Social Psychology: An under-used tool in Cybersecurity

Helen Thackray, John McAlaney, Huseyin Dogan, Jacqui Taylor, Christopher Richardson
Faculty of Science and Technology
Bournemouth University, United Kingdom
{hthackray,jmcalaney,hdogan,jtaylor,crichardson}@bournemouth.ac.uk

In cyber-security the weakest link is often seen as the human factor. This has led to discussions about the optimal methods in preventing cyber security breaches. This paper proposes that the fusion of cybersecurity and social psychology can inform and advance attempts to educate those on both sides of the law. Awareness and education will lead to more effective communication between parties and greater understanding of the risks and consequences for cyber attackers and defenders alike.

Social psychology, cybersecurity, hacking, hacktivist, cyber-crime, social identity, group process.

1. INTRODUCTION

The development of tools that can help protect users, businesses and states online can also be used by those committing illegitimate activities. This can lead to a potential arms race with regards to attacking and defending online assets, with the advantage going to whomever has the most up to date tools. Social psychology research into human-computer interaction aims to give cybersecurity specialists a better understanding of hacktivism and cybercrime through engagement with people involved in such groups and understanding of group processes. This paper puts forward the need to investigate such methods, focussing on interdisciplinary fusion and advises caution in accepting the negative stereotypes as fact. It is evident that there are a number of young people engaged in hacking and hacktivism groups who are clever, skilled and passionate about their causes. It is better to act with such individuals to explore ways of bringing about positive change, than to leave them to become criminalised.

2. HACKERS, HACKTIVISTS AND MOTIVATION

Definitions and categorisations of 'hacker' have been contentious and the use has evolved over the last couple of decades. In this paper 'hacker' will refer to someone who gains access to a "computer system, regardless of motivation or the extent of the damage caused," (Seebruck, 2015:38). By understanding the social and psychological influences and motivations on individuals and groups it may be possible to identify common factors or behaviours that precede a cyber-attack.

Typologies for hackers have been created and updated throughout the history of the term (Chantler, 1996; Landreth, 1985; Seebruck, 2015; Taylor, 1999). Recent recommendations in hacker typologies have been made to include the increase in social and ideological motivations in hacking, incorporating those who are seen as 'hacktivists', also a contentious term but meaning a combination of 'hacker' and 'activist' (Krapp, 2005). This growth of social and ideological motivations have been attributed in part to the fact that a generation has been raised in a time of digital evolution and innovation (Seebruck, 2015), with increased user generated content and unrestrained communication increasing the confidence and perception of power individuals possess.

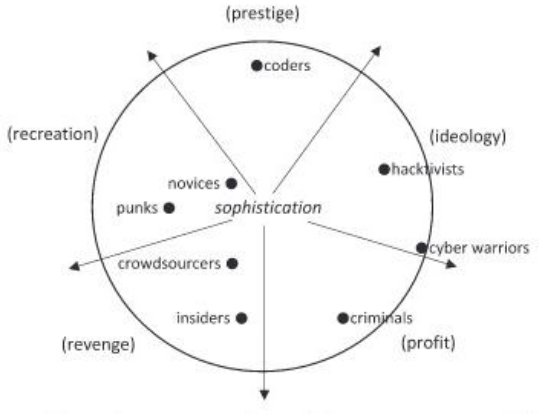

Figure 1: *Hacker Types. Nodes depict hacker types; Nodes nearer the edge are more sophisticated; regular text indicates hacker groups; parenthesised text indicates motivations (Seebruck, 2015).*

It has also been highlighted that there is a need for increased research on who is involved in hacking and their motivations. Greater understanding of the skills and motivations of cyber adversaries would "benefit a security industry that is over-dependent on technical solutions" (Glenny, 2011:269). The motivations of hackers have been redefined and updated (Seebruck, 2015:39) to include:

- Recreation: those who hack for pleasure, such as intellectual curiosity, thrill, or mischief;

- Prestige: non-material gains such as notoriety, the primary motivation of non-malicious coders (e.g. white hat hackers);
- Revenge: personal vengeance and larger social justice issues (e.g. online crowdsourcing movements);
- Profit: material gain, the primary motivation for criminals;
- Ideology: political or social activists and nationalists (attacks initiated by patriotic civilians or state-sponsored cyber warfare).

It should be noted that all of these motivations are related to social identity and group processes; the authority of a group should not be underestimated.

2.1 Group Processes and Collectives

While looking at the online influences and motivations, the effects of group processes on the individual must be considered. Intergroup attribution research (Hewstone & Jaspars, 1982) can help explain the achievements of group actions by hacktivism and other cyber adversarial groups in terms of strengthening individual members' beliefs that they are highly skilled and influential. This can lead members to conclude that the success of opposing groups is attributable to external circumstances and luck. This may encourage the group to carry out additional actions against other organisations, especially if that group identity is reinforced by media reporting. It has been observed that early news reports about Anonymous generally exaggerated the intensity of cohesiveness between group members and organisational structure of the group (Olson, 2012), which has then been a factor in the group becoming more cohesive and organised. The cohesiveness of hacker groups was affected by the shock of the "Sabu-tage" when a high status member of Lulzsec was exposed as having been an informant for the FBI. His information led to the arrests of prominent group members. There have been significant changes to the group behaviours since (Coleman, 2015), with greater antipathy of 'leader-fags', suspicion of new or unknown members, and those who seem to be desiring attention.

