Foreword

Introductions to books such as this one very often include proclamations that "this is a timely volume", to the extent that the phrase becomes something of a cliché. In this case, however, it is absolutely true. The themes and topics covered by this book bear directly on our understanding of, and reactions to, events that have an ongoing, significant and sustained impact on the world in which we live.

Formal definitions of 'cyber security' typically revolve around systems, standards, technologies and processes for protecting computer systems, networks and the data they contain from unauthorised access or malicious attacks. Such a definition may imply that cyber security is somewhat of a dry, technically focused enterprise, mainly of concern to computer scientists and industry professionals. That is a long way from the truth: cyber security, and security violations, have profound implications for all of us.

We now live in a world where all manner of devices, services and the people who use them are networked and vulnerable to electronic attack. These range from obvious targets like traditional computer and telecommunications systems, to nuclear reactors, children's toys and domestic appliances. All may be threatened or exploited in different ways. As our reliance on communication technologies and networked devices inexorably grows, cyber security will become more and more critical to society.

At the time when this book was being written, various aspects of cyber security were rarely far from the headlines. Businesses and public services including hospitals, were crippled by ransomware attacks. Online fraud was rampant, with costs to economies and individuals that are hard to quantify. In a number of countries, there were allegations that foreign states had hacked political campaign organisations, resulting in the theft and publication of emails for political purposes. There were accusations of meddling in multiple elections by electronic means. There were frequent concerns about online influence leading to political and religious extremism, and the use of telecommunications and networks by terrorists, criminals and national security agencies. Loss, theft, and publication of personal information were depressingly frequent, ranging from the personal photos of celebrities to very large scale losses of personal data and breaches of confidentiality by public and private organisations. Whether directly or indirectly, issues such as these touched all of our lives.

In any technical field, there is a tendency to prioritise technical approaches to solving problems. However, hardware and software engineering can only ever be part of the solution to cyber security. Since the days of the earliest computer hackers, it has been known that the human element is among the weakest components in any system. The use of 'social engineering' techniques (manipulating people in various ways to gain access to secure computer systems) was, and remains, a key weapon in the arsenal of those who seek to illegitimately access or attack the systems, services and infrastructure underpinning many aspects of modern life.

Humans will always interact with any information system at some level, and human behaviour thus becomes a part of the system. And of course, a human actor is always the instigator of any attack upon a system. It is therefore imperative to understand how people interact with the technologies at hand, and what individual behaviours may introduce vulnerabilities. For example, what factors might make some individuals or organisations more susceptible to malicious influence? How do psychological phenomena and information technologies mediate, underpin or facilitate such processes of influence? What can be done to protect individuals, groups and systems from such attacks? These questions are clearly in the domain of psychology and the behavioural sciences. Without considering them, no approach to cyber security can ever be successful.

This collection of chapters deals with several key themes around the intersection of psychology and cyber security. One of the areas explored is individual decision making in online environments, which leads to the considerations of privacy protection behaviour, trust formation and individual cyber security concerns affecting consumer behaviour and ultimately victimisation. Next, a number of phenomena relevant to cyber security on a global level are addressed. In particular, this volume investigates how culture and religion might impact upon security, arguing that cyber security measures and technology acceptance are affected by individual cultural differences. The discussion delves into the issues connected to online radicalisation and cyber terrorism reflecting the currency of this volume in light of the recent attacks worldwide and the pressing need to bring this phenomenon to an end. Cyber security professionals often say that we can never achieve a perfect cyber security posture. The risk of cyber security threats rather is said to be minimised through the application of protective mechanisms and security controls. The discussion of cyber security will not be complete without addressing two key elements in this: how can we educate and motivate individuals to behave in a way that reduces risk?

Drawing on up-to-date research findings, each chapter addresses key practical and theoretical issues in a variety of important applied contexts. The questions addressed here are not just of academic interest; they have critical implications for the security of our society. Taken together, these chapters provide an excellent overview of current research and thinking across a broad spectrum of cyber security-related issues and behavioural phenomena. They will prove a valuable resource both for those working in the behavioural sciences, and those with a more technical focus. It is only by different disciplines working together across that boundary that risk can be reduced and security enhanced.

Tom Buchanan
University of Westminster, UK

Preface

Researchers in a variety of disciplines turn to psychology to help understand human behaviour and decision making. Psychology has a long history of understanding human behaviour, thoughts and actions. By applying that research and theoretical knowledge to the topic of cyber security, academics and practitioners may be able to better understand why and when people engage in cyberattacks. Such knowledge is useful to those in law enforcement and policy. It is also crucial to those working in organisations who try to keep their companies safe.

Threats can come from inside the organisation or from outside. Insider threats pose a particularly difficult challenge as one has to monitor who may be a threat and to some extent why they are a threat at any given time. To know that, we must rely on psychology to help us analyse human behaviour. Without a foundation in how to better understand human behaviour, we could be at a loss to predict who may be an inside threat.

Outside threats are in some ways easier to understand and many cyber threats originating outside an organisation require no assistance from insiders. There is only so much technology can do to keep corporations safe. As good as the technology is, humans are adept thinkers and will be able to navigate a way around most security systems. That is not to say that anyone could do so, but those who have a knack for it and are so inclined could breach the security. Those who are less skilled but equally as motivated, may be able to pay someone to breach the organisation's security.

Concepts such as trust and relationship development are relevant to this work. Psychology has long studied these ideas and can contribute a significant literature to them. For example, in trust studies, psychological research has investigated how the concept is developed, and how it is fostered. It looks at what leads to a breakdown in trust in dyads as well as in larger group settings. Through this sort of research, we may be able to apply it and develop a greater understanding towards how hacking groups are formed and rely on each other to breach a security wall. We may also use it to try to mitigate such violations by developing interventions to build trust within an organisation or between the organisation and potential outside hackers.

Similarly, we may rely on psychological research in relationship development. We could look at how relationships are created and who wants to be part of certain relationships. We could look for weaknesses in relationships and what holds people together. Understanding why certain people are drawn to others, what motivates groups to form and to have a particular agenda, is all crucial in considering security of cyber systems.

Aspects of disinhibition and anonymity in the online setting need to be considered as well. Disinhibition has been studied in psychology since at least the 1960s. Addressing what increases people's chances of acting in a particular circumstance or failing to act in others is not new to the field. What

is new, however, is looking to see how that research and those findings may be applied to the online environment. What features about individual differences may increase someone's chances of using the internet to engage or encourage terrorism? What might make an individual think about why s/he should use online media for a social protest or choose to protest in a more traditional way, or not at all? Theories and research in social psychology have studied why people may be inhibited or disinhibited to act in certain ways; these book chapters are able to use that foundation as a cornerstone to better explore how the human agent is relevant in cyber security.

Anonymity is an interesting concept to consider both in psychology and cyber security. We know from psychology that in large groups when people feel that they cannot be identified (that is, they are anonymous) they are more likely to engage in risky behaviour. It is possible, therefore, that we would expect that sort of behaviour in the online environment where identity may be protected. The importance of this to cyber security is not to be considered lightly. If techno-savvy people can protect their identity, this leaves a vulnerable online environment rife for infiltration. Infiltration could come from multiple sources as many of these chapters attest to. The insider threat, especially if the culprit could remain anonymous, is undoubtedly of concern. The hackers or those who are simply interested in breaching cyber security for the thrill of it with low risk of getting caught may feel a challenge waiting. Engaging in social protest again with a low cost as the methods of finding the perpetrator are not well established could lead to those with only minor grievances to consider violating the security wall. More structured groups who wish to see a corporation's downfall are able to spend the time, effort and energy to develop a well-planned security breach. They may be able to call on outsiders to help, again as the prospect of remaining unknown is substantial.

Ethics is another area where psychology has spent a fair amount of time trying to consider how to understand human behaviour from a theoretical perspective whilst also ensuring that human rights are not violated. In doing so it provides a good cornerstone to address cyber security from multiple angles. First, by considering the research that has been done to understand human behaviour, someone looking at violations of cyber security can rely on solid design with ethical guidelines fully considered. From the organisation's viewpoint, second, a foundation in psychology can help to guide strict approaches to prevent breaches while still mainly an ethically appropriate approach to employees and those who use and interact with the organisation. Third, company may consider, again ethically, how to prevent security breaches whilst maintaining a usable online platform.

Using these concepts as well as other aspects that are cornerstones of psychological research we can see how it is a crucial field to consider when looking at cyber security. Human behaviour is at fault for a number of security violations, especially if the technology becomes more and more robust. Relying on well evidenced and well researched concepts within human behaviour, we see how the human element is a base to understand and mitigate intrusions in cyber security.

