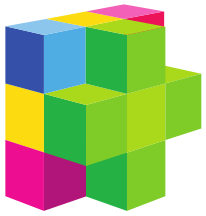
Sustainable
Society Network



WORKING PAPERS OF THE SUSTAINABLE SOCIETY NETWORK+
Vol. 3
February 2015

1st International Conference on Cyber Security for Sustainable Society

February 26-27th, 2015

Conference Proceedings

Digital Economy
Transforming Business and Society

 ISSN 2052-8604

Author

John McAlaney, Jacqui Taylor and Shamal Faily

Sustainable
Society Network

 ISSN 2052-8604

THE SOCIAL PSYCHOLOGY OF CYBERSECURITY

Abstract

As the fields of HCI, cybersecurity and psychology continue to grow and diversify there is greater overlap between these areas and new opportunities for interdisciplinary collaboration. This paper argues for a focus specifically on the role of social psychology in cybersecurity. Social psychological research may help explore the dynamics within online adversary groups, and how these processes can be used to predict and perhaps prevent cybersecurity incidents. In addition the issue of motivations of cyber adversaries and the social context in which they operate and will be discussed. Finally the benefits of the shared experience of psychologists and cyber security practitioners in addressing issues of methodology and conceptual development will be explored.

Scope of this Document

The scope of this document is to discuss and evaluate the role of social psychology in understanding the actions of cyber adversaries, and to evaluate how collaborative research might be used to improve approaches to prevention and mitigation.

Digital Economy Transforming Business and Society

Sustainable Society Network

The growth of social media provides cybersecurity actors, both adversaries and targets, with more ways to present themselves in terms of the motivations for their actions and their responses to incidents

As has been observed a limitation of research into information security behaviours of end-users is a lack of understanding of the social context in which these end-users operate – the same comment could perhaps be applied to cyber adversaries

TABLE OF CONTENTS

1 Background

Cybersecurity incidents extend beyond the technological aspects of the attack. Recent incidents involving large organisations such as Sony serve as examples of both the wider social causes and social consequences of cybersecurity incidents. The growth of social media provides cybersecurity actors, both adversaries and targets, with more ways to present themselves in terms of the motivations for their actions and their responses to incidents. This dialogue in turn contributes to the social and cultural context that cybersecurity actors operate within, and which in a case of reciprocal causality is also a determinant of their actions. The collective nature of some cybersecurity incidents and the social roles of those involved in cybersecurity incidents has become the focus of study and comment by anthropologists[1] and social media analysts[2], yet there remains a lack of research. A better understanding of the social factors of those who instigate cybersecurity incidents is important in a number of ways for the development of prevention and mitigation techniques.

Social psychology research focuses on how the behaviour and cognition of individuals is influenced by the real, imagined or implied presence of others[3]. As such it is one area of study that can be used to begin to explore the social psychological factors of cyber-adversaries. There is of course already a history of collaboration between psychology and computing through the interdisciplinary research conducted within Human-Computer Interaction (HCI), however it could be argued that the focus of this work has been more on the cognitive aspects of psychological processes rather than the social aspects. This paper will discuss and evaluate how social psychology research is currently incorporated into cybersecurity, and what further contributions the field may make for cybersecurity practice. This discussion will be arranged to reflect the conceptual model of the role of social psychology of cyber adversaries in cybersecurity that is shown in Figure 1, the case for which will be argued in the following sections. This will be followed by a discussion on directions for future research, and how the collaborative work of social psychologists and cybersecurity practitioners may further complement each field.

2 Group processes

When examining cybersecurity incidents it would appear that the actions of many cyber adversaries are group based in nature, as in the case of well-known hacktivist collectives such as Anonymous[4]. The activities of these groups often appear to be the result of conversations held on message boards such as 4chan or Internet Relay Chat (IRC)[1]. However it is important to note that as demonstrated in social psychology research there does not need to be actual contact between individuals for group processes to influence behaviour. As commented the imagined or implied presence of others can also influence individual behaviour[3].This may be particularly relevant to anonymous online discussions or the posting of messages on websites such as 4chan, where it may not be immediately clear to an individual if their actions are in fact being observed by others. In contrast to an offline situation such as a group activity in a physical room an individual who is acting online may have very little sense of how much of an audience they have, and what status within a group they have. In these situations the imagined or implied presence of others may become particularly pertinent.

