INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 12, December 2023, pp : 235-239

e-ISSN : 2583-1062

Impact Factor : 5.725

CYBERPSYCHOLOGY AND ORGANIZED CYBERCRIME

Siddhi Bhasin[1], Dr. Charulata M. Kulkarni[2]

[1]Student, OP Jindal University, India.

[2]Assistant Professor, RMD Sinhgad Management School Kondhapuri, Tal. Shirur, Pune, India.

ABSTRACT

Cyberpsychologists and enterprise cybersecurity practitioners both stress the need to better understand how people interact with technology to create a stronger cybersecurity posture. They point to statistics showing that most breaches involve some sort of human misstep. According a report "74% of all breaches include the human element, with people being involved either via error, privilege misuse, use of stolen credentials or social engineering." Cyberpsychology is the study of the impact of emerging technology on human behavior. Cyberpsychologists provide insight into the intersection between humans and technology. This article serves as an overview and introduction to the discipline of cyberpsychology. Research and scholarship on the interaction of technology and human behavior through the lens of psychology has exploded, and relatedly the field of cyberpsychology.

Keywords: Cyberpsychology, cyber crime, internet, computer, social media.

1. INTRODUCTION

We have entered a new era in the field of psychology. Approximately 58% of the world's 7 billion people use the internet. The creation and sharing of information and ideas through social media has become a primary form of communication and information exchange. The combination of new technologies and "digital natives", that is, those who have grown up using the internet, computers, and mobile devices, is transforming the ways in which we learn, communicate, and socialize in the world. Social interactions, communication, and patterns of behavior in almost every sphere of life have been transformed. Electronic messaging has become the medium of choice for business and personal communication.

Greater convenience and extended information access related to "always on" connectivity and mobility have led to technology entering the private spheres of human lives. Users have a "technological intimacy" with many devices, carrying and using them wherever they go. Traditional hierarchical structures have flattened, accessibility to political institutions has been enhanced, and the ability to build personal and professional networks has surged. The use of mobile devices alone has decentralized communication networks and has the potential to facilitate groups of unrelated people at a moment's notice.

With the growth of new technologies and an increasingly interconnected world, the field of cyberpsychology has emerged as a unique discipline. Defined as the discipline of understanding the psychological processes related to, and underlying, all aspects and features of technologically interconnected human behavior, cyberpsychology includes multiple and intersecting disciplines such as human–computer interaction, computer science, engineering, and psychology. Advances in global communication and technologies, social media and networking sites, and technological intimacy created through developments such as the iPhone have created shifts in perspectives and behaviors.

Welcome to the emerging realm of 'cyberpsychology'. It already exists, albeit on the fringes of the cybersecurity world, and arguably it demands more attention (and more budget) from those with the most to lose from cybercrime. Cyberpsychology recognizes that the most used channel for cybercrime – the so-called 'attack vector' – is not based on digital technology or network design flaws but on the usually unwitting behaviour of people inside the organisation.

As Huffman says, hackers "don't want to go toe-to-toe with your firewall. They don't want to challenge your antivirus, because that's very difficult, not when they can exploit the largest vulnerability on every network on the planet right now -- that's us, people. Cybercriminals are not just hacking computers; they are hacking humans. Because ... unlike computers, we actually respond to propaganda."

Psychology gets at why humans do what they do, says Huffman, founder of cybersecurity services firm Handshake Leadership. There are multiple psychological reasons why people fall for phishing schemes and other hacker scams, according to Huffman, Hadlington and others looking at the role of human nature in cybersecurity.

Cybercrime has been on the rise since the internet became widespread in the mid-1990s, and it saw massive increases during the COVID-19 pandemic across the globe (Buil-Gil, Zeng and Kemp, 2021; Lallie et al., 2021). For the purpose of this article, we take the comprehensive definition of cybercrime presented by McGuire and Dowling

(2013), which is used as a primary criterion to record cybercrime data in the UK and elsewhere. Cybercrime is defined as a set of offenses that are either dependent on, or enabled by, computer systems, computer networks or other information and communication technologies (ICT). While 'cyber-dependent crimes' are those offenses that can only take place through digital systems, and include crimes such as malware, hacking, phishing and denial of service attacks; 'cyber-enabled crimes' comprise more traditional crime types which have increased in scale or reach due to the use of digital technologies, such as cyber-enabled fraud and other cyber-enabled predatory or personal offenses (McGuire and Dowling, 2013).

