mental disorder or disability, provocation, self-defence, a misbelief of doing a merciful job and age. Mitigating circumstances could have different forms depending on the offence. For example, in a robbery case it relates to the value of items stolen, the intimidation caused to the victims and whether the motivation is desperation or need.

In cybercrime, we argue that a new range of mitigating circumstances would emerge if we accept an association between the design of the medium, i.e. the cyber space, and the cyber behaviour of an offender. We observe that the cyber design could drive certain behaviours leading to committing an offence. This also includes the case when the design does not do enough precautionary procedures to reduce the likelihood of a cybercrime or to reduce the effect. Some cyber designs utilize motivational approaches, similar to those in games, gamification [2] and persuasive technology [3], aiming to improve the engagement of users and while doing that a user would be heavily immersed or tempted towards certain rewards or achievement creating deviant and criminal behavior.

We advocate the role of software in enacting countermeasures against a pathological or problematic usage style. Recent studies have advocated the need for warning messages and labels to users on their usage style which could be addictive [1], i.e. excessive, compulsive, impulsive and hasty. Such a usage style could be detected early on so that certain precautionary procedures could be taken by the software to prevent possible deviant behaviors. To maintain users' experience, these approaches are advised to take a persuasive approach towards a behavior change to a healthier usage style [4, 29]. That is, while certain applications of persuasive approaches drive a pathological usage, corrective and protective software could bring that back to a desired status using, similarly, a persuasive approach as a counter measures.

Mitigating circumstances concern also the mental status of the person committing an offence. The online disinhibition effect [5], for example, is a reason for a cyber-behaviour which does not follow or reflect the actual values of users and their behaviour in the real world. This gap between the online and actual self may be especially pronounced if the online platform creates a sense of anonymity. Research suggests that the less likely people feel they are to meet an online contact in person the more likely they are to present an online image that differs from their offline self [14]. The difference in behaviours on both worlds makes it challenging to judge how an "online self" represents an "actual self" and this, consequently, introduces a space for a mitigating circumstances claim. In the case of social media it has been argued that the accumulation of information individuals post online become a social avatar [15]. Indeed, as predicted by social compensation theory certain people with limited social skills in person will seek compensation online by being overly open and social [16], which could at a certain point lead to irresistible impulse to get recognition and actin hasty style accepting the risk of committing an offence.

The two aspects, i.e. the cyber design and the cyber psychological aspects, converge in the case when the offender is immersed in the online space which is designed following a persuasive and engaging style without proper cautions and awareness raising mechanisms, to an extent where the cyber behaviour is not entirely a conscious decision. Thus a committed crime would be counted on the online-self and seen as a result of a pathway facilitated by the design of cyber space and the cyber-psychological status of an offender. An example is a social network user who posts abusive and possibly illegal pictures or comments via a persuasive design which makes that doable in a one-click style after being overwhelmed with a high volume of social information for several hours.

This paper raises a debate whether mitigation circumstances need to be considered in cybercrime. We study different facets of the argument including the role and social responsibility of a cyber design, the effect of cyber psychological status of an offender, the digital forensics and law aspects and an analogy to similar legal debates in traditional crimes.

II. CYBER DESIGN AND MITIGATING CIRCUMSTANCES

While manufacturers of media known for their dual use and association with deviant behaviour have already recognized their social responsibility in that regard, the cyber world design is still at the first stages in accepting that responsibility. For example, alcohol, tobacco and gambling industries put an age restriction and warning labels to make it clear that they could lead to addictive behaviour and consequences. Tests for alcohol on drivers are enshrined by law while we do not have a test for a cyber-user who is heavily immersed in a cyber-interaction for hours where the possibility to make mistakes is often higher. Age, expertise in IT, personality traits, the cyber behaviour and vulnerability to follow a deviant behaviour are all elements which may form such a test.

As noted by McKenna [13] online and offline interactions differ in terms of pacing and timing. The social interaction in the cyber space and its concrete nature as well as speed and volume may introduce criteria different from those we use to judge people offence cases committed in person and this could be a basis for a mitigating circumstances claim. In cyber interactions, regretting and trying to compensate an offence may not be, in some cases, possible and this might be surprising to users who possesses a limited understanding of technology. The same reason could lead to offences that cause harm at a scale which was not speculated by the offender. For example, once a picture or a comment is posted online, others could share it and this makes it hard to apologize or ask for conflict resolution and compensation in a classical way. The offender was unsure or with limited awareness how people will share the comment and what the technology allows in that regard, e.g. delete with cascade for the shared versions.