Overall it could be argued that there are very few cybersecurity incidents that are instigated by entirely an individual without there being any influence of group processes, even when the individual is primarily responsible for the incident.

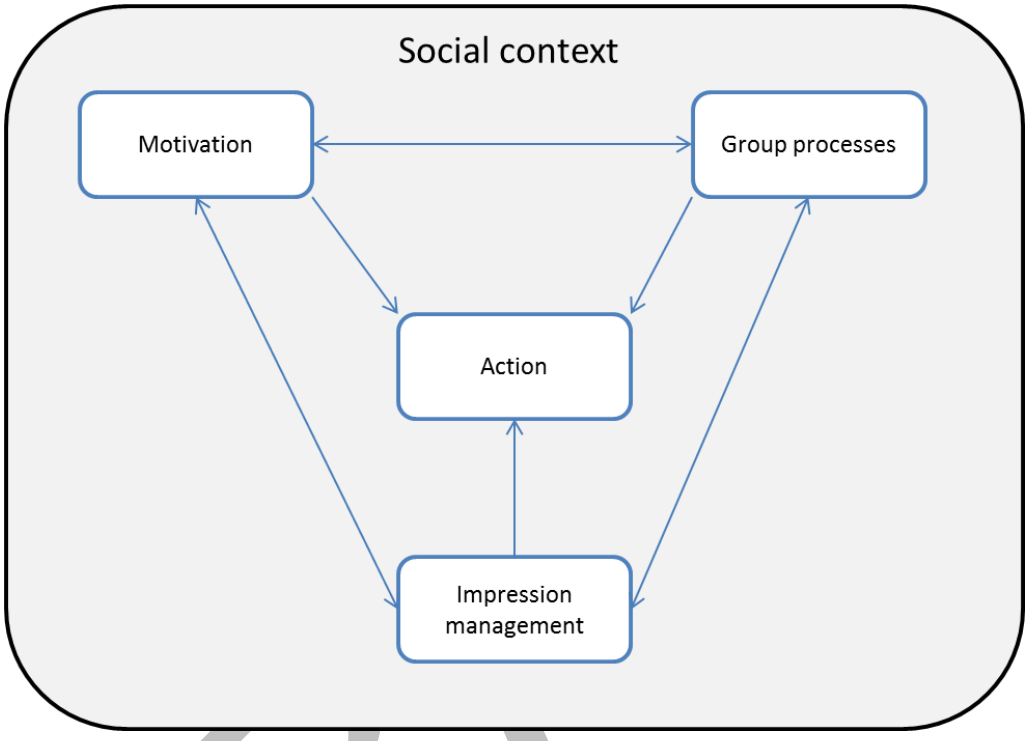


Figure 1: A conceptual model of the social psychology of cyber adversaries

When considering group processes social psychological research on social influence, attitude and behavioural dynamics is particularly relevant. In the case of Anonymous it has been stated that the majority of harm associated with some of the incidents was caused by a small number of technologically skilled individuals, though use for example of botnets[4]. There may have indeed only been a handful of people in this technologically skilled, smaller group but they were acting within a social context where group members were praising them and encouraging them to attack new targets. This type of positive reinforcement would be expected to increase the likelihood of individuals of the more technologically skilled group engaging in further, similar acts, as predicted by a multitude of social psychological theories of behaviour[3]. At the same time it is claimed[4] that members of the wider collective were manipulated by those leading the group action into believing that their actions using LOIC software was in fact what was primarily responsible for the incidents. In other words, social engineering was used within the group. By giving people the perception of having a role in the achievement of a goal the individual's sense of membership will be solidified, as predicted by social psychology research [5]. It would be of interest to explore how members of these groups would respond to the knowledge that they may have been manipulated by in-group members. As noted in psychology research people can respond negatively to the suggestion that

they are being manipulated in some way, a response known as reactance[6]. There have been some examples of this type of reaction within hacktivist groups. For instance the revelation that one especially prominent and respected member of Anonymous was in fact working undercover for the FBI appeared to cause serious distress to other group members, as well as bringing disruption to their activities[4].