The ongoing increase in cybercrime is known to affect individual victims as well as businesses and public organizations, and all types of victims can suffer severe financial, reputational and emotional harms (Button et al., 2021; Henson, Reyns and Fisher, 2016; Ignatuschtschenko, 2021; Paoli, Visschers and Verstraete, 2018). While all types of victims are exposed to cybercrime, some estimates indicate that the financial losses faced by organizations may greatly exceed that suffered by individual victims. As an example, in 2017, the UK Annual Fraud Indicator estimated that frauds were responsible for £140 billion losses for the private sector, £40 billion losses for the public sector and £6.8 billion losses for individuals (Crowe, 2017). In the period November 2021-November 2022, 39,758 cybercrimes and frauds suffered by organizations were reported to the UK Action Fraud, with reported losses exceeding £2.2 billion, while incidents reported by individuals totaled 345,510 incidents and £2 billion in losses (City of London Police, n.d.). These are likely to be underestimates, with UK survey data indicating that only 8% of companies that suffer cybersecurity incidents report these to public authorities (Kemp et al., 2021). Furthermore, some have noted an increase in the frequency and harms of cases in which organizations, both legitimate businesses and organized crime groups, are directly and indirectly involved in cybercrime, either as offenders or facilitators (Broadhurst et al., 2014; Leukfeldt et al., 2020; Musotto and Wall, 2022; UNODC, 2022).

There has been a wealth of research on cybercrime victimization and offending in the last 20 years. Researchers from a variety of disciplinary fields undertake cross-cutting studies to better understand the technical (e.g., Gupta et al., 2020; Lezzi, Lazoi and Corallo, 2018), legal (e.g., Clough, 2015), psychological (e.g., Attrill-Smith and Wesson, 2020), financial (e.g., Anderson et al., 2013) and social aspects of cybercrime (e.g., Yar, 2013). Here we synthesize the main themes of criminological research on cybercrime, to enable readers to familiarize themselves with this emerging subfield of criminological scholarship and to introduce the need to dedicate more efforts to investigating the 'organizational' aspects of online crime.

If these varieties of cyber attack and the psychological patterns that underlie them seem arcane, it is worth remembering that cybercrime is ubiquitous, it affects everyone whether directly or indirectly, and it happens every day, every minute. So it is unsurprising that the list of organisations seriously damaged by cybercrime in 2023 alone is very long, and includes among thousands of cases many universities, government agencies including health authorities, along with Deutsche Bank, ChatGPT, UPS, Reddit, T-Mobile, Uber, Western Digital, AT&T, Pepsi, Paypal, the social media menace formerly known as Twitter as well as cybersecurity specialists Verizon and even somewhat ironically BreachForums which is a large marketplace for, yes, hacked data.

According to IBM the average cost to an organisation of an individual data breach is now $4.4m. That cost eventually passes to the wider economy: in its latest annual 'Cost of a Data Breach' survey, IBM also says that over half of companies have increased prices as a result of data breaches. If psychology has anything to contribute when it comes to limiting those costs, perhaps businesses and governments should be paying attention.

The challenge for cyberpsychology is the challenge of shaping human behaviour. The benefit of making people less prone to online error is great, but so is the difficulty of achieving it. As organizations have already learned, when you tell people not to do a thing they quickly become desensitized to the message, and just go on doing it. But cyberpsychologists do have some tools at their disposal, and they are based on understanding the behavioural weaknesses that cybercriminals exploit.

The cyberpsychologist might also look at the complexity of organisations and their cyber defences, and how to simplify these defences. In cybersecurity complexity spells trouble, because complex systems usually cause people to develop ad hoc 'workarounds', and workarounds are untested and not secure. Complex passwords are a case in point: we are frequently told that a password has to be long, both upper and lower case and including non-standard characters because that is hard to crack. But it is also hard to use so people end up writing the passwords down or storing them in insecure files. In practice a password of three short random words is long enough and strong enough for most purposes. These approaches are only the beginning for cyberpsychology – but at least they are a beginning. If organisations are going to get to grips with the extraordinary threat that cybercrime now poses, they are also going to need to move beyond today's almost total reliance on technology-as-defence.

Online Behavior and Personality

As individuals increasingly engage with the world through cyber technology in many areas of their lives, research on online behavior has also increased. These investigations include the ways in which people behave in cyberspace relative to face-to-face and the relationship between personality characteristics and a range of online behavior such as social media preferences and use, dating activity, cybersecurity measures, and online bullying.

People often behave differently in cyberspace versus offline. The online disinhibition effect is a term used to describe the lowering of psychological restraints in online social environments, reflected in reduced behavioral inhibitions and lowered regard for behavioral boundaries in cyberspace. The lack of eye contact and anonymity in cyberspace are two factors that reduce inhibitions and result in cyber-specific behavior, including self-disclosure.