This book covers a variety of topics and addresses different challenges that have emerged in response to changes in the ways in which it is possible to study various areas of decision making, behaviour and human interaction in relation to cyber security.

Each of the chapters brings its own contribution on how psychology furthers our understanding of cyber security. The innovative chapters link a strong foundation in human behaviour research with application to a topic of crucial importance in today's world. By looking at the chapters (see descriptions below) it should be clear how this topic is of the utmost importance in today's world. Understanding

cyber security and breaches in it can only help to make all of us safer. Looking at ways to protect our finances, our images stored online and companies protected data, helps us all. Considering research on psychology and cultural identity may help us in understanding who and in what circumstances someone may decide to encroach on secure systems.

In a world as complex and fast moving technologically as one in which we find ourselves, a reference book such as this is a must. It provides the foundation of understanding aspects of human behaviour coupled with an area of real concern criminologically. It is necessary at this juncture of technology and human behaviour to understand who, when and why people might breach security systems. Who are the players most likely to do this and what can the authorities, policymakers and organisations themselves do to mitigate these threats? When are breaches likely to take place? Does it happen when political tensions rise and those prone to engaging in terrorism might increase? Does it happen when employees become disgruntled? How about when people want to set themselves a challenge to see if they can violate a security system? There are numerous questions about why these intrusions may happen at this particular time and in particular places. Culture, decision making, spotting vulnerabilities, etc. all make for an online system that is rife to be breached. In today's society, we cannot take a lax approach to our security nor to leaving human behaviour to the academics. We must join forces to make sure that we all stay safe, and continue to understand, before the violators do, what cyber vulnerabilities we have exposed.

This book was written with a large audience in mind. First, it was created for the practitioner. When understanding your own organisation and how to protect it, we thought a base in human behaviour would be relevant. If human behaviour and a century of research in this field is ignored, we are not using our collective knowledge to help society today.

Second, this book is addressed to the policymaker. Knowing what the risks are from the organisational perspective interwoven with research is crucial when considering applications of academe. Policymakers often do not have the luxury of reading the latest research in a field before needing to consider the political agenda. Hopefully this book gives a summary of relevant literature when contemplating cyber security.

Third, this book was conceived for the academic and researcher. These chapters show how theoretical work in psychology can be applied to a timely and real world problem. As much as researchers enjoy studying concepts to support or refute theory, to do so and see it have great impact in the broader community is pleasing. This book exemplifies how such work can provide said impact. Reading the chapters provides a trail map of concepts in psychology being applied to keeping us all safe in the cyberworld.

Finally, technology developers should read this book. Those who work in the field of cyber security undeniably see the thin line that is walked between staying secure and keeping cyber systems free. We all want systems that allow as many people to use them as possible and to keep our lives as simple as they can be. But, creating a banking system for people to use from the comfort of their home, while it may keep our lives simpler as we do not need to go to the bank during opening hours, is not useful if our finances are at risk. A fine balance must be found by our technology counterparts to ensure that social groups may use online fora without posing a risk for terrorist attacks. If the technologists can find that happy medium, we are in as safe and user friendly a world as possible. The problem of course is that that line often moves and the technologists may use this book to better understand how human behaviour can change and shift over time, providing them a stronger foundation for which to understand where that line is moving to next.

Below is a brief summary of the chapters in this book. They range across topics as you will see but hopefully gives a flavour of how psychology can contribute to this field. As both psychology and cyber

security are vast, it does not attempt to be an exhaustive book. Yet, it should give a strong foundation on understanding a range of relevant topics from decision making, cognitive bias, terrorism, social media and guidance on how to do one's own study in an ethically appropriate way.

Chapter 1, "Online Decision Making: Online Influence and Implications for Cyber Security," addresses the challenges of understanding the differences between decision making that is performed online and research that uses an online forum alone. This chapter looks at how computer mediated communication impacts on how we make decisions online. Developing perspectives on decision making, and the applicability of the theories to the online environment is considered, with issues such as buying behaviour to radicalisation being addressed. This chapter encourages joint thinking from the practitioner and the researcher. It offers the idea that multiple models and perspectives are needed to understand how CMC influences our capacity to make decisions in the online forums.

Chapter 2, "Human Factors Leading to Online Fraud Victimisation: Literature Review and Exploring the Role of Personality Traits," highlights the role human behaviour has as the weakest link in cyber security. This literature review explores the role of personality traits, seeks an explanation for online fraud victimisation, and does so from a criminological and psychological perspective. First, a review of the literature in this area is presented. More specifically, the routine activity approach and the Big Five personality traits are discussed and applied to online fraud. Second, a novel empirical study on personality traits is presented, in which the influence of the Big Five personality traits on online fraud victimisation is assessed. This chapter ends by presenting implications for online fraud prevention as well as possibilities to advance the study of cyber victimisation.

Chapter 3, "The 'Human Factor' in Cyber Security: Exploring the Accidental Insider," describes the threat posed by members of an organisation. These threats may come from disgruntled employees or more innocuously from ignorance. Either way, they pose a potentially serious threat to information security. This chapter discussing aspects of the insider threat as well as the human factors that may contribute to one becoming a threat. Methods to detect and mitigate the threats are presented here.

Chapter 4, "Cyber + Culture: Exploring the Relationship," highlights some of the findings of a selection of recent studies on the relationship between national culture and specific cyber behaviours. The goal of this work was to understand the ongoing problem of attribution in cyber security as advances in technology is showing improvement in cyber-attack attribution, albeit slowly. Interest in the psychological research of decision making and the role of the human in perception management lead to the belief that behaviour may be able to ward off some cyber-attacks by defending and training users. In modelling behaviours related to cyber security, one needs to consider the role of culture in values which shape behaviours. This chapter crucially contributes to an area of research that is lacking by providing foundational work in this field.

Chapter 5, "Examinations of Email Fraud Susceptibility: Perspectives From Academic Research and Industry Practice," covers issues associated with the positive and negative sides of the internet being used for entertainment, commerce and communication. The potential for human advancement in this venue is substantial but so is the risk of increasingly sophisticated cyber-attacks. These undoubtedly could have serious personal and commercial implications. From a psychological viewpoint the attacks offer an insight into the decision making processes which may lead to being a victim of online fraud. The authors use their chapter to attempt to understand responses to phishing emails whilst exploring how industry and academic research might collaborate to better address email fraud threats. Various methods to understand susceptibility and considering preventable security measures are used to try to develop integrative solutions.

Chapter 6, "Introducing Psychological Concepts and Methods to Cyber Security Students," discusses the role and impact of psychology research on cyber security education. By using both prior cross-disciplinary teaching experience and observations of teaching psychological principles and methods to undergraduate and postgraduate cyber security students, the authors have compiled information about their experiences. There is a strong focus on making the material accessible and engaging. Suggestions as to how to integrate psychological into the cyber security curriculum completes the chapter.

Chapter 7, "The Role of Psychology in Understanding Online Trust," addresses the challenges of trusting people in the online environment. The authors discuss the manipulation of trust and the sometimes dire economic and psychological consequences. Literature on developing trust online is reviewed and several case studies describe trust relationships. Crowdfunding, online health forums and online dating help us to understand the need for stronger security measures which can increase trust judgments and minimise the risk of falling prey to fraud online.

Chapter 8, "Volunteered Surveillance," addresses the issues of data collection, data ownership, digital tracking, digital privacy, cyber security and ad-blocking in modern society through managerial, psychological and behavioural lenses. As technology advances more parties gain access to private data relying on "agree or leave" contracts, forcing individuals to give up ownership of their own behavioural patterns. These data are then commonly used for commercial purposes in forms of advertising, targeted marketing or more. Consumers on the other hand, seem to react to this in a very broad spectrum ranging from ad-blocking software to voluntary data submission. This chapter analyses why and how these reactions happen and propose solutions that could be beneficial to all parties included. This is a very novel macro concern and requires institutionalised oversight of all concerned stakeholders; governments, digital service providers and publishers, advertisers, self-regulatory organisations in related sectors and non-governmental organisations protecting consumers.

Chapter 9, "Psychological and Behavioral Examinations of Online Terrorism," presents mixed method research results on how terrorists use the internet to further their agendas. Several studies have investigated how terrorists use the online environment and the chapter first explores current knowledge about the online behaviour of terrorists. It follows on to describe how qualitative and quantitative combined studies can be used to consider how to conduct research in this area. After that a serious discussion is given to the difficult area of ethics in this field of research. The chapter closes by imparting information to the reader about the skills and knowledge necessary to undertake one's own research in this arena along with consideration of the ethics around such work.

