Combating Violent Extremism and Radicalization in the Digital Era

Majeed Khader
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Loo Seng Neo
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Gabriel Ong
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Eunice Tan Mingyi
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Jeffery Chin
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

A volume in the Advances in Religious and
Cultural Studies (ARCS) Book Series

Information Science
REFERENCE
An Imprint of IGI Global

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Khader, Majeed, 1966- editor.
Title: Combating violent extremism and radicalization in the digital era / Majeed Khader, Loo Seng Neo, Gabriel Ong, Eunice Tan Mingyi, and Jeffery Chin, editors.
Description: Hershey, PA : Information Science Reference, [2016] | Includes bibliographical references and index.
Identifiers: LCCN 2015051297| ISBN 9781522501565 (hardcover) | ISBN 9781522501572 (ebook)
Subjects: LCSH: Cyberterrorism. | Internet and terrorism. | Extremist Web sites. | Terrorists--Recruiting. | Radicalism. | Terrorism--Prevention.
Classification: LCC HV6773.15.C97 C65 2016 | DDC 363.325--dc 3 LC record available at http://lccn.loc.gov/2015051297

This book is published in the IGI Global book series Advances in Religious and Cultural Studies (ARCS) (ISSN: Pending; eISSN: Pending)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.

Chapter 6
Understanding Personality and Person-Specific Predictors of Cyber-Based Insider Threat

Joyce S. Pang
Nanyang Technological University, Singapore

ABSTRACT

The chapter aims to provide an opinion on major challenges for ongoing personality research on cyber security, especially in the area of insider threat. While research on the prevention and perpetuation of insider threat activity within cyberspace has grown substantially in the recent decade, there remain many unanswered challenges and unchartered territories of knowledge in the field. Specifically, compared to the amount of work done on algorithmic modelling approaches, much of the psychological data is scant and focuses on correlations between the so-called Big Five personality traits (i.e., extraversion, openness to experience, agreeableness, emotional stability, conscientiousness) or demographic variables (e.g., gender, age) with insider threat activity. Thus, the focus of this article is to articulate the major challenges for understanding insider threat in the context of cyber security, particularly from a personality and person-specific perspective that emphasises internal characteristics of the individual actor as explanations of actions and events.

INTRODUCTION AND GENERAL APPROACH

The aim of this chapter is to provide an opinion on the major challenges for ongoing personality research on cyber security, especially in the area of insider threat. Cyber security refers to the field involved in the monitoring of criminal activities in cyberspace, in order to maintain a safe environment for the transfer of resources and for the dissemination and protection of information. Insider threat refers to the presence of trusted individuals who are either members of an organisation or who have privileged access to organisation resources, and who engage in activities from within the organisation to threaten the interests of that organisation (cf. Probst, Hunker, Gollmann, & Bishop, 2010). In relation to cyber security, the major categories of insider threat are IT sabotage, fraud, theft of intellectual property (IP

DOI: 10.4018/978-1-5225-0156-5.ch006

theft), and espionage. While research on the prevention and perpetuation of insider threat activity within cyberspace has grown substantially in the recent decade, there remain many unanswered challenges and unchartered territories of knowledge in the field. Specifically, compared to the amount of work done on logging software and algorithmic modelling approaches, relatively less work has been carried out to clarify the important psychological and sociological factors for cyber security and for insider threat. Importantly, much of the psychological data is scant and focuses on correlations between the so-called Big Five personality traits (i.e., extraversion, openness to experience, agreeableness, emotional stability, conscientiousness; John & Srivastava, 1999; see Axelrad, Sticha, Brdiczka, & Shen, 2013, for an example of a Bayesian network model of insider threat using the Big Five traits) or demographic variables (e.g., gender and age; see Chang & Lim, 2014) with insider threat activity. Thus, the focus of this chapter is to articulate the major challenges for understanding insider threat in the context of cyber security, particularly from a personality and person-specific perspective.

By a 'personality and person-specific perspective', I am referring to a perspective that emphasises internal characteristics of the individual actor as explanations of actions and events. These internal characteristics can come from personality dimensions – which are a system of thoughts, feelings, and behaviours that an individual exhibits consistently across time and over situations – or they can come from person-specific dimensions that are externally ascribed to an individual usually because of his or her social category. Examples of personality dimensions are traits (e.g., extraversion), explanatory styles (e.g., pessimism), motives (e.g., power motivation), skills and competencies (e.g., intelligence, creativity), and values (e.g., benevolence). Individuals differ on these personality dimensions because of biology, influence from social contexts, upbringing, and exposure to significant others, as well as through a combination of learning experiences and interaction with social and physical environments. Examples of person-specific dimensions include gender, age, and socioeconomic class.