The relationship between individual personality and online behavior such as cybersecurity measures has also been studied. Cybersecurity is an area that continues to benefit from psychological research findings.

For example, using a regression model, found that conscientiousness, agreeableness, openness, emotional stability, and risk-taking propensity explained a significant amount of the variance in information security awareness, with conscientiousness the most important contributor, followed by agreeableness and risk-taking propensity. Similarly, characteristics such as rational decision-making and extraversion were found to be significant unique predictors of careful computer security behaviors (i.e., device securement, updating) after controlling for demographic factors such as age and gender.

Other investigations have included exploring social psychological factors that contribute to online criminal activity and ways in which fraudsters deceive their victims, cyberattacks, and cyber terrorism, the social psychological impact of cybercrime victimization, factors that influence privacy precautions, such as perceptions of risks and rewards; and evidence-based practices for helping to raise public awareness and promote related precautions.

An area of online behavior which has received attention in both the popular press and among researchers is cyberbullying. Cyberbullying is defined as “willful and repeated harm inflicted through the use of computers, cell phone, or other electronic devices”. The dissemination of sexually explicit images or video of an ex-partner via the internet is a particular form of cyberbullying, otherwise known as “revenge porn.”

Social Media Use and Psychological Functioning

The relationship between social media use and psychological functioning, especially anxiety and depression, has demonstrated varied results. Some studies have found that social media use has a positive impact on well-being by facilitating online social connections and/or enhancing physical (offline) interactions. For example, Facebook use is associated with perceptions of online social support. Such support seems to be related to number of Facebook friends, which, in turn, is associated with reduced stress and feelings of well-being. Having a larger Twitter social network and being more active in that network seems to be particularly helpful to people with lower levels of in-person social support in alleviating depressive thoughts and symptoms. Relatedly, online self-disclosure seems to moderate the relationship between excessive smartphone use and stress and loneliness with significant reductions in loneliness and stress for excessive smartphone users who communicate their feelings and anxieties online, but increased stress for those who engaged in little online self-disclosure.

Games and Gaming

The development and use of video games has grown within the last few decades. Technically, “video games” are electronic games that use visual feedback.

The ESA reports that 93% of American households own a smartphone and, of those, almost half of them use it to play video games. “Gamer” communities have grown, allowing people to interact in a shared space regardless of geographical location. “Digital games” is a broader term referring to any game that is played in an electronic platform including games used for learning or health.

Telepsychology

Telepsychology is defined as the provision of psychological services using telecommunication technologies. Telecommunication technologies include, but are not limited to, telephone, mobile devices, interactive videoconferencing/webcam, email, chat, text, and internet (e.g., self-help websites, blogs, and social media).

These communications may be synchronous, with multiple parties communicating in real time (e.g., interactive videoconferencing, telephone), or asynchronous (e.g., email, online bulletin boards, storing and forwarding of information). Technology-based mental health interventions have the potential to transform access for those limited geographically such as persons living in rural areas, by medical condition, financial constraint, or other barriers.

Artificial Intelligence

Developments in simulated experiences and environments via VR and AI have converged with clinical, diagnostic, and educational applications for a range of psychological and social issues. VR is an advanced form of human–computer interface that allows users to interact with and/or become immersed within a computer-generated simulated environment/virtual environment (VE). Real-time computer graphics and sensory input devices are utilized. Head-mounted displays and tracking systems are often employed to deliver computer-generated images and sounds in a virtual scene, similar to what one would see and hear in the real world. People act and respond to events and situations within VR as if these were real, also known as "presence". AI replicates or simulates human intelligence in machines whereby technological devices are programmed with the perception of a responsive being. AI includes virtual human agents such as animated avatars and robots. Immersive exposure experiences through VR and AI provide an opportunity to activate emotional and behavioral responses and modify them as needed (such as in the case of phobias and trauma/PTSD), or distract one from the real world (such as in the case of pain management).

2. CONCLUSION

The field of cyberpsychology will increasingly flourish as technology continues to develop and is utilized. Developments in cyber have had a profound impact on practically every aspect of human life, including education, healthcare, the workforce, and mundane activities such as shopping. Psychologists, through their training and skills, are uniquely positioned to be a force for innovation and good as we navigate this new world. Moreover, 21st-century science calls for psychologists to engage in interdisciplinary work with other professionals such as computer scientists, engineers, and bioinformatics experts. Psychologists and other social scientists must take the lead in providing the necessary infrastructure to allow cyberpsychology to flourish in the most scientific and ethical way possible with applications to solving real-world problems.