As commented previously, one of the goals of many online platforms is to create an immersive environment that heavily engages the user, through use of a range of techniques including gamification [2] and persuasive technology [3]. As such it is important to consider the psychological state known as flow which results after being influenced by such immersion. This is characterised by an experience of high but subjectively effortless attention to a task accompanied by a sense of control, loss of self-awareness and altered perceptions of time and enjoyment [22]. This phenomena has been studied in relation to a range of activities including video gaming where it has been found to be associated with physiological changes [23], supporting the view that flow is a distinct psychological state. Flow is often discussed in positive terms as something which benefits an individual who is engaged in a task, however it has also been noted that those in a flow state can experience impaired risk awareness and be more likely to engage in risky behaviour [24]. It could be argued that many online platforms actively aim to create a flow state in users, and in doing so it may be that they are also inadvertently increasing the risk of that user engaging in inappropriate or illegal behaviour. It has been further argued that experiencing a flow state can become addictive [25], which could contribute to hasty and compulsive online actions that may be criminal in nature.

As a social responsibility, we argue that the cyber design would need to be equipped with precautionary procedures and corrective measures to reduce the possibility and alleviate the side effects of a cybercrime. The lack of these mechanisms could make a basis for a mitigating circumstances claim. In the same time, the cyber design would need to provide mechanisms to detect the validity of a mitigating circumstance claim and produce evidence. This also introduces the dilemma of having users acting in a way that leads to a generation of that evidence and concealing their intentional, deliberate and pre-planned offences. The cyber space is a medium which could detect and react and this is a unique feature in comparison to other media and platforms for crimes and offences. While alcohol cannot warn a person of a possible consequence of committing an offence under intoxication, software can alert a user of the risks of ending up with a cyber-offence in certain usage contexts. That is, the intelligence and interactivity of the cyber space make it a more powerful medium to detect and act, proactively and reactively, with regards to cybercrimes and their forensics.

III. CYBER PSYCHOLOGY OF MITIGATING CIRCUMSTANCES

There is psychological research to support the view that the characteristics of online environments may influence the behaviour and decision making processes of individuals, leading them to engage in actions that they would not otherwise do. An example of this can be seen with people, many of them lacking in technical knowledge, who faced criminal prosecution after using LOIC software to participate in denial of service attacks against the Church of Scientology. Interviews with these individuals suggest that they were deliberately mislead by some members of hacktivist collectives on how likely it was that they could be identified [17]. This demonstrates a factor which may be especially pertinent to online behaviour and cybercrime, which is that when individuals are in a new or unfamiliar environment they are particularly susceptible to informational influence [18].

In the absence of established norms of cyber behaviour, individuals will look to each other to determine how to act. As a consequence individuals may come to misperceive how morally acceptable their actions within the online environment will be seen by the wider society. For instance an individual who becomes part of an online group and witnesses other members posting inappropriate images, such as incidents of revenge porn, may reach a warped view of considering these actions as acceptable practice. Similarly, an individual participating in an online group that shares pirated material may rely on the information provided by other group members to come to a determination of how acceptable this activity is. Group interactions facilitated by social media and Internet communication may lead to further decision making biases that the individual is unaware of. Individuals are known to make riskier decisions when they are in a group as opposed to when they are alone [19]. However, they also often under-estimate the influence that the group is having upon them [20].

The perception created by some online platforms that individuals are anonymous, or at least difficult to identify in real life, may lead to divergence from the real life decision making outcomes. In essence, the perception of anonymity leading to unobservability creates an inverse panopticon effect. In offline social systems individuals are aware that negative behaviours or attitudes may lead to social sanctions, such as for example exclusion from a group or disapproval from peers. If an individual believes that they are unlikely to experience social sanctions as a result of their (mis)perception that they are anonymous, they are more likely to lose self-control [21]. Given the wide number of social rules which individuals have to conform to, it is not perhaps surprising that they take the opportunity to break some of these rules when they feel they can do so with no consequences. It may also explain why online identity appears to be so highly valued by some online users, and why doxing (revealing an individual's offline identity) is seen in some online platforms to be one of the worst actions that can be carried out [17]. Embedding warning labels into online systems that prompt users to consider if their actions are as anonymous as they think make them give more consideration to otherwise hasty online actions.