Chapter 10, "The Role of Religiosity in Technology Acceptance: The Case of Privacy in Saudi Arabia," covers issues associated with how religion affects user behaviour and the acceptance of emerging technology. Religiosity is used to measure individual beliefs; this chapter explains how Islam influences user behaviour and intention to use technology. Saudi Arabia, as an example of a hardline Islamic nation according to the author of this chapter, is used for the discussions of privacy and technology influence in a single religion country. The chapter presents conclusions on how religion influences people's behaviour, privacy perceptions and acceptance technology.

Chapter 11, "Groups Online: Hacktivism and Social Protest," reviews the broadly defined topic of hacktivism. It offers up the proviso that it can be viewed as a legitimate form of online protest or one of illegal hacking. Additionally, there are those who feel that there is truth to both arguments, and believe it is imperative to protect those who engage in hacktivism. These counter definitions make it difficult to understand how to bridge the gap in assessing motivations. The authors give a brief introduction to hacktivism and online social protest online. In particular, the socio-psychological and cognitive factors

possibly providing the foundation for individuals to take part in hacktivism groups are addressed. Within the socio-psychological arena, the authors consider the concepts of social ties and influence. These are subfields that are important to address when looking at how individuals join, form and remain in groups. The subfield of cognitive biases is important as well and biases are examined in light of how people think and process information given the biases we each hold. Conclusions are drawn with strategies to mitigate and support vulnerabilities considering hacktivism and social protest.

Chapter 12, "A Cyber-Psychological and Behavioral Approach to Online Radicalization," addresses the challenges of bringing mainstream theories of radicalisation and cyberpsychology together with a goal towards understanding who might become radicalised. The chapter uses Islamic State of Iraq and al-Sham (ISIS) as a case study to understand how radicalised groups use cyberspace. By using academic theory, the chapter considers behavioural aspects of the radicalisation process. It also reviews how those theories are relevant in explaining, facilitating and attracting people online to a radicalisation pathway.

Chapter 13, "Insider Attack Analysis in Building Effective Cyber Security for an Organization," provides a detailed study on how behaviours from those inside may hinder security of the organisation. A number of recent studies had shown that even though there are highly advanced and secure technical controls, several cyber-attacks were carried out across multiple organisations yielding the release of confidential information. It should be clear then that technical advancements of cyber defences are not impenetrable to organisational security. Insiders often have the advantage of being a trusted party when engaging in cyber-attacks and monitoring said insiders is very challenging. The insider has the potential to cause problems to the social credibility of the organisation as well as damage its financial stability. The author reviews behaviours of insiders who may pose a cyber security threat to an organisation and provides some guidance for reliable security frameworks.

Chapter 14, "A Study of Good-Enough Security in the Context of Rural Business Process Outsourcing," presents insights using scenarios of object decomposition and sharing. By looking at low value data objects such as insurance or data-entry forms the chapter is able to explore how information is shared between a client and Rural Business Process Outsourcing (RBPO) organisations. Such sharing is usually across tasks like translation, proof-reading and data entry. These data objects are decomposed into smaller parts before being sent to the RBPO allowing for each RBPO user to only access a few parts of a complete data object. Nevertheless, this information could be leaked to unauthorised users which would breach the data security. As the value of these parts is low there is little incentive for them to truly be leaked. Here is where the idea of a good enough security system comes in. The good enough model should provide reasonable security to a group of low value data objects. This chapter describes the work of secure data assignment and leakage in RBPO. By modelling this work as an optimisation problem, the authors are able to review object decomposition scenarios in light of sharing, penalty assignment and data leakage.

Chapter 15, "Online Research Methods," opens the discussion on the use of more contemporary approaches to data collection than traditional pen and paper questionnaires. Although the traditional methods are still more readily used, various online methodologies may enhance scientific investigation and understandings of particular phenomena. The chapter explores how these could be potentially useful in understanding psychological issues related to a range of cyber security problems.

Chapter 16, "Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape," presents an overview of emerging issues in psychology of human behaviour and the evolving nature of cyber threats. The chapter reflects on the role of social engineering as the entry point of many sophisticated attacks and highlights the relevance of the human element as the starting

point of implementing cyber security programmes in organisations as well as securing individual online behaviour. Issues associated with the emerging trends in human behaviour research and ethics are presented for further discussion. The chapter concludes with a set of open research questions warranting immediate academic attention to avoid the exponential growth of information breaches in the future.

This publication addresses the emerging importance of digital psychology and the opportunities offered by cyber researchers. We hope that experts from all areas of research, information systems, psychology, sociology, human resources, leadership, strategy, innovation, law, finance and others, will find this book useful in their practice.

John McAlaney
Bournemouth University, UK

Vladlena Benson
University of West London, UK

Lara A. Frumkin
Open University, UK

Acknowledgment

First and foremost, we would like to thank our families for their patience and unresolved support during numerous late nights and weekends spent working on this book. It was a long and difficult journey for them. We would like to express our gratitude to Professors Jonathan Loo and Shanyu Tang for their valuable insights when steering this project through its final (and lengthy) stages. We would like to thank Professors Tom Buchanan and Debi Ashenden for deeming the subject of the book interesting and the project worthwhile.

We wish to thank many people who saw us through this book; to all those who provided support, talked things over, read, wrote, offered comments, and assisted in the editing, proofreading and design.

We would like to thank the IGI project team for enabling us to publish this book.

Detailed Table of Contents

effectively understand and potentially tackle the persistent threat of email fraud. In doing this, the authors address alternative methodological approaches taken to understand susceptibility, key insights drawn from each, how useful these are in working towards preventative security measures, and the usability of each approach. It is hoped that these can contribute to collaborative solutions.

Chapter 6

This chapter begins with a brief review of the literature that highlights what psychology research and practice can offer to cybersecurity education. The authors draw on their wide-ranging inter-disciplinary teaching experience, and in this chapter, they discuss their observations gained from teaching psychological principles and methods to undergraduate and postgraduate cybersecurity students. The authors pay special attention to the consideration of the characteristics of cybersecurity students so that psychology is taught in a way that is accessible and engaging. Finally, the authors offer some practical suggestions for academics to help them incorporate psychology into the cybersecurity curriculum.

Chapter 7

Across many online contexts, internet users are required to make judgments of trustworthiness in the systems or other users that they are connecting with. But how can a user know that the interactions they engage in are legitimate? In cases where trust is manipulated, there can be severe consequences for the user both economically and psychologically. In this chapter, the authors outline key psychological literature to date that has addressed the question of how trust develops in online environments. Specifically, three use cases in which trust relationships emerge are discussed: crowdfunding, online health forums, and online dating. By including examples of different types of online interaction, the authors aim to demonstrate the need for advanced security measures that ensure valid trust judgments and minimise the risk of fraud victimisation.

Chapter 8

As the front end of the digitized commercial world, corporations, marketers, and advertisers are under the spotlight for taking advantage of some part of the big data provided by consumers via their digital presence and digital advertising. Now, collectors and users of that data have escalated the level of their asymmetric power with scope and depth of the instant and historical data on consumers. Since consumers

Chapter 11
Groups Online:
Hacktivism and Social Protest

Helen Thackray
Bournemouth University, UK

John McAlaney
Bournemouth University, UK

ABSTRACT

This chapter provides a brief introduction to hacktivism and social protest online and highlights some of the socio-psychological and cognitive factors that can lead to individuals taking part in hacktivism groups. Hacktivism is an ill-defined area which some claim as a legitimate form of protest in the online world and others regard as illegal hacking; there is truth to both arguments, and those who believe it should be protected will continue to work for it to be recognised. The chapter explains how the depth of social ties and influence are still being examined, and whilst cognitive biases are recognised, strategies to mitigate and combat the vulnerability they present are still being developed.

INTRODUCTION

The internet is a significant aspect of global social change, and has greatly altered the nature of collective action and social movements (Jensen, 2015, Postmes & Brunsting, 2002). Hacktivism, a term combining 'hacking' and 'activism', is the use of various computer hacking tactics for political, social, and ideological motivations; hacktivists use nonviolent but often illegal digital tools to achieve these goals (Hampson, 2012, Krapp, 2005, Solomon, 2017). The common methods of hacktivism include defacing websites, using DDoS attacks, and other types of internet disruption (see Table 2, Hanna et al, 2016). The use of these tactics has led to challenges in distinguishing between hacktivism and hacking, as it can be that only the individuals' motivation is different. This chapter will discuss the current understanding and context surrounding hacktivism, before examining the cognitive and social psychological factors that can influence those involved in hacktivism and online social protest.