3. REFERENCES

[1] Argilés-Bosch, J.M., Somoza, A., Ravenda, D., and García-Blandón, J. (2020). An Empirical Examination of the Influence of E-Commerce on Tax Avoidance in Europe. Journal of International Accounting, Auditing and Taxation, 41, 100339.

[2] Back, S., Soor, S., and LaPrade, J. (2018). Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory. International Journal of Cybersecurity Intelligence & Cybercrime, 1(1), 40-55.

[3] Buil-Gil, D., Lord, N., and Barrett, E. (2021). The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. Victims & Offenders, 16(3), 286-315.

[4] Buil-Gil, D., Trajtenberg, N., and Aebi, M.F. (2023). Measuring Cybercrime and Cyberdeviance in Surveys. SocArXiv. https://doi.org/10.31235/osf.io/r8ygd

[5] Buil-Gil, D., and Saldaña-Taboada, P. (2022). Offending Concentration on the Internet: An Exploratory Analysis of Bitcoin-related Cybercrime. Deviant Behavior, 43(12), 1453-1470.

[6] Burruss, G.W., Howell, C.J., Maimon, D., and Wang, F. (2022). Website Defacer Classification: A Finite Mixture Model Approach. Social Science Computer Review, 40(3), 775-787.

[7] Correia, S.G. (2022). Making the Most of Cybercrime and Fraud Crime Report Data: A Case Study of UK Action Fraud. International Journal of Population Data Science, 7(1), 09.

[8] Del-Real, C., and Díaz-Fernández, A.M. (2022). Understanding the Plural Landscape of Cybersecurity Governance in Spain: A Matter of Capital Exchange. International Cybersecurity Law Review, 3, 313-343.

[9] Follis, L., and Fish, A. (2022). State Hacking at the Edge of Code, Capitalism and Culture. Information, Communication & Society, 25(2), 242-257.

[10] Gottschalk, P., and Hamerton, C. (2021). White-collar Crime Online: Deviance, Organizational Behaviour and Risk. Cham: Palgrave Macmillan.

[11] Gupta, B.B., Martinez Perez, G., Agrawal, D.P., and Gupta, D. (Eds.) (2020). Handbook of Computer Networks and Cyber Security: Principles and Paradigms. Cham: Springer.

[12] Holt, T.J. (2023). Understanding the State of Criminological Scholarship on Cybercrimes. Computers in Human Behavior, 139, 107493.

[13] Hou, T., and Wang, V. (2020). Industrial Espionage - A Systematic Literature Review (SLR). Computer & Security, 98, 102019.

[14] Ignatuschtschenko, E. (2021). Assessing Harm from Cybercrime. In P. Cornish (Ed.), The Oxford Handbook of Cyber Security (pp. 127-141). Oxford: Oxford University Press.

[15] Kemp, S. (2023). Exploring Public Cybercrime Prevention Campaigns and Victimization of Businesses: A Bayesian Model Averaging Approach. Computers & Security, 127, 103089.

[16] Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C., and Bellekens, X. (2021). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic. Computers & Security, 105, 102248.

[17] Musotto, R., and Wall, D.S. (2022). More Amazon than Mafia: Analysing a DDoS Stresser Service as Organised Cybercrime. Trends in Organized Crime, 25, 173-191.

[18] Nguyen, T., and Luong, H.T. (2021). The Structure of Cybercrime Networks: Transnational Computer Fraud in Vietnam. Journal of Crime and Justice, 44(4), 419-440.

[19] Poehlmann, N., Caramancion, K.M., Tatar, I., Li, Y., Barati, M., and Merz, T. (2021). The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review. In K. Daimi, H.R. Arabnia, L. Deligiannidis, M.S. Hwang and F.G. Tinetti, F.G. (Eds.), Advances in Security, Networks, and Internet of Things (pp. 377-395). Cham: Springer.

[20] UNODC. (2022). Digest of Cyber Organized Crime. Second Edition. Vienna: United Nations.

[21] Wall, D.S. (2021). Cybercrime aS A Transnational Organized Criminal Activity. In F Allum and S. Gilmour (Eds.), Routledge Handbook of Transnational Organized Crime (pp. 318-336). London: Routledge.

[22] Weulen Kranenbarg, M., Ruiter, S., and Van Gelder, J.L. (2021). Do Cyber-Birds Flock Together? Comparing Deviance Among Social Network Members of Cyber-Dependent Offenders and Traditional Offenders. European Journal of Criminology, 18(3), 386-406.

[23] Zeng, Y. (2021). Organising Insider Dealing in Financial Markets: Scripts and Networks. PhD thesis, The University of Manchester.