There are two major decisions for a behavioural scientist who is trying to understand person-specific characteristics of cyber-based insider threat; these involve the questions of what and how to study cybercrime and insider threat. In considering the question of what should be studied, I will make use of the excellent groundwork carried out recently by researchers in the fields of cyber security and insider threat. I will conduct a targeted review of recently published frameworks for understanding insider threat, specifically the models of Nurse et al. (2014) and Moore et al. (2011).

Whilst Nurse and colleagues did an admirable job of summarising main themes in the field, their framework is relatively general and thus allows for much more categories of study to be uncovered. Hence, Nurse at al.'s (2014) model can be a jumping off point, from which I will discuss more context-specific areas for future research inquiry, such as regarding the motivation of offenders.

I will also discuss offender profiles and types of cyber-insiders, using recent work by Moore and colleagues. Moore, Cappelli, and Trzeciak (2008) and Moore et al. (2011) have provided some insight into offender profiles in insider crime, specifically in the areas of fraud and IP theft. Using research in the related fields of organisational psychology and personality psychology (e.g., Murphy & Dacin, 2011), I suggest some extensions of Moore and colleagues' work by identifying some other promising variables and/or productive dimensions for categorising cyber offenders of insider attacks.

For the question of how to study cyber-based insider attacks, in the latter part of the chapter, I will discuss some methodological considerations, such as how to derive an approach for the field that is both theory and data driven, and how psychological and behavioural data should be collected and/or treated for validation purposes and for application purposes.

NURSE ET AL.'S (2014) MODEL FOR CHARACTERISING INSIDER ATTACKS

Nurse and his colleagues (2014) set out to formulate a framework of the insider threat problem. In order to do so, they collected a dataset of 80 insider threat cases from various sources, including CERT (Computer Emergency Response Team; for more information, see Cappelli, Moore, & Trzeciak, 2012) and CPNI (Centre for the Protection of National Infrastructure), as well as various news sources in the United States and the United Kingdom. They then analysed each case, as well as consulted literature in order to come up with consistent themes and relationships.

There are four major sections in Nurse et al.'s (2014) framework: the *catalyst* or precipitating event that triggers the insider attack; *actor* characteristics of the offender; *attack* characteristics; and *organisational* characteristics. For this review, since we are concerned with the personality of the offender, we will limit our discussion to the portion of the model that discusses actor characteristics.

Nurse et al. (2014) take a dimensional approach to understand the person characteristics of the offender in insider attacks. There are 12 elements in the insider/actor characteristics in Nurse et al.'s model. These are: personality characteristics, historical behaviour, psychological state, attitude towards work, motivation to attack, skill set, opportunity, enterprise role, type of actor, state of relationship, observed physical behaviour, and observed cyber behaviour. In general, all these elements also apply to cyber-based offenders conducting insider attacks. However, I propose that further research is needed, particularly in three key elements of personality – personality characteristics of the actor, the actor's current psychological state, and the actor's motivation to attack – before personality researchers can adapt the model more specifically to cyber security.

Personality Characteristics

Personality characteristics discussed by Nurse et al. (2014) mostly belong to the category of dispositions best described as static. Specifically, static notions of personality see dispositional characteristics as being relatively stable and enduring. In other words, it is assumed that, after a certain period of development, there is a stability of beliefs, attitudes, cognitions, and emotions in the style and content of interactions between an individual and his/her environment. Moreover, there is also the assumption that static personality is resistant to change (such as via the process of maturation, or because of exposure to traumatic and/or significant life events). This view of personality is encapsulated in James' (1890) famous comment that most of the character is 'set in plaster' by the age of thirty. In this type of conceptualisation, assessments of personality display relatively high test-retest and inter-rater reliability[1].

There are some dimensions of personality (e.g., traits, temperaments), which display relatively high temporal stability, and thus can be easily classified as static. Specifically, there is ample evidence that the traits of neuroticism, extroversion, and openness exhibit only small declines, and that agreeableness and conscientiousness exhibit only small increases from ages 20 to 40, and moreover, there is little change thereafter (Duggan, 2004).