The concept of mitigating circumstances is closely related to diminished responsibility concept in murder which mainly considers cases where the offender commits a crime because of a medically recognized condition, e.g. depression, epilepsy and paranoia. Diminished responsibility is a topic that is widely debated in both psychology and the legal profession, although there is a lack of consensus on how it should be defined and operationalized [26]. A common example of when diminished responsibility may be put forward by a defence team is alcohol intoxication, as in an individual should be held less responsible for actions conducted whilst they were intoxicated and incapable of a rational decision making process. There has naturally been much debate within the legal system as to how valid this defence is and how it should be implemented. One argument that has been put forward is that diminished responsibility should be judged on whether the individual would have still committed the crime had they not been intoxicated. If this is deemed to be unlikely then diminished responsibility may be considered to be a factor. A similar question could be asked in cases of cybercrime, as in whether an individual would have behaved in the same way if they were not acting online.

Diminished responsibility may also be deemed to be applicable is the presence of a mental disorder such as schizophrenia. This is relevant in light of recent debates around problematic internet use, or digital addiction, and whether this can be considered a mental disorder [27]. The most recent version of the Diagnostic and Statistical Manual (DSM) of the American Psychiatric Association list internet addiction as disorder in need of further investigation, but does not currently include it in the main list of mental disorders [28]. It should be acknowledged that the DSM is not widely used as a diagnostic tool within Europe. Nevertheless it is an influential publication, and the placement of digital/ internet addiction within it will inevitably have implications for the acceptance of compulsive internet use as a mitigating circumstance.

IV. Digital Forensic and Mitigating Circumstances

Information was persistently difficult to define and understand; quite unsurprisingly it took many years to discover that information is just another quantity in Physics, just like mass and heat are. This discovery is attributed to Bekenstein, a theoretical physicist who has contributed to identifying the relationship between information and gravitation. As such, an average cyber user may find it difficult to comprehend the potential power of information and the harm that it can cause if misused especially for new technology or new cyber features introduced without a proper management including raising awareness of the potential for making a crime. Hence, the forensics for cybercrimes and mitigating circumstances would not only need to look for the culpatory evidence but also its context including the behaviour, intention, the cyber psychological status of the users and familiarity with the cyberspace and actions taken.

Traditionally, and during an investigation of incident, investigators are less concerned about the culpability of individuals than they are about how culpatory evidence is and whether it supports (inculpatory evidence) or contradicts (exculpatory evidence) some theory or hypothesis. A hypothesis might state the individual associated with the incident, such that inculpatory evidence indicates a person's guilt, while exculpatory evidence indicates innocence [8].

While software engineering and cybersecurity communities have considered how investigators might be better supported by processes or tools, their focus has been on establishing provenance. As such, it is implicitly assumed that the behaviour of any subject is observable [9] and, when building forensic ready systems, forensic requirements and arguments are associated with potential crime scenes and hypotheses [10]. However, a subject's mitigating circumstances might be such that his motivations or intentions are neither observable, nor readily associable with culpatory or inculpatory evidence.

In lieu of evidence of culpability from forensic evidence, investigators need to rely on the design and implementation of some artefact to determine whether or not some agent is worthy of blame, should this be the basis of some hypothesis under investigation. In theory, the data used to build user and design models of an artefact might be useful for establishing culpability, and how warranted mitigating circumstances might be. Unfortunately, this is often difficult because user models often assume blameless users, and design models are similarly designed based on error-free software and hardware [11].

To establish whether some product was fit for a person's use, it needs to be put in context. However, as the forensic ergonomics community [12], have found, attributing culpability still remains challenging. The more complex a system is, the more responsibility is likely to be split among multiple agents. As a result, the lack of direct link between an action and a resulting harm means an agent's contribution may only be a rough estimate. As [12] also suggest, designing for security also means designing for secure outcomes. Consequently, should a subject's actions contribute to cybercrime then the violation may make them appear more culpable than they actually are.