DOI: 10.4018/978-1-5225-4053-3.ch011

BACKGROUND

It is important to remember that cybersecurity incidents occur within a social context; even if it is not face to face, online interactions fulfil and rely on the same social or task needs as offline interaction with others (McKenna & Green, 2002). There remains, however, a lack of insight into the influence of psychological factors and social norms online, especially in the case of hacktivism. All actors within cybersecurity incidents interact with each other and within each group. Whilst hacktivism is regarded as a contested area, stuck between definitions of justified civil action and illegal hacking, there remains a strong need to challenge the stereotypes around it. The conflation of the terms "hacker" and "hacktivist", with "cybercriminal" and "cyberterrorist" adds to the confusion surrounding the different typologies identified (see Table 1). A divisive and complex issue, there are many governments and businesses see hacktivism as a threat, akin to cyber-terrorism and cybercrime (Drucker & Gumpert, 2000, Kubitschko, 2015, Manion & Goodrum, 2000, Shaw, 2006); others argue that social protest and change have always been a part of society (Scheuerman, 2016, Schrock, 2016), and that hacktivism is the progression of social protest (Kubitschko, 2015, Postill, 2014, Solomon, 2017).

Hacktivism is not a 21st century addition to the internet. The origins lie in computer based activism as early as the mid-1980s (Wray, 1998). One of the first known instances of a DDoS attack occurred in 1995, when a group of Italian artists blocked websites of the French government, in protest of the decision to undertake a series of nuclear tests (Milan & Atton, 2015). Hacktivism was not, however, a well-known phenomenon until the mid to late 2000s. One of the more predominant groups, Anonymous, began to use media attention as part of their strategy; previously activist groups had preferred to remain undetected in order to protect their projects from law enforcement (Milan & Atton, 2015). As such Anonymous is probably the most widely known hacktivist group by the general population.

Since the mid-1990s the continued rise of hacktivism has surprised and worried many; but its' growth in popularity can be attributed to several reasons. The ease of contributing from one's home or place of choice means that distance is no longer an issue in supporting a cause, even if it is quite literally the other side of the world. Hacktivism also comes with a lower level of risk when compared to physical public demonstrations, whilst still allowing their messages and protests to be seen by the public across the internet – although this is not to say that it is risk free as some once perceived it to be (see cognitive

Table 1. Key terms

(Computer) Hacker	One with the ability to access a computer or system without admission (Raymond, 1996).
Hacktivism	A method to express dissatisfaction with elements of political and social reality using online resources (Milan & Atton, 2015).
Slacktivism	Critical term for low-profile online activism, such as signing petitions and using online badges (Hanna et al, 2016).
Whistle-blowing	The leaking of confidential information to the public as a form of raising awareness about a contentious issue (Hanna et al, 2016).
Cybercriminal	A criminal who uses a computer or network to commit the crime (Anderson et al, 2013, Halder & Jaishankar, 2011, Moore, 2005, NCA, 2016).
Cyberterrorist	One who uses computer/network technology to terrorise opponents to further political or social objectives (Rogers, 2003).
Cyber delinquent	One who engages in illegal behaviours, such as verbal violence, hacking, and illegal copying of software in online environments (Hong & Kim, 2011).

factors). For many hacktivists now, there is also the motivation that state actors and law enforcement agencies have chosen to use electronic surveillance and hacking. As such the hacktivists regard their actions as a "means of levelling the playing field" (Solomon, 2017:3).

As a community, hacktivism is itself a social identity group, an "imagined community" (Anderson, 1983, Jordan & Taylor, 1998); a socially constructed community where there is no physical or geographical connection within the group, only the strong shared choice of interest and identity. It is known that hackers and hacktivists create social groups that provide expertise, support, and training within their communities (Jordan & Taylor, 1998:757). This being the case, the social psychological processes have a strong influence on the internal group behaviours, as well as their interaction with other groups. Studies investigating unifying identity traits have emphasised that the traditional stereotypes may not be as prevalent as previously believed (Jordan, 2001, Rogers, 2010, Tanczer, 2015). Along with these communities being divided by different aims and tasks, there are also cultural divisions to be acknowledged, although it is not as clear how big an impact these differences make. Groups with different cultural backgrounds and opposing causes will still use the same hacktivist techniques. For example the Syrian Electric Army, a group that supported the Assad Syrian government in 2011, used website defacements, spamming, and electronic surveillance against their opponents, such as the Western media (Perlroth, 2013), hijacking headlines and Twitter accounts to communicate their messages.

THEN AND NOW: MASS SOCIAL MOVEMENTS

Mass social movements were historically regarded as being negatively influenced by personal elements of self-esteem or satisfaction with life. It was believed that personality attributes such as "impotence, selfishness and boredom characterised the…individuals prone to join mass movements" (Travaligno, 2014:5). In the 20th century however, with the closer study of such movements, and the growth in popularity and public support, these activities became regarded as more of a symptom that something was wrong in society (Travaligno, 2014), for example the movements for civil rights and anti-war protests in the USA. These periods emphasised the differences between the academic explanations for mass

Table 2. Common Hacktivist tactics

Denial of Service attack (DoS attack)	Using one computer and one internet connection the targeted server is overloaded by repeated requests. This makes the server unreachable to others, thus blocking the website.
Distributed Denial of Service attack (DDoS attack)	Many computers and many connections from all over the world (sometimes in botnets) are used to overwhelm the server with requests.
Site redirects	Site redirects send visitors from the target website to another website of the hacktivists choosing.
Information theft	Involves unauthorised access to a computer or network and stealing data. The illegality of information theft is unambiguous despite its wide acceptance among hacktivists (Hampson, 2012).
Site defacements	With unauthorised access to a web server the hacktivist replaces or alters the web page to convey their message. This is the most common and usually least damaging form of hacktivism (Solomon, 2017).
Viruses and malware	Viruses and other malware can be used as a means of sabotage, infiltration or even making a political statement.

social movements, and the reality that was being witnessed. These significant contributions marked the departure from classic views of masses and crowds as irrational and disorganised (Gamson, 1975; Jenkins, 1985; cited in Travaligno, 2014). In fact, there developed socio-psychological models which showed that social movements were "more likely to emerge under conditions of structural stability, social connectedness and favourable mobilisation of resources" (Travaligno, 2014:5). Protesters came to be understood as rational actors, who weighed the cost and benefit of participating in such protests.

As such, it has been assumed that those involved in social movements, including hacktivism, will be equally rational actors. Within hacktivist groups, the entry requirements no longer entail elite computing knowledge, and those wanting to participate in hacking and hacktivism now can find multiple resources in seconds through search engines; it is similarly quick and easy to download computing tools written by others. Groups like Anonymous have been proponents of such techniques, making it simpler for people to be involved, and using strength in numbers rather than a smaller group of experts. The forms of hacktivist groups are dictated by the medium used; the internet allows them to exist in a decentralised "community without structure" (Leach, 2009:1059). As such, the most common feature across different groups is a consensus-based based approach to their activities. For the most part this means that through necessity hacktivist groupings are still relatively small, and regulated by trust and loyalty (Milan & Atton, 2015).

It has been suggested that some individuals, often adolescents and young adults, become involved in the activities of groups associated with cybersecurity incidents without a clear understanding of the risks involved (Olsen, 2012, Wolfradt & Doll, 2001); therefore they have not fully understood the relationship between the cost and benefit of their involvement in the groups. This participation and subsequent arrest of adolescents and young adults has continued with events such as the TalkTalk hack (Farrell, 2016) and the hacking collective "Crackas with Attitude" (Whitehead, 2016). It is now being recognised that cybercrime is a societal issue, with the UK's National Crime Agency running campaigns to educate young people about the dangers of getting involved in cybercrime (NCA, 2016). However the confusion surrounding the internet and international law, and the fact that many laws pre-date the widespread and versatile use of the internet, means that even those wishing to remain on the side of the law when engaging in hacktivism may struggle to find relevant legislation.

Social Protest or Hacking Crime?

Social movements can be defined as broad and informal networks of interaction, that participate independently in collective action which is "motivated by a shared concern about a particular set of political issues…but not separately from governmental institutions" (Meuleman & Boushel, 2014:50). Social movement organisations refer to many different types, ranging from formal, organised institutions to the radically informal, from the local to the global (Meuleman & Boushel, 2014). This in turn requires the recognition of the cultural differences that may be present between all those involved, whether participants or targets.

It is agreed that there must be certain characteristics in order for these networks to be categorised as a social movement; Although there is a wide diversity of forms of social protest, analysis of these forms by Hanna et al (2016) suggests they have only seven functions (purposes). The purposes overlap, and an individual protest action may seek to achieve several of these purposes. Most protests involve the coordination of many activities or forms of protest and exist in a nested hierarchy as part of a wider campaign within a social movement.