In keeping with intergroup attribution research [7] the success of the group actions of collectives such as Anonymous could also have been expected to strengthen individual members' beliefs that they are highly skilled, and that any successes of opposing groups such as law enforcement are more attributable to external circumstances and luck. This process could lead to decision making biases within the group, and could be argued to have emboldened the group to take further actions against other organisations, in the erroneous belief that their risk of being individually identified by law enforcement was lower than it actually was. Indeed many of the main individual adversaries that orchestrated the incidents associated with Anonymous in the early days of the collective have now been arrested and prosecuted[4]. Linked to these decision making biases is the effect that media reporting could have on such groups. It has been commented that early news reports about Anonymous generally overstated both the level of cohesiveness between group members and organisational structure of the group[4]. The category differentiation model of social psychology[8] suggests that the simple act of an external entity identifying a group as being a group can increase the likelihood of individuals identifying themselves as group members. In addition it has been observed that self-esteem is in part derived from membership within groups [9], particularly when that group has been engaged in conflict with what is seen to be a larger oppressor. In order to protect the self-esteem gained from these group memberships individuals may react strongly to exclude anyone who is seen to be threatening the group norms or group cohesion. This may explain some of the tensions and intra-group conflicts that invariably seem to appear within any kind of online group or hacktivist collective, where it is common for splinter groups to form and target one another[1]. Monitoring these types of reactions could be used as an indicator of how cohesive a group is becoming, which in turn helps inform how likely they are to take collective action against a target. In order to help prevent future cybersecurity incidents the media could also, as argued by Rogers[10], take more responsible approach to the reporting of cybercriminals so as to avoid glamourizing individuals and setting them up as role models.

3 Impression management

As with any online relationship individuals may also engage in what is termed impression management, in which an individual may attempt to construct what they see to be a desirable image of themselves[11]. There can be several motivations behind impression management, including the desire to be liked and to appear competent, and of particular relevance perhaps to cyber adversaries, the desire to appear dangerous[12]. It has been noted that the depth to which individuals engage in online impression management is linked to how likely it is they think they will meet someone offline[13]. Given that those involved in the instigation of cybersecurity incidents are already motivated to conceal their identity due to the risk of being pursued by law enforcement it could be argued that such individuals are therefore particularly likely to engage in impression

management. However, there are added complications to understanding the role of impression management within online collectives. One of the websites associated with the growth of Anonymous and other cyber adversaries[1], 4chan, operates on a principle of anonymity. Users are not generally able to identify themselves when posting content or comments, and indeed users who do attempt to bypass this restriction are often met with harsh criticism for doing so[4]. This prevents individuals from building up a personal reputation or seeking fame or leadership roles. From a social psychological perspective this system of interaction is surprising, particularly in Western cultures which are characterised by individualism as opposed to collectivism[14]. As such it is an area which could be argued to be unchartered territory for social psychologists, and one which needs to be researched in much greater depth.

Groups can also engage in forms of collective impression management. It has been claimed for example that Anonymous engaged in impression management by overstating their capabilities to journalists[4]. The group also used sophisticated impression management techniques when targeting the Church of Scientology. The 'Message to Scientology' video that was posted on YouTube by the group stressed the severity of the threat they posed and how likely it would be that they would successfully shut down the Church of Scientology. This is consistent with Protection Motivation Theory[15], which states that individuals decide how to respond to a threat based on how severe that threat is perceived to be and how vulnerable they perceive themselves to be. The message also claimed that attempts to counter the actions of the group would be ineffectual. This reflects work into fear appeals that suggests that people are less likely to take action to protect themselves if they do not believe that they have the ability to do so[16]. Finally the group also made use of expectation management. It is stated in the video that they realise that they will not bring about an end to Scientology overnight, adding credibility to their claims of what they will achieve. Combined with the ominous background music and the voice synthesised narration the overall effect is a psychologically sophisticated video which aims to intimidate the opponent.

Linked to impression management is doxing, which refers to revealing an individual's real life identity, as well as possibly personal contact information such as their home address. The act of doxing someone is used as a weapon within these online communities that are based on anonymous participation[4]. The effort that is put into doxing another individual can be extensive, and in some cases involving collectives associated with cyber security incidents stems from intra-group conflict about the ideology, group identity and actions of the group[4]. Doxing raises a number of interesting and challenging questions from a psychological perspective. There can obviously be a number of real life consequences of being doxed, such as being targeted at home or being pursued by law enforcement. Yet there are also potentially psychological consequences. In offline forms of conflict a common goal can be dehumanise and depersonalise an opponent, such as for example in the oppression of dissidents in dictatorships[17]. In the case of doxing however the opposite is achieved, with the target's offline identity revealed. When this happens the person effectively has their ability to engage in impression management severely curtailed, since they no longer have the ability to control and alter what information about their identity they want to be disseminated. In light of the way in which the internet allows people to create an alternative identity it can be seen why robbing someone of this ability is perceived as one of the worst possible actions in some online communities. When planning how to dissuade cyber adversaries it may be that highlighting the risk of being doxed

could be an effective strategy. It may be the case that the potential loss of an online identity is so threatening to an individual that this is an effective strategy even when there is no possibility of the legal action being taken against the individual. Of course, this approach could raise a number of ethical questions.