V. CONTRIBUTORY NEGLIGENCE ARGUMENT

The concept of mitigation circumstances is common within academic circles. It often used to consider more favourably the performance of students. In the process of considering a mitigating circumstances claim, the evaluators apply a judgement that attempts to consider whether their circumstances, e.g., illness or personal conditions, had a detrimental effect upon their performance. If so, the evaluators may suggest acting more leniently, e.g. by giving a deadline extension. We note above that the immersion aspects might be considered as mitigating circumstances for cyber offences. For example, there are suggestions that one's norms become adjusted by the continued exposure to an online environment. An analogy to that is how a driving style may alter after some hours of motorway miles so that risks are undermined and the perception of the road and other cars becomes different. Similarly, we have argued earlier that a continued use of software and being immersed in the cyber world have an impact on the judgment that users make especially when being in groups [20].

Another debate is that the system or environment itself, in some ways invites the deviant behaviour. This is historically a controversial view, and the use of contributory negligence to dismiss cases often tends to be derided. An extreme, but well-known example, was where a rapist was merely fined rather than jailed because the judge decided that the scanty attire of the victim was 'contributory negligence', and had, to some extent, 'invited the crime'. Although this was a prevalent view in the 1960s and somehow 1970s, such comments are now considered as archaic [6, 7]. However, just because we accept, rightly, that the clothing worn by a rape victim should not be seen as an excuse for an abhorrent crime, one has to bear in mind that for many who commit cybercrimes, the sense of having a tangible victim is already much reduced, and, therefore, a small difference in the system's attractiveness to the crime may be a factor in its likelihood.

In addition, in England, it is still the case that although a case may not be typically denied on the grounds of contributory negligence, such arguments are still used to reduce the amount of damages paid out to victims, where there actions are seen in some way negligent. Classic examples include where drivers have been injured in an accident, but as they were not wearing a seatbelt, damages or 'pay-outs' to them were reduced significantly. Similarly, historically in the US, reductions were made on the grounds of contributory negligence to motorcyclists who had not been wearing helmets. Negligence is factored in most sectors were contractual agreements exist. In banking for instance, a customer may not be compensated if their ATM card is stolen and they admit that their PIN was written down and placed close to the card.

Taking this analogy back to software and cyber systems, one might argue that if we do not do absolutely everything we can to deter the potential cyber criminals from their actions, then we are indeed, in some small way negligent, particularly if it could be shown that by taking some precautionary actions this could be deterred. Note that software is naturally a medium that can, as suggested in our work on labelling [1], be at the very least reactive to behaviour, and ideally pro-active, in adapting such that it alerts or better deters the user from acting inappropriately.

VI. CONCLUSION AND FUTURE WORK

In this position paper, we argued the need to consider mitigating circumstances in cybercrime and discussed the concept from different perspectives. Our argument is based on several observations in which the committed crime is driven, facilitated or at least allowed with no precaution by the cyber design and also by the peer pressure and social interaction online. This calls for cyber designs which are intelligent and socially responsible to minimize the chance and alleviate the effects of a cybercrime and also to generate evidence when a mitigating circumstances claim is made. The dual use of these research findings is a dilemma of mitigating circumstances and diminished responsibility claims and could be seen differently in different legal frameworks. This makes it hard to generalize results. It also introduces the dilemma of a cybercrime committed in a cyber and globalized space while members are physically located in different areas and following different laws and value systems. This paper was mainly meant to raise the question and initiate a research on the topic.

Acknowledgement. We thank Neil McDonald for reviewing the paper from a legal perspective.

REFERENCES

[1] Ali, R., Jinag, N., Phalp, K., Muir, S., McAlaney, J. The Emerging Requirement for Digital Addiction Labels. The 20th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2015). Essen, Germany. March 2015.

[2] Deterding, S., Dixon, D., Khaled, R., Nacke, L. From game design elements to gamefulness: defining gamification. The International Academic MindTrek Conference: Envisioning Future Media Environments. pp. 9–15 (2011).

[3] Fogg, B. J. Persuasive technology: using computers to change what we think and do. Ubiquity 2002. Dec 2002.