Table 3. Social movement characteristics

1. Information	To distribute information to the wider public in order to raise awareness about 'the cause' or the situation that is the subject of protest.
2. Fundraising	To raise funds to support the campaign.
3. Publicity	To gain publicity (media attention) through the undertaking of actions usually having a performative dimension.
4. Mobilization	To enlist participants for a specific protest event or campaign.
5. Solidarity building	To build solidarity (unity and commitment) and a sense of worth amongst protesters and toward the protest cause in general.
6. Political pressure	To apply pressure, through direct or indirect targeting, on authorities or decision-makers regarding their action/decision on a specific issue.
7. Direct action	To cause immediate disruption to a specific project (e.g. a blockade), usually performed as acts of civil disobedience.

(Hanna et al, 2016)

Bearing this in mind, hacktivist groups can claim to meet these criteria as a social movement. When using the internet for activism, Vegh et al. (2003) suggest that are two forms— internet-based and internet-enhanced. In internet-based activism, such as hacktivism or digital sit-ins, the internet is where the protest occurs. Internet-enhanced activism however is more about the organisation of the protest than any fundamental change to the protest itself. Solomon argues that there is "in reality little distinction between hacktivism and traditional protests" (2017:11), reasoning that hacktivists state similar motivations (a political or social cause), suggesting that hacktivists view themselves as working with more traditional protesters. An example of this was during the Arab Spring in 2011, where protesters physically present in Tunisia were aided via the internet by members of Anonymous when the government blocked access to the internet (Goode, 2015).

It has also been argued that hacktivism is the progression of social protest (Kubitschko, 2015, Postill, 2014, Solomon, 2017), with protest moving from the physical world into cyberspace, as are many other traditional activities, such as shopping and banking. Some hacktivists regard their work itself as comparable to a physical sit-in protest (Jordan, 2015), with others making their protests through social media sites (Tufekci & Wilson, 2012, Valenzuela, 2013). It is suggested that there is potentially a need to protect and legitimise to some of the less controversial forms of hacktivism (Douglas et al, 2017, Solomon, 2017), acknowledging that the right to protest is protected by international human rights. There are articles which protect freedom of opinion and expression and covers developments in ICT, interpreted to 'include all forms of audio-visual as well as electronic and Internet-based modes of expression.' (UN Assembly, 1966). For this to apply to hacktivism there must be features, such as clear communication, which distinguishes this type of civil disobedience from radical protest. Douglas et al (2017) state that the civil disobedience of hacktivism must achieve the following: 1) provoke a political or social response; 2) allow that change is possible within the existing social and political structure. In this way, they argue, even a controversial tactic of a DDoS attack may be classified an act of civil obedience, despite being an illegal action, as in some cases it has the aim of communicating dissent to the public conscientious motivation.

It has been noted that hackers seem to be less motivated by their values and more by what they dislike (Madarie, 2017); the same could be observed of social media website users (Tufekci & Wilson, 2012,

Valenzuela, 2013). Whilst hacktivism is primarily committed through individual action, such as coding and hacking, these actions gain meaning in the interaction with peers (Douglas et al, 2017).

Case Study: Anonymous and Lulzsec

Possibly the most infamous hacktivist group is the one known as Anonymous. With its origins on 4chan, the group started by pranking and "trolling" other online (and offline) communities, for entertainment. Over time this evolved in to people trying to use this group activity for "good" causes. This eventually led to a division in the group; those who wanted to prank and enjoy the "lulz", and those who wanted to be "white knights" (see Coleman (2014) for more details).

As participation within Anonymous became more about political and social causes, rather than just mischief making, many of those who became involved in hacktivism cited their motivation as a desire to counteract the increase in surveillance and repression of such activities (Coleman, 2014, Douglas et al, 2017). Anonymous has used these motivations as a recruitment tactic, manipulating publicity, both negative and positive, to draw attention and support. This policy however has attracted criticism, due to the imprisonment of a number of hacktivists who took part in large operations, as well as a general lack of transparency and poor accountability from the group (Douglas et al, 2017). This is an example of the problems in hacktivism where groups, Anonymous especially, have always maintained that they do not have leaders and hierarchy (Coleman, 2014).

The hacks or "operations" carried out by Anonymous have ranged from simple pranks to serious on going campaigns. For the past few years, the name or brand has almost exclusively been used for hacktivism; those who claim Anonymous involvement in causes that do not meet the criteria have been denounced publicly, often through official Twitter accounts. This has in turn led to a lot of in fighting, as some argue that there are no leaders, therefore no one can decide who is or is not a member of Anonymous. One of the methods the group uses to monitor and control group membership is assertive speech; it is the mode of communication not the speaker that matters; therefore by using and maintaining control via social media accounts, this is how they get the message across to others. The group has also been noted for their controversial control of group identity, and have doxed individuals (revealing their real life identity and personal information), revoking their Anonymous membership (Dobusch & Schoeneborn, 2015).

Anonymous are a contentious topic; some members feel they made serious contributions to bringing hacktivism to the fore of current activism and protest, other commentator and critics feel it was a group of children and "wannabes" causing trouble, meaning the Anonymous has, at one point or another, been categorised as being relevant to all the terms in Table 1. Regardless of which argument is supported, it cannot be denied that Anonymous did draw attention and awareness to the importance of cyber-security.

Case Study: The Chaos Computer Club (CCC)

The Chaos Computer Club (CCC) is Europe's oldest and one of the world's largest hacker organizations – and they have a very different approach to Anonymous. Created via a newspaper advert in 1981, the CCC started as a loose group of individuals, but formally became a not-for profit association in 1984, with continued interactions with institutions and political organisations (Kubitschko, 2015). This active decision to remain legal in the face of "anti-hacking" government legislation is one of the most interesting elements about this group. The group describes itself as a non-governmental, non-partisan, not-for-profit,

and voluntary-based club that is sustained by membership fees and donations (Kubitschko, 2015). The CCC supports the principles hacker ethic (Levy, 2010) which stresses openness, sharing, decentralization, free access to computers and world improvement, as well as advocating more transparency in government, communication as a human right (Coleman, 2011, Kubitschko, 2015, Nissenbaum, 2004).

What makes the CCC significantly different to other hacker collectives is not their political dimension but their insistence on working as a legitimately recognised collective, even if they use illegitimate methods. One of the Club's aims is to teach the public to use technological skills and bring about political change. The groups hacks include exposing flaws in financial and political areas; for example in 1984, CCC members exploited a security flaw which allowed them to transfer 135,000 Deutschmark (ca. €68,000) from a German savings bank to their own (Kubitschko, 2015). The money was transferred back immediately and the flaw reported. The group has been involved in hacks which have either been a grey are or clearly illegal; this led to a period of decline in popularity in the 1990s. Within this group there appears to be the need to continue their legitimacy within the state of Germany, which struggled when members were conflicted about the group methods. The group rejuvenated itself in the 2000s, demonstrating flaws in a voting computer system that was in use in several countries and exposing the vulnerability of biometric identity systems. In 2011 they published an analysis of a malware program in use by the German police, which was used for surveillance; this highlighted the ability for the computer to be controlled remotely, as well as able to activate the microphone or camera (Kubitschko, 2015). It is emphasised that the CCC has a reputation for expertise, which they believe needs to be brought to the established centres of power by engaging with politicians, legislators and judges, (Kubitschko, 2015), because for the CCC, hacktivism is only one part of their purpose (Coleman, 2014, Kubischko, 2015).

SOCIO-PSYCHOLOGICAL FACTORS

As with all cyber-interactions, hacktivism occurs within a social context. As more individuals become involved in online communities relating to hacktivism, more groups develop and work together, and so the growth of potential online influence over individuals strengthens. This growth, especially in regard to social and ideological motivations, has been attributed in part to the fact that there is now a generation raised that has never known the world without the technology and innovation we have now (Seebruck, 2015), with increased user generated content increasing the confidence and perception of power individuals possess.