4 Motivation

Group processes and impression management may determine the characteristics of a group or hacktivist collective and how they present themselves to society, but they do not in themselves predict the actions of the group. For this an understanding of motivation is needed. There are obvious financial motivations to cybercrime, but the reasons behind other cybersecurity incidents are not as apparent. Cyberwarfare, hacktivism and online social protest can all produce similar results and are not always easily to differentiate from one another. It can also be difficult to predict what will drive a group to move towards acts that are focussed on social protest. As has been commented the change in Anonymous from a group that was characterised by random actions and anarchy to one that engaged in active social protest and aided in supporting political protestors around the world was highly unexpected[1]. A better understanding of the motivations of those involved in these activities may be useful in distinguishing between cybercrime and online social protest, as well anticipating future actions. Alberici et al[18] argue that there are four motivations that drive people to collective action:

- Identification with a group which is involved in a conflict with a larger organisation
- Negative emotions arising from perception that the situations of one's own group is unfair
- A shared belief that through joint efforts the group will be able to achieve its goals
- The perception that core moral principles have been violated and that these must be defended and reinstated

These motivations would appear to be consistent with a number of cybersecurity incidents that could be termed hacktivism or online social protest. They may also be useful in developing a productive dialogue with online adversaries as to why an organisation is being targeted, and what actions might be taken to resolve the conflict between the adversaries and the target. This is not an approach that has been adopted particularly often in the past. Instead organisations such as the Church of Scientology have responded to situations involving cyber adversaries with a more confrontational approach[4], which could be argued to have fuelled further action by the cyber adversaries by reinforcing the motivations of the type identified by Alberici et al[18]. Referring back to the topic of reactance discussed above it has been noted that reactance is particularly pronounced when there is a perceived threat to personal freedom, which is known as the boomerang effect[19]. This fits with the motivations identified by Alberici et al[18], particularly if the freedom of information is viewed by the individual as being a core moral principle.

When viewing interviews of members of Anonymous and similar online groups one common theme appears to be a sense of anger[20]. At times this is directed towards specific organisations such as the aforementioned Church of Scientology, at other times it appears to be a more diffuse sense of

anger towards society in general. Whether or not the actions against an organisation are morally acceptable or not is a matter of the perspective of the individual. Whilst Anonymous have been implicated in cybersecurity incidents involving apparently random targets they have also taken part in actions such as providing internet access to protestors in Tunisia during the 2011 uprising[4], after the Tunisian government attempted to block all internet traffic within the country. Examples such as this suggest that there is more to some cybersecurity incidents than simply financial gain or criminal intent. Whilst the insights of forensic psychology and criminology will undoubtedly continue to be of great importance to the field of cybersecurity there is a need to better understand the social context and social psychology of cyber adversaries. One particular psychological phenomena which may be of relevance is cognitive dissonance[21], which refers to the tendency of people to avoid holding contradictory views or attitudes. By focussing on the greater good of battling perceived social injustice members of online groups may be able to justify to themselves the act of committing criminal acts. If this is the case then attempts to dissuade individuals from acting as cyber adversaries by highlighting the criminality of their behaviour may not be effective, as the individual has already processed and discounted that information.

There would though appear to be overlap between a genuine desire to achieve social change and to acting only for personal enjoyment, or for the lulz to use the language of some online groups. As previously commented this difference in the motivations of individuals has been a source of intra-group conflict[4], with disagreements over what the ideology and goals of the group should be. If as previously discussed individuals do derive their sense of self-esteem and identity from membership of such groups then it is understandable that a lack of agreement on the purpose of that group could lead to conflict. Attempts to deliberately create conflict within groups by provoking discussions around the goals of the group also appear to be evident within the communications of some groups. This could be trolling behaviours by individuals, or it may be more organised and deliberate efforts by other groups to create tensions. As has been observed a limitation of research into information security behaviours of end-users is a lack of understanding of the social context in which these end-users operate[22] – the same comment could perhaps be applied to cyber adversaries.