Hacker groups also experience indirect attacks, on group brand or reputation. It has been claimed by some Anonymous related Twitter accounts that multiple "ops" are false flag attacks, malicious efforts to undermine the successes and status of the hacktivist groups. By creating many different ops on social media, attackers of hacktivist groups weaken the power of numbers (which is a large part of Anonymous' success) and then use the failed ops as examples of how the hacktivist groups are declining and far less influential than they once were which would in turn affect their recruitment and membership.

3. SOCIAL PSYCHOLOGY AS A TOOL

Social psychological theories should be further examined to inform methods used to educate and communicate with these hacker communities and individuals. Cyberpsychology and social psychology both highlight the importance of not only what is said but how it is said as well (McMahon, 2016).

Generalised trust is believed to make a person more willing to engage in collective efforts and cooperate with other people (Gunnarson, 2014). In the context of hacking, there is usually a paranoid and suspicious mindset, so how do these groups establish trust? The online disinhibition effect is the removal or reduction of the social and psychological restraints that individuals experience in everyday face to face interaction (Suler, 2004, Joinson, 2007). It could be argued that anonymity and online disinhibition can be positive, allowing the internet to be an open place where individuals can be honest on subjects that they may otherwise not wish to be identified with. This privacy combined with openness is what many involved in hacking and hacktivism claim to want to protect.

Hacker groups have evolved on the internet, developing alternative ways to signal identity and status. These collectives subtly create the ingroup through methods based on knowledge (Bernstein et al, 2011). Online groups might be better understood as fluid collectives (Dobusch & Schoeneborn, 2015) rather than traditional groups. For example Anonymous use assertive speech to form identity, through established lines of communication that can be used by many individuals – it is the mode of communication that is significant not the speaker. They also use controversial control of group identity through methods such as doxing – showing that even anonymous group membership can be revoked (Dobusch & Schoeneborn, 2015).

4. CONCLUSION

There is currently a strong emphasis on teaching coding. By teaching individuals the skills that are essential in cyber hacking (regardless of intention), our research becomes all the more important. Not only do we need to teach coding but also about the risks and consequences of actions online. Global internet regulation is beyond our research, our focus is to help protect and educate users. By identifying groups and individuals at-risk of becoming involved in cyber-crime, campaigns on awareness and informed use can be targeted. The more that is known and shared about the functions and influences of these groups, the more prepared the next generation will be to make deliberate choices regarding HCI and online behaviour.

REFERENCES

Bernstein, M. S., Monroy-Hernandez, A., Harry, D., Andre, P., Panovich, K., Vargas, G. (2011) 4chan and /b/: An Analysis of Anonymity and Ephemerality in a Large Online Community. In: *Fifth International AAAI Conference on Weblogs and Social Media,* ICWSM, 50-57.

Bojarski, K. (2015) Dealer, Hacker, Lawyer, Spy: Modern Techniques and Legal Boundaries of Counter-cybercrime Operations. *The European Review of Organised Crime*, 2 (2), 25-50.

Coleman, G. (2014) *Hacker, hoaxer, whistleblower, spy: The Many Faces of Anonymous*. London: Verso.

Coleman, G. (2015) Epilogue: The State of Anonymous. In *Hacker, hoaxer, whistleblower, spy: The Many Faces of Anonymous*. London: Verso, 401-461.

Chantler, N. (1996) *Profile of a computer hacker*. Florida: Infowar.

Dobusch, L. & Schoeneborn, D. (2015) Fluidity, Identity, and Organizationality: The Communicative Constitution of Anonymous. *Journal of Management Studies*, 52 (8), 1005-1035.

Glenny, M. (2011) *Dark market: How hackers became the new mafia*. New York: Vintage.

Gunnarson, C. (2014) Changing the Game: Addiopizzo's Mobilisation against Racketeering in Palermo. *The European Review of Organised Crime,* 1 (1), 39-77.

Joinson, A. N. (2007) Disinhibition and the Internet. In: J. Gackenbach (ed). *Psychology and the Internet: Intrapersonal, interpersonal, and transpersonal implications* (2nd ed). San Diego: Academic Press. 75-92.

Krapp, P. (2005) *Terror and play; or what was hacktivism?*. Grey Room MIT Press, 21, 70-93.

Landreth, B., & Rheingold, H. (1985) *Out of the inner circle: a hacker's guide to computer security*. Bellevue, Washington: Microsoft Press.

Lapidot-Lefler, N., & Barak, A. (2015) The benign online disinhibition effect: Could situational factors induce self-disclosure and prosocial behaviors?. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 9 (2), 2-3.

McEvoy Manjikian, M. (2010) From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly*, 54, 381–401.

McMahon, C. (2016) Cyber-Psychology: The Key to Securing the Human Element in Your Organization. *Info Security Magazine,* available from: https://www.infosecurity-magazine.com/magazine-features/cyberpsychology-securing-human/, accessed 12/03/16.

Olsen, P. (2013) *We are Anonymous.* London: Random House.

Rogers, M. K. (2006) A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation,* 3 (2), 97-102.

Rogers, M. K. (2010) The psyche of cybercriminals: a psycho-social perspective. In: Ghosh S., Turrini E. (eds). *Cybercrimes: A Multidisciplinary Analysis*. Berlin: Springer, 217-35.

Seebruck, R. (2015) A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation,* 14, 36-45.

Suler, J. (2004) The Online Disinhibition Effect. *CyberPsychology & Behavior,* 7 (3), 321–326.

Taylor, P. (1999) *Hackers: crime in the digital sublime.* London: Routledge.