There are those who contend that online communication loses meaning and significance in understanding, due to the lack of visual face-to-face clues and prompts (Suler, 2004); this also however allows a group identity to develop, with its own language, and norms that group participants use to signal membership (Dobusch & Schoeneborn, 2015, McKenna & Green, 2002). These are strong contributors to the formation of an online collective identity and there is still a significant amount of social information available to help users decipher meaning that is not plainly stated. Similarly, Postmes & Brunsting dispute the statement that computers damage social ties (Turkle, 1999), arguing to the contrary, that it has been observed that the Internet "strengthens existing social movements, stimulates the formation of new ones, and mobilizes sizable numbers of people for collective action," (Postmes & Brunsting, 2002:294). There are various studies on the motivations of those who engage in hacking, ranging from financial gain, prestige, curiosity (Seebruck, 2015). These however have not found to be the strongest indicator of the occurrence of participation; when it comes to hacking related involvement it is the "social

motivators (i.e., peer recognition/respect and team-play) and not the personal motivators (i.e., intellectual challenge/curiosity and justice) that are relevant to the frequency of involvement" (Madarie, 2017:93).

Intergroup attribution research (Branscombe & Wann, 1994, Cialdini et al, 1976, Hewstone & Jaspars, 1982, Ho & Lloyd, 1982, Tarrant & North, 2004) has shown that the achievements of group actions can strengthen individual members' beliefs that their group and members are highly skilled. It can also lead group members to attribute the success of opposing groups to external circumstances and luck. This has been thought to encourage online groups to carry out additional actions in hacktivism and against other cyber adversarial groups, especially if the group identity is reinforced, either by the actions involved (combining tactics shown in Tables 2 & 3) or by the subsequent media reporting. It has been observed that early news reports about Anonymous generally exaggerated the cohesiveness between members and the organisational structure of the group (Olson, 2012), which has then contributed to the group becoming more cohesive and organised.

The cohesiveness of newer hacking collectives was affected in 2012 by the exposure of a high profile member of Lulzsec, Sabu, as having been an informant for the FBI. His information led to the arrests of prominent group members in the USA, the UK and Ireland. There have been significant changes to the group behaviours since (Coleman, 2015), with greater antipathy of 'leader-fags', or those wanting to take charge, suspicion of new or unknown members, and of any one who seems to be desiring attention. This is despite repeated claims from groups such as Anonymous that they do not have an official leader or hierarchy (Coleman, 2014). This may or may not be the case, but regardless it is relevant that many members of such collectives believe this to be true, which potentially leaves them open to manipulation. After all, the creation of the internet was heavily influenced by those who wished to see technology move towards a "decentralised, and non-hierarchical version of society," (Rosenzweig, 1998:1552), and so those that follow these ideals may prefer to believe that a non-hierarchy has been achieved, a form of confirmation bias. It cannot be assumed that there is a complete lack of hierarchy in these communities, as there are obvious examples, especially in forums or Internet-Relay Chat (IRC) channels where it is necessary for administrators to moderate the content submitted by users (Dupont et al, 2016, Uitermark, 2016).

Another social element within these communities is the behavioural consequences of trust. Trusting behaviour requires the individual to relinquish control over valuable outcomes with the expectation that the other will reciprocate. On the internet many will openly talk about not trusting others, as there is no way to verify claims. Within hacktivism however, it has been shown that group membership is a strong predictor of trusting behaviour (Tanis & Postmes, 2005). Therefore, those who join a particular group or share a hacktivist identity are more inclined to trust other group members with no other influencing factor. Generalised trust is also believed to make a person more willing to engage in collective efforts and cooperate with other people (Sturgis et al, 2012, Van Lange, 2015), thereby encouraging individuals to take part in hacktivist tactics (see Table 2).

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, Hu et al, 2015, Joinson, 2007, Lapidot-Lefler & Barak, 2015). 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 (McKenna & Green, 2002). This privacy combined with openness is what many involved in hacking and hacktivism claim to want to protect (Levy, 2010).

Within investigations into the elements that predict involvement or carrying out hacktivist actions, there is often a heavy focus on adolescents (Harris-McKoy & Cui, 2013, Wilcox et al, 2003, Wright et al, 2015). Unsurprisingly, one of the strongest factors predicting the change of cyber delinquency in young

people was the amount of computer use (Wilcox et al, 2003, Wright, et al, 2015). This, combined with further studies, has led some to claim that there is a parental responsibility that needs to be acknowledged; a study in Korea concluded that to avoid computer delinquency parents should take responsibility for educating their children about the negative outcomes of illegal or criminal behaviours (Harris-McKoy & Cui, 2013). This is similar to an awareness raising campaign launched by the NCA (2015) in the UK, urging parents to be conscious of what their children might be doing online, and being aware of the legality of their actions.

Such studies as Harris-McKoy and Cui (2013) also highlight the importance of considering cultural differences and approaches. There has been a trend to place more importance on cognitive factors, looking at the cognitive influence on individual perception of risk, which has meant that cultural and social influences are sometimes neglected. The Cultural Theory of Risk however explains that social structures are associated with individual perceptions of societal dangers. Depending on the community and social structures people are used to and the values and social norms they have been taught, people understand risks differently. This means that the values of certain social or cultural contexts shape the individual's perception and evaluation of risks (Rippl, 2002). For example, at a higher level, Eastern cultures stress group solidarity and relationships with other people; Western cultures emphasize the self and autonomy (Wright et al, 2015). The extent to which this is evident in hacking groups is still not known but it must be considered as a factor.

Groupthink is another significant offline group phenomenon must be considered in the online group context (Packer, 2009). Janis (1972) defines groupthink as the psychological drive for consensus at any cost that suppresses is agreement and prevents the appraisal of alternatives in cohesive decision-making groups. He also identified the symptoms of Groupthink, which transpire when a group tries to make decisions. These include the illusion of invulnerability; collective rationalisation; stereotyped views of different groups; group pressure to conform; and self-censorship (Janis, 1972). Although groupthink does not always occur, it is more common when the groups are highly cohesive, especially in high-pressure situations. When there is pressure for agreement it has been found that group members can be more vulnerable to inaccurate and irrational thinking; as such decisions formed by groupthink have reduced probability of attaining successful outcomes (Janis, 1972). This has been seen in some hacktivist attempts, such as the manipulation of individuals to download and use software for DDoS attacks (The Paypal 14, see Coleman, 2014), with little information given and reassurance from other group members that this was a good and constructive action to take for the benefit of their cause. In the case of the PayPal 14, the individuals were later arrested and prosecuted by the US government (Coleman, 2014).

COGNITIVE FACTORS

As the significance of psychology becomes more widely acknowledged within the fields of computing and security, the cognitive factors influencing human behaviour must be re-examined. There are a number of acknowledged biases and heuristics that affect how individuals perceive and understand their surroundings. This section will discuss some of the more common ones that influence decision making and judgement.

There have been many concerns as computing and technology advanced that the "overuse of computers may have a deleterious effect on cognitive functioning" (Vujic, 2017:152). Theoretical-based predictions have so far supported the view that computer and Internet use can have a negative impact

on short-term memory processing and sustained attention (Vujic, 2017). This has spread to the public perception that internet and computer use impair cognitive abilities, and encourage "lazy" patterns of thinking, particularly affecting memory and concentration (Nasi & Koivusilta, 2013). It has been identified that "the quality of computer use may be just as important as the measuring the quantity of computer use" (Vujic, 2017:159). This suggests that those who use computers over long periods of time daily are at greater risk of greater biased cognition, as well as lower attention (Tsohou et al, 2015, Vujic, 2017).

There have however also been studies that suggest evidence of a positive relationship between interactive computer use and cognitive performance (Small et al, 2009, Tun & Lachman, 2010, Vujic, 2017). Comparing a computer/internet "savvy" group and a net "naïve" group, the results revealed the internet "savvy" individuals experienced double the activity increase in the areas of the brain associated with complex reasoning, decision making and visual processing (Small et al., 2009). One explanation for these differences was the concept different "systems" of processing information. The first "System 1" or "bottom-up" is theorised to be automatic, unconscious, heuristic responses with minimal resources; "System 2" or "top-down" is considered resource-intensive and attention driven (Evans, 2003, Slovic et al, 2002, Vujic, 2017), requiring more mental effort, which is harder to sustain.

When it comes decision making and judgements, individuals have been found to over-rely on heuristics such as such as availability, and anchoring, therefore using simplified strategies to make choices (Tversky, 1972), without recognising the bias. The availability heuristic implies that in any decision-making process, easily remembered information is given greater weight by decision makers. In this way, recent events and vivid memories are given more importance by the individuals or groups as they are easier to recall (Tsohou et al, 2015), which allows potentially inaccurate information to be the basis of their decision. In a numerical comparison, anchoring is when an individual's numerical estimate is influenced toward an arbitrary value. Final estimations are strongly swayed by the initial value provided, making it easier to manipulate individuals when giving them initial information (Tsohou et al, 2015).