5 Future directions

It has been argued in this paper that a better understanding of the social psychological processes behind cybersecurity incidents will help inform prevention and mitigation approaches. However it has to be acknowledged that social psychological processes are not merely something which act upon cyber adversaries. As evident in many cybersecurity incidents cyber adversaries actively use social psychological principles in the form of social engineering as a tool with which to gain access to secure systems[23]. There are numerous examples of those who are extremely skilled social engineers and books on the topic of how to apply social engineering principles[23], although it could be commented that much of this is based on anecdotal evidence, case studies and observational research. There is less work which has investigated social engineering using an experimental approach. This could be a reflection of the challenges inherent in securing ethical approval for studies that use deception or other forms of participant manipulation. Similarly studies into security behaviour often rely on measurements of intended future behaviours, rather than the actual

behaviours themselves[22]. Direct observation of behaviour can lead to demand characteristics such as the Hawthorne effect, in which research participants alter their behaviour simply due to the fact that they know they are being observed by researchers. To avoid these effects it may be necessary to observe participants covertly, which can prompt ethical questions around informed consent.

Social psychologists may be able to aide in these methodological and ethical challenges. Deception and manipulation are part of many psychology studies, and as such the field has developed extensive guidelines on how these issues should be addressed[24]. Indeed, many of the ethical approval processes used in the UK could be said to have stemmed from psychological research, particularly those relating to the potential for psychological harm to participants. Being able to demonstrate that planned research is consistent with the recommendations of the British Psychological Society, the professional accreditation body for Chartered Psychologists, may help facilitate approval at the institutional level. The need to understand the psychological impact of social engineering has also been an unintended consequence of attempts to incorporate social engineering into `ethical hacking' methodologies. For example, Dimkov et al.[25] found that debriefing deceived security staff on social engineering tests was more stressful than carrying out the test itself. The risk was not identified when planning the test, despite the fact their methodology had been warranted as ethically sound.

One area of particular relevance to the understanding of social engineering is social marketing, which represents the interface between social psychology and consumer psychology. As in what could be termed commercial marketing the goal of social marketing is to bring about change, although for a social good rather than commercial profit. It has been noted that social marketing can be utilised to bring about behaviour change within organisations, specifically for cybersecurity related behaviours by end users. As Ashenden and Lawrence[22] comment simply raising awareness of security issues or changing attitudes, as has often been the goal of more traditional behaviour change strategies, does not necessarily result in behaviour change. Similarly the efficacy of attempts to modify cybersecurity behaviours through the use of fear appeals is inconsistent [7]. This has been the experience of psychologists working in the areas of health and social psychology[26], who have in turn also attempted to utilise social marketing to achieve long term behaviour change. The technique is related to the Nudge approach[27], which aims to encourage individuals towards sensible choices without actually removing options from them. Despite the adoption of the approach by a number of UK government bodies there are different views on how effective the Nudge approach actually is, although as has been observed both it and social marketing have the advantage of being relatively easily applied by those without expertise in social science[27].

It may be that by working jointly the fields of social psychology and cybersecurity are able to make a unique contribution to these types of approach. Social marketing is based largely upon the principles of commercial marketing, which were themselves informed by trial and error experience of what is successful and cost effective in the business world. Similarly it may be that further exploration of the experiences of social engineers could help inform better ways of implementing social marketing campaigns. Ultimately after all the goal of both companies and social engineers is to develop a relationship with the target and use this to prompt certain behaviours; just as for companies there are costs in terms of resources and potential risk to the social engineer if they misjudge how best to

go about these activities. The experience of psychologists in conducting interviews on sensitive and potentially illegal activities could be used to complement the work already being undertaken in this field. Of course it must be commented that in light of the issue of ideology and reactance that have been discussed cyber adversaries who are experienced in social engineering may not be inclined overall to work with cybersecurity practitioners. However even with these differences there are areas where collaboration may occur. Despite the fact that websites such as 4chan are almost defined by the practice of producing the most shocking content possible it has been observed there is zero tolerance amongst users for child pornography, and indeed those attempting to obtain or disseminate child pornography material on the website often become the targets of social engineering based attempts by others users to identify and entrap them[4]. Using the experience of users who have applied social engineering to trick and deter paedophiles could aide cybersecurity practitioners and educators in the development of techniques to promote online safety in young people.