[4] Jiang, J., Phalp, K., Ali, R. Digital Addiction: Gamification for Precautionary and Recovery Requirements. The 20th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2015). Essen, Germany. March 2015.

[5] Suler, J. The online disinhibition effect. Cyberpsychology & behavior 7, no. 3 (2004): 321-326.

[6] Radford, J. Contributory Negligence or Being a Woman?. in P. Scraton and P. Gordon (eds), Causes for Concern: Questions of Law and Justice, Pelican: London. (1982)

[7] Rumney, P., Fenton, R. A. Comment, Judicial Training and Rape, The Journal of Criminal Law, 75, (2011): 473-481

[8] Rowlingson, R. A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence 2, 3 (2004), 1–28.

[9] Casey, E., Back, G., and Barnum, S. Leveraging CybOX to standardize representation and exchange of digital forensic information. Digital Investigation 12, 1 (March 2015), S102–S110.

[10] Pasquale, L., Yu, Y., Salehie, M., Cavallaro, L., Tun, T. T., and Nuseibeh, B. Requirements- driven adaptive digital forensics. In Requirements Engineering Conference (RE), 2013 21st IEEE International (2013), pp. 340–341.

[11] Cooper, A., Reimann, R., Cronin, D., and Noessel, C. About Face: The Essentials of Interaction Design. John Wiley & Sons, 2014.

[12] Gilson, R. D., and Facci, E. L. Forensic aviation human factors: Accident/incident analysis for legal proceedings. In Handbook of Aviation Human Factors, J. A. Wise, V. D. Hopkin, and D. J. Garland, Eds. CRC Press, 2010.

[13] McKenna KYA, Green AS, Gleason MEJ. Relationship formation on the Internet: What's the big attraction? Journal of Social Issues. 2002; 58(1): 9-31.

[14] Underwood JDM, Kerlin L, Farrington-Flint L. The lies we tell and what they say about us: Using behavioural characteristics to explain Facebook activity. Computers in Human Behavior. 2011; 27(5): 1621-6.

[15] Brunskill D. Social media, social avatars and the psyche: Is Facebook good for us? Australasian Psychiatry. 2013; 21(6): 527-32.

[16] Barker V. Older Adolescents' Motivations for Social Network Site Use: The Influence of Gender, Group Identity, and Collective Self-Esteem. Cyberpsychology & Behavior. 2009; 12(2): 209-13.

[17] Coleman EG. Hacker, hoaxer, whistleblower, spy : the many faces of Anonymous. Verso, 2014.

[18] Festinger L. A theory of social comparison processes. Human Communications. 1954; 7: 117 - 40.

[19] Wallach MA, Kogan N, Bem D.J. GROUP INFLUENCE ON INDIVIDUAL RISK-TAKING. Journal of Abnormal Psychology. 1962; 65(2): 75-&.

[20] Darley JM. Social Organization for the Production of Evil. Psychological Inquiry. 1992; 3(2): 199-218.

[21] Mason KL. Cyberbullying: A preliminary assessment for school personnel. Psychology in the Schools. 2008; 45(4): 323-48.

[22] Bruya B. Effortless attention : a new perspective in the cognitive science of attention and action. The MIT Press, 2010.

[23] Harmat L, de Manzano O, Theorell T, Hogman L, Fischer H, Ullen F. Physiological correlates of the flow experience during computer game playing. International Journal of Psychophysiology. 2015; 97(1): 1-7.

[24] Schuler J, Nakamura J. Does flow experience lead to risk? How and for whom. Appl Psychol Health Well Being. 2013; 5(3): 311-31.

[25] Csikszentmihalyi M. Flow: The classic work on how to achieve happiness. Rider, 2002.

[26] Patil P, Rasquinha N. Diminished Responsibility In England And Wales: Historical And Current Perspectives. European Psychiatry. 2013; 28: 1.

[27] Moreno MA, Jelenchick L, Cox E, Young H, Christakis DA. Problematic internet use among US youth: a systematic review. Arch Pediatr Adolesc Med. 2011; 165(9): 797-805.

[28] American Psychiatric Association. Diagnostic and statistical manual of mental disorders. 2013.

[29] Thaler, R.H, Sunstein, C.R.: Nudge: Improving Decisions About Health, Wealth and Happiness. Yale University Press (2009).