The affect heuristic is when an individual makes judgments and decisions quickly based on their emotional impressions. A common outcome of the affect heuristic is that people tend to underestimate risks and costs connected with things they like, and overestimate the risks and costs when they are related to things they dislike (Tsohou et al, 2015). Similarly, confirmation bias is where people tend to seek information that is consistent with their current hypothesis and are unlikely to seek information expected to be inconsistent with it (Chapman and Johnson, 2002, Tsohou et al, 2015). This is sometimes seen in social movement behaviours (see Table 3), where members will not look for external sources of information, trusting the other group members (as per generalised trust). Confirmation bias is considered to be one of the most prominent biases affecting decision making (Kahneman et al., 2011).

These attributes and biases are present in hacktivist groups, with many accounts from Anonymous members or former members having examples of optimism bias. Optimism bias leads individuals have a consistent tendency to believe that they are less at risk of experiencing a negative event themselves compared to others (Tsohou et al, 2015), therefore even if they did take part in an illegal activity they would be at less risk of being tracked by law enforcement agencies. This has been disproved through the arrests of those involved in Lulzsec, the PayPal 14, the TalkTalk hack, and Crackas with Attitude (Coleman, 2014, Farrell, 2016, Olsen, 2012, Whitehead, 2016). When recounting their individual experiences within the groups, the individuals stated that they were aware of the risk, aware that they were carrying out illegal actions but felt that they would not be caught, in part because they were aware of the risk and "it wouldn't happen to them" (Olsen, 2012, Coleman, 2014).

CONCLUSION

This chapter has provided a brief introduction to hacktivism and social protest online, and highlighted some of the socio-psychological and cognitive factors that can lead to individuals taking part in hacktivism groups. As stated, hacktivism is an ill-defined area which some people claim as a legitimate form of protest in the online world, and others regard as illegal hacking; there is truth to both arguments. Those who believe it should be protected will continue to work for it to be recognised. In terms of further study this area has a lot of potential for future research. The depth of social ties and influence is still being examined; and whilst cognitive biases are recognised, strategies to mitigate and combat the vulnerability they present are still being developed. What is clear from many studies and examples is that hackers are often skilled and intelligent individuals, who can offer a lot of knowledge and information. As the world continues to become more integrated with the online world, their knowledge and skill becomes even more valuable. The policies and laws that govern the internet need to be made with a greater awareness of the online world, and steps should be taken to protect the internet as the free, open and invaluable resource that it is.

REFERENCES

Anderson, B. (1983). *Imagined communities: Reflections on the origin and spread of nationalism*. London: Verso.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265–300). Berlin: Springer. doi:10.1007/978-3-642-39498-0_12

Bae, S. M. (2017). The influence of strain factors, social control factors, self-control and computer use on adolescent cyber delinquency: Korean National Panel Study. *Children and Youth Services Review*, *78*, 74–80. doi:10.1016/j.childyouth.2017.05.008

Benjamin, V., Zhang, B., Nunamaker, J. F. Jr, & Chen, H. (2016). Examining Hacker Participation Length in Cybercriminal Internet-Relay-Chat Communities. *Journal of Management Information Systems*, *33*(2), 482–510. doi:10.1080/07421222.2016.1205918

Branscombe, N. R., & Wann, D. L. (1994). Collective self-esteem consequences of outgroup derogation when a valued social identity is on trial. *European Journal of Social Psychology*, *24*(6), 641–657. doi:10.1002/ejsp.2420240603

Cialdini, R. B., Borden, R. J., Thorne, A., Walker, M. R., Freeman, S., & Sloan, L. R. (1976). Basking in reflected glory: Three (football) field studies. *Journal of Personality and Social Psychology*, *34*(3), 366–375. doi:10.1037/0022-3514.34.3.366

Clough, J. (2010). Principles of Cybercrime. Cambridge University Press. doi:10.1017/CBO9780511845123

Coleman, G. (2011). Hacker politics and publics. *Public Culture, 23*(65), 511-516.

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* (pp. 401–461). London: Verso.

Dobusch, L., & Schoeneborn, D. (2015). Fluidity, Identity, and Organizationality: The Communicative Constitution of Anonymous. *Journal of Management Studies*, *52*(8), 1005–1035. doi:10.1111/joms.12139

Douglas, D., Santanna, J.J., de Oliveira Schmidt, R., Granville, L.Z., & Pras, A. (2017). Booters: Can Anything Justify Distributed Denial-of-Service (DDoS) Attacks for Hire? *Journal of Information, Communication and Ethics in Society, 15*(1).

Drucker, S., & Gumpert, G. (2000). Cybercrime and punishment. *Critical Studies in Media Communication*, *17*(2), 133–158. doi:10.1080/15295030009388387

Dupont, B., Côté, A., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime*, *17*(2), 129–151. doi:10.1080/17440572.2016.1157480

Evans, J. S. B. (2003). In two minds: Dual-process accounts of reasoning. *Trends in Cognitive Sciences*, *7*(10), 454–459. doi:10.1016/j.tics.2003.08.012 PMID:14550493

Farrell, S. (2016). TalkTalk counts costs of cyber-attack. *The Guardian*. Retrieved from https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave accessed 24/09/16

Festinger, L. (1950). Informal social communication. *Psychological Review*, *57*(5), 271–282. doi:10.1037/h0056932 PMID:14776174

Goode, L. (2015). Anonymous and the political ethos of hacktivism. *Popular Communication*, *13*(1), 74–86. doi:10.1080/15405702.2014.978000

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA: IGI Global.

Hampson, N. C. (2012). Hacktivism: A new breed of protest in a networked world. *BC Int'l & Comp. L. Rev.*, *35*, 511.

Hanna, P., Vanclay, F., Langdon, E. J., & Arts, J. (2016). Conceptualizing social protest and the significance of protest actions to large projects. *The Extractive Industries and Society*, *3*(1), 217–239. doi:10.1016/j.exis.2015.10.006

Harris-McKoy, D., & Cui, M. (2013). Parental control, adolescent delinquency, and young adult criminal behavior. *Journal of Child and Family Studies*, *22*(6), 836–843. doi:10.1007/s10826-012-9641-x

Hewstone, M., & Jaspars, J. M. F. (1982). Intergroup relations and attribution processes. In H. Tajfel (Ed.), *Social Identity and Intergroup Relations* (pp. 99–133). Cambridge, UK: Cambridge University Press.

Ho, R., & Lloyd, J. I. (1983). Intergroup attribution: The role of social categories in causal attribution for behaviour. *Australian Journal of Psychology*, *35*(1), 49–59. doi:10.1080/00049538308255302

Hu, C., Zhao, L., & Huang, J. (2015). Achieving self-congruency? Examining why individuals reconstruct their virtual identity in communities of interest established within social network platforms. *Computers in Human Behavior*, *50*, 465–475. doi:10.1016/j.chb.2015.04.027

Janis, I. L. (1972). *Victims of Groupthink*. New York: Houghton Mifflin.

Jensen, E. T. (2015). Cyber sovereignty: The way ahead. *Tex. Int'l LJ*, *50*, 275.

Joinson, A. N. (2007). Disinhibition and the Internet. In J. Gackenbach (Ed.), *Psychology and the Internet: Intrapersonal, interpersonal, and transpersonal implications* (2nd ed.; pp. 75–92). San Diego, CA: Academic Press. doi:10.1016/B978-012369425-6/50023-0

Jordan, T. (2001). Mapping hacktivism: Mass virtual direct action (MVDA), individual virtual direct action (IVDA) and cyber-wars. *Computer Fraud & Security*, *4*(4), 8–11. doi:10.1016/S1361-3723(01)00416-X

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757–780. doi:10.1111/1467-954X.00139

Krapp, P. (2005). Terror and play; or what was hacktivism? *Grey Room MIT Press*, *21*, 70–93. doi:10.1162/152638105774539770

Kubitschko, S. (2015). Hackers' media practices: Demonstrating and articulating expertise as interlocking arrangements. *Convergence*, *21*(3), 388–402. doi:10.1177/1354856515579847

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), article 3.

Leach, D. K. (2009). An elusive 'we': Anti-dogmatism, democratic practice, and the contradictory identity of the German Autonomen. *The American Behavioral Scientist*, *52*(7), 1042–1068. doi:10.1177/0002764208327674

Levy, S. (2010). *Hackers: Heroes of the Computer Revolution*. Sebastopol, CA: O'Reilly Media.

Madarie, R. (2017). Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. *International Journal of Cyber Criminology*, *11*(1).