There is also a need for a better understanding of the social context of cyber security. As conceptualised in Figure 1 all cybersecurity incidents occur within the context of wider society, which depending on the situation may occur at multiple levels from the local to the international. Researchers such as Holt have provided in-depth explorations of the behaviour of hackers, including less technologically skilled individuals such as script kiddies[28]. However as online technology becomes increasingly social in nature it could be argued that the social context of hackers may have widened. The users on 4chan and other sites who became involved in the online protests against the Church of Scientology were not all hackers, and may not have even been script kiddies. Yet they played a part in these protest through supporting those who did have the technological skills, and by taking part in the offline protests that continue today. Rogers[10] suggests that increasing contact between cybercriminals and more mainstream internet users may result in a change to the social environment that would discourage participation in cybersecurity incidents. This is consistent with the contact hypothesis from social psychology research, which suggests that contact between groups can reduce the conflict between them[29], particularly when cross-group friendships area created[30]. Indeed there is evidence that even asking people to imagine contact with another group can reduce intra-group hostility [31].

Social psychological research has demonstrated however that certain requirements must be met if this type of contact is to be effective. First, there must be a wider social climate which encourages integration between the opposing groups. Secondly, the contact must take place under conditions of equal social status. Finally, the contact must involve cooperation towards a shared goal. It is difficult to envisage how some of these principles could be applied to real life cybersecurity situation. For instance as discussed members of some online groups may derive their social identity and self-esteem from being members of a persecuted group that it is acting against a larger organisation, and therefore the engaging with another group under a sense of equal social status may not be consistent with their sense of group identity. Similarly organisations who have been a victim of cyber a cybersecurity incident may be unwilling to engage in a dialogue as equals. One way to start this dialogue could be to consider social psychological research that demonstrates that people often hold negative misperceptions about others, even their own peers[32]. Challenging these negative stereotypes and misperceptions and instead focussing on positive change has been found to be an

effective form of behaviour change[32], perhaps because it is based on empowerment rather than fear appeals. An interesting comment is made by several of the participants in the documentary film *We Are Legion: The Story of the Hacktivists*[20], which is that they were surprised by the diversity of the people who attended the street protests against the Church of Scientology. To paraphrase one of the film participants these people were not all socially awkward male adolescents, as perhaps the stereotype would predict, but instead men and women of a range of backgrounds and of different ages.

In conclusion there is potential for collaborative research in social psychology and cybersecurity to benefit both disciplines. Cybersecurity researchers and practitioners can aide social psychologists in accessing and understanding online social groups of a type which are vastly under-studied. The social dynamics of these groups may represent novel processes that could have paradigm shifting implications for the field of social psychology. Social psychologists can in turn provide cybersecurity experts with evidence based approaches on how to predict and if necessary attempt to mitigate group based cybersecurity incidents, as well as aiding in the methodological and ethical challenges inherent in studying some of the human factors of cybersecurity. Through such collaboration new ways of promoting online safety and empowering individuals to make informed decisions about their participation in cybersecurity incidents may be reached.

6 References

1. Coleman, G., *Hacker, Hoaxer, Whistleblower, Spy : The Many Faces Of Anonymous*. 2014, London: Verso.
2. Bartlett, J., *The Dark Net*. 2014: William Heinemann.
3. Fiske, S.T., *Social Beings: Core Motives In Social Psychology*. 2010, Hoboken, NJ: John Wiley & Sons.
4. Olson, P., *We Are Anonymous*. 2012, New York: Back Bay Books.
5. Bettencourt, B.A. and K. Sheldon, *Social roles as mechanisms for psychological need satisfaction within social groups.* Journal of Personality and Social Psychology, 2001. **81**(6): p. 1131-43.
6. Tormala, Z.L. and R.E. Petty, *What doesn't kill me makes me stronger: The effects of resisting persuasion on attitude certainty.* Journal of Personality and Social Psychology, 2002. **83**(6): p. 1298-1313.
7. Hewstone, M. and J.M.F. Jaspars, *Intergroup relations and attribution processes*, in *Social Identity And Intergroup Relations*, H. Tajfel, Editor. 1982, Cambridge University Press: Cambridge. p. 99 - 133.
8. Doise, W., *Groups And Individuals: Explanations In Social Psychology*. 1978, Cambridge: Cambridge University Press.
9. Marques, J.M., D. Abrams, and R.G. Serodio, *Being better by being right: Subjective group dynamics and derogation of in-group deviants when generic norms are undermined.* Journal of Personality and Social Psychology, 2001. **81**(3): p. 436-447.

10. Rogers, M.K., *The psyche of cybercriminals: A psycho-social perspective*, in *Cybercrimes: A Multidisciplinary Analysis*, G. Ghosh and E. Turrini, Editors. 2010.
11. Goffman, E., *The Presentation of Self in Everyday Life*. 1959, New York: Anchor Books.
12. Jones, E.E. and T. Pittman, *Toward a general theory of strategic self-presentation*, in *Psychological Perspectives on the Self*, J. Suls, Editor. 1982, Erlbaum: Hillsdale, NJ.
13. Underwood, J.D.M., L. Kerlin, and L. Farrington-Flint, *The lies we tell and what they say about us: Using behavioural characteristics to explain Facebook activity.* Computers in Human Behavior, 2011. **27**(5): p. 1621-1626.
14. Hofstede, G.H., G.J. Hofstede, and M. Minkov, *Cultures And Organizations : Software Of The Mind : Intercultural Cooperation And Its Importance For Survival*. 3rd ed. 2010, New York: McGraw-Hill. xiv, 561 p.
15. Rogers, R.W., *A protection motivation theory of fear appeals and attitude change.* Journal of Psychology, 1975. **91**(1): p. 93.
16. Johnston, A.C. and M. Warkentin, *Fear appeals and information security behaviors: An empirical study.* Mis Quarterly, 2010. **34**(3): p. 549-566.
17. Haslam, S.A. and S. Reicher, *Debating the psychology of tyranny: Fundamental issues of theory, perspective and science - Response.* British Journal of Social Psychology, 2006. **45**: p. 55-63.
18. Alberici, I.A., et al., *Comparing social movements and political parties' activism: The psychosocial predictors of collective action and the role of the internet.* Contention, 2012. **0**(0).
19. Brehm, S. and J. Brehm, *Psychological Reactance: A Theory of Freedom and Control*. 1981, New York, NY: Academic Press.
20. Knappenberger, B., *We Are Legion: The Story of the Hacktivists*. 2012.
21. Festinger, L., *A Theory Of Cognitive Dissonance*. 1957, Evanston, Ill.,: Row. 291 p.
22. Ashenden, D. and D. Lawrence, *Can we sell security like soap?: a new approach to behaviour change*, in *Proceedings of the 2013 workshop on New security paradigms workshop*. 2013, ACM: Banff, Alberta, Canada. p. 87-94.
23. Hadnagy, C., *Social Engineering: The Act of Human Hacking*. 2011, Indianapolis: Wiley Publishing Inc.
24. British Psychological Association, *Code of Human Research Ethics*. 2010, British Psychological Society: Leicester.
25. Dimkov, T., W. Pieters, and P.H. Hartel, *Two methodologies for physical penetration testing using social engineering*, in *Annual Computer Security Applications Conference*. 2010: Austin, Texas.
26. Foxcroft, D., et al., *Longer-term primary prevention for alcohol misuse in young people: A systematic review.* Addiction, 2003. **98**: p. 397 - 411.
27. Thaler, R.H. and C.R. Sunstein, *Nudge: Improving Decisions About Health, Wealth and Happiness*. 2009: Penguin.
28. Holt, T.J., *Examining the role of technology in the formation of deviant subcultures.* Social Science Computer Review, 2010. **28**(4): p. 466-481.
29. Allport, G., *The Nature of Prejudice*. 1954, Reading, MA.: Addison-Wesley.
30. Pettigrew, T.F. and L.R. Tropp, *A meta-analytic test of intergroup contact theory.* Journal of Personality and Social Psychology, 2006. **90**(5): p. 751-83.

31. Crisp, R.J. and R.N. Turner, *Can imagined interactions produce positive perceptions? Reducing prejudice through simulated social contact.* American Psychologist, 2009. **64**(4): p. 231-240.
32. McAlaney, J., B. Bewick, and C. Hughes, *The international development of the 'Social Norms' approach to drug education and prevention.* Drugs: Education, Prevention, and Policy, 2011. **18**(2): p. 81-89.