Manion, M., & Goodrum, A. (2000). Terrorism or civil disobedience: Toward a hacktivist ethic. *ACM SIGCAS Computers and Society*, *30*(2), 14–19. doi:10.1145/572230.572232

Matusitz, J. (2005). Cyberterrorism: How Can American Foreign Policy Be Strengthened in the Information Age? *American Foreign Policy Interests*, *27*(2), 137–147. doi:10.1080/10803920590935376

McKenna, K. Y., & Green, A. S. (2002). Virtual group dynamics. *Group Dynamics*, *6*(1), 116–127. doi:10.1037/1089-2699.6.1.116

Meuleman, B., & Boushel, C. (2014). Hashtags, ruling relations and the everyday: Institutional ethnography insights on social movements. *Contemporary Social Science*, *9*(1), 49–62. doi:10.1080/21582041.2013.851410

Milan, S., & Atton, C. (2015). Hacktivism as a radical media practice. *Routledge companion to alternative and community media*, 550-560.

Moore, R. (2005). *Cyber crime: Investigating High-Technology Computer Crime*. Cleveland, MI: Anderson Publishing.

Näsi, M., & Koivusilta, L. (2013). Internet and everyday life: The perceived implications of internet use on memory and ability to concentrate. *Cyberpsychology, Behavior, and Social Networking*, *16*(2), 88–93. doi:10.1089/cyber.2012.0058 PMID:23113691

NCA. (2016). *Cyber crime: Preventing young people from getting involved*. National Crime Agency. Retrieved from http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media & Society*, *6*(2), 195–217. doi:10.1177/1461444804041445

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

Packer, D. J. (2009). Avoiding groupthink: Whereas weakly identified members remain silent, strongly identified members dissent about collective problems. *Psychological Science*, *20*(5), 546–548. doi:10.1111/j.1467-9280.2009.02333.x PMID:19389133

Perlroth, N. (2013, May 17). Hunting for Syrian hackers' Chain of Command. *New York Times*. Retrieved from https://nyti.ms/2jPZmbx

Postill, J. (2014). Freedom technologists and the new protest movements: A theory of protest formulas. *Convergence*, *20*(4), 402–418. doi:10.1177/1354856514541350

Postmes, T., & Brunsting, S. (2002). Collective action in the age of the Internet: Mass communication and online mobilization. *Social Science Computer Review*, *20*(3), 290–301. doi:10.1177/089443930202000306

Raymond, E. (1996). *The New Hacker's Dictionary*. MIT Press.

Rippl, S. (2002). Cultural theory and risk perception: A proposal for a better measurement. *Journal of Risk Research*, *5*(2), 147–165. doi:10.1080/13669870110042598

Rogers, M. (2003). The psychology of cyber-terrorism. Terrorists, Victims and Society: Psychological. *Perspectives on Terrorism and Its Consequences*, 75-92.

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation*, *3*(2), 97–102. doi:10.1016/j.diin.2006.03.001

Rogers, M. K. (2011). The psyche of cybercriminals: A psycho-Social perspective. In Cybercrimes: A multidisciplinary analysis (pp. 217-235). Springer. doi:10.1007/978-3-642-13547-7_14

Rosenzweig, R. (1998). Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet. *The American Historical Review*, *103*(5), 1530–1552. doi:10.2307/2649970

Scheuerman, W. E. (2016). Digital disobedience and the law. *New Political Science*, *38*(3), 299–314. doi:10.1080/07393148.2016.1189027

Schrock, A. R. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. *New Media & Society*, *18*(4), 581–599. doi:10.1177/1461444816629469

Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation*, *14*, 36–45. doi:10.1016/j.diin.2015.07.002

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*, *34*(4), 495–518. doi:10.1177/0022427897034004005

Slovic, P., Finucane, M., Peters, E., & MacGregor, D. G. (2002). Rational actors or rational fools: Implications of the affect heuristic for behavioural economics. *Journal of Socio-Economics*, *31*(4), 329–342. doi:10.1016/S1053-5357(02)00174-9

Small, G. W., Moody, T. D., Siddarth, P., & Bookheimer, S. Y. (2009). Your brain on Google: Patterns of cerebral activation during internet searching. *The American Journal of Geriatric Psychiatry*, *17*(2), 116–126. doi:10.1097/JGP.0b013e3181953a02 PMID:19155745

Solomon, R. (2017). Electronic protests: Hacktivism as a form of protest in Uganda. *Computer Law & Security Review*, *33*(5), 718–728. doi:10.1016/j.clsr.2017.03.024

Sturgis, P., Patulny, R., Allum, N., & Buscha, F. (2012). Social connectedness and generalized trust: a longitudinal perspective. *ISER Working Paper Series*, 1-23.

Suler, J. (2004). The Online Disinhibition Effect. *Cyberpsychology & Behavior*, *7*(3), 321–326. doi:10.1089/1094931041291295 PMID:15257832

Tanczer, L. M. (2016). Hacktivism and the male-only stereotype. *New Media & Society*, *18*(8), 1599–1615. doi:10.1177/1461444814567983

Tanis, M., & Postmes, T. (2005). A social identity approach to trust: Interpersonal perception, group membership and trusting behaviour. *European Journal of Social Psychology*, *35*(3), 413–424. doi:10.1002/ejsp.256

Tarrant, M., & North, A. C. (2004). Explanations for positive and negative behavior: The intergroup attribution bias in achieved groups. *Current Psychology (New Brunswick, N.J.)*, *23*(161). doi:10.1007/BF02903076

Travaglino, G. A. (2014). Social sciences and social movements: The theoretical context. *Contemporary Social Science*, *9*(1), 1–14. doi:10.1080/21582041.2013.851406

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, *52*, 128–141. doi:10.1016/j.cose.2015.04.006

Tufekci, Z., & Wilson, C. (2012). Social media and the decision to participate in political protest: Observations from Tahrir Square. *Journal of Communication*, *62*(2), 363–379. doi:10.1111/j.1460-2466.2012.01629.x

Tun, P. A., & Lachman, M. E. (2010). The association between computer use and cognition across adulthood: Use it so you won't lose it? *Psychology and Aging*, *25*(3), 560–568. doi:10.1037/a0019543 PMID:20677884

Turkle, S. (1999). Cyberspace and Identity. *Contemporary Sociology, 28*(6), 643–648.

Tversky, A. (1972). Elimination by aspects: A theory of choice. *Psychological Review*, *79*(4), 281–299. doi:10.1037/h0032955

Uitermark, J. (2017). Complex contention: Analyzing power dynamics within Anonymous. *Social Movement Studies*, *16*(4), 403–417. doi:10.1080/14742837.2016.1184136

UN General Assembly. (1966). *International Covenant on Civil and Political Rights*. Available at: http://www.refworld.org/docid/3ae6b3aa0.html

Valenzuela, S. (2013). Unpacking the use of social media for protest behavior: The roles of information, opinion expression, and activism. *The American Behavioral Scientist*, *57*(7), 920–942. doi:10.1177/0002764213479375

Van Lange, P. A. M. (2015). Generalized Trust: Four Lessons From Genetics and Culture. *Current Directions in Psychological Science*, *24*(1), 71–76. doi:10.1177/0963721414552473

Vegh, S., Ayers, M. D., & McCaughey, M. (2003). Classifying forms of online activism. In M. McCaughey & M. Ayers (Eds.), *Cyberactivism: Online Activism in Theory and Practice* (pp. 71–96). London: Routledge.

Vujic, A. (2017). Switching on or switching off? Everyday computer use as a predictor of sustained attention and cognitive reflection. *Computers in Human Behavior*, *72*, 152–162. doi:10.1016/j.chb.2017.02.040

Whitehead, T. (2016). British teenager suspected of being a mystery hacker who stole CIA boss emails. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/uknews/crime/12154592/British-teenager-suspected-of-being-a-mystery-hacker-who-stole-CIA-boss-emails.html

Wilcox, P., Land, K., & Hunt, S. A. (2004). Criminal circumstance: A multicontextual criminal opportunity theory. *Symbolic Interaction*, *27*(1).

Wolfradt, U., & Doll, J. (2001). Motives of Adolescents to use the internet as a function of personality traits, personal and social factors. *Journal of Educational Computing Research*, *24*(1), 13–27. doi:10.2190/ANPM-LN97-AUT2-D2EJ

Wray, S. (1998). Electronic civil disobedience and the World Wide Web of hacktivism. *Switch New Media Journal, 4*(2). Retrieved from http://switch.sjsu.edu/web/v4n2/stefan/

Wright, M. F., Kamble, S. V., & Soudi, S. P. (2015). Indian adolescents' cyber aggression involvement and cultural values: The moderation of peer attachment. *School Psychology International*, *36*(4), 410–427. doi:10.1177/0143034315584696