However, most personality characteristics tend to be dynamic. In dynamic notions of personality (e.g., Costa & McCrae, 1994), basic tendencies and innate characteristics such as biological tendencies, temperaments, intelligence, gender, etc. interact with the environment to produce so-called characteristic adaptations. These adaptations manifest in the form of dimensions of personality, such as attitudes, values, and other traits. For instance, the person might possess a certain degree of general intelligence (basic tendency) which, when exposed to a stimulating home environment and a challenging school environment, produces conscientiousness (a trait) and high need for achievement (a motive), both of which are characteristic adaptations. Following this line of reasoning, even though there are some personality dimensions that are relatively stable (e.g., a controlled temperament), these stable dimensions could still lead to a variety of different behavioural outcomes (e.g., depression versus overachievement), depending on the specific environment to which the person is exposed (troubled home environment versus competitive school environment). Another particularly important point which Moore, Detert, Treviño, Baker, and Mayer (2012) also mention is that all the person-specific and personality dimensions, whether they are basic tendencies or characteristic adaptations, are interlinked and interact with each other. In this way, personality characteristics are dynamic and mutually interacting, which makes them more difficult to assess or to model. Nonetheless, there is evidence of some predictive validity for a combination of personality traits that seem to go together in predicting unethical work or counterproductive work behaviours. Specifically, counterproductive workplace behaviours are typically perpetrated by those with high negative emotionality or high neuroticism, low agreeableness, and low conscientiousness (see Salgado, 2002; Marcus, Lee, & Ashton, 2007).

Another reason that many actor characteristics should be treated as dynamic is because of the need to consider the local context when considering the interaction of all the actor characteristics. For instance, a practitioner who is seeking to use personality research to predict behavioural outcomes would not only need to know the type of behaviour a personality trait predicts, but also the specific environmental condition that is most likely to cause the behaviour to manifest. It is precisely because of the influence of context and the dynamic nature of many personality traits, that many researchers of criminal behaviour have found that risk assessments that are based on personality inventories exhibit only moderate levels of inter-rater and field reliability ranging around 0.6-0.75 (e.g., Miller, Kimonis, Otto, Kline, & Wasserman, 2012). It is likely that some items on these personality based risk assessments are less susceptible to contextual influences than others, and these items would hence display relatively higher inter-rater and field reliabilities. Future research is needed to assess which particular items of standard risk assessment instruments display better rater agreement than others. Another precaution that practitioners interested in personality based risk assessments of insider threat can take is to bear in mind that such instruments should only play a secondary role in informing decisions about personnel selection and monitoring, especially in high-pressure, high-stakes environments, like legal judgments and national security.

Regrettably, most of the work done on insider threat and in the related field of counterproductive work behaviour (see Sackett, Berry, Wiemann, & Laczo, 2006) has focused on static personality characteristics like the Big Five personality traits of extraversion, conscientiousness, openness to experience, emotional stability, and agreeableness. In this line of research, typical findings are that personality traits such as Machiavellianism and neuroticism are positively associated with counterproductive work behaviour (e.g., Marcus & Schuler, 2004) or with insider threat activity (e.g., Axelrad et al., 2013). While they are helpful in describing the structure of personality and in developing typologies for typical offender profiles, conceptions of personality that are solely trait-based have limited field validity because a purely descriptive taxonomy of between-person individual differences does not address why the same person will behave differently across different situations (Cervone, Shoda, & Downey, 2007; cf. Graber, Laurenceau, & Carver, 2011).

Instead of seeing personality as a constellation of traits, popular contemporary notions of personality (e.g., the Cognitive-Affective Processing System [CAPS]; Mischel & Shoda, 1995) emphasise a more process-oriented view that represents the individual as a combination of different dimensions (which includes traits but also other dimensions of personality) that continually interact and transact with the environment. In these process-oriented models, individuals exhibit behavioural signatures, which work in a contingent, if-then fashion. In other words, traits can predict behavioural outcomes only in certain situations, and only if the traits are activated within and/or applicable to that specific situation. For instance, following Mischel and Shoda's (1995) CAPS model, Graber et al. (2011) developed a multilevel-modelling framework for studying personality and close dyadic relationships. In their model, personality is conceptualised as the person-specific factor of relationship satisfaction. Specifically, individuals may differ in the general degree to which they experience relationship satisfaction. Graber et al.'s (2011) final multilevel model showed that degree of relationship satisfaction is related to person-specific differences in propensity to experience relationship satisfaction as well as the outcome of negative behaviours towards one's partner, in a complex fashion. Specifically, there is within-person variability in relationship satisfaction on a day-to-day level over the 21 days of their study, and there is also between-person variability in relationship threat (i.e., the amount of conflict the couple experiences during each day). The day-to-day variation in relationship satisfaction is related to the day-to-day variation in between-person variability in relationship threat, which in turn is related to the overall between-person variation in amount of negative behaviours each individual expresses to their partner.

This type of analysis of personality in research like Graber et al.'s (2011; see also Cooper, Barber, Zhaoyang, & Talley, 2010, for an example with multilevel modelling of sexually deviant behaviour) illustrates that personality and person-specific variables are linked to behavioural outcomes through a complex series of interactions with the environment (e.g., the level of conflict with one's partner on a day-to-day basis). Accordingly, in order to increase the predictive value of trait-based conceptualisations of personality, researchers should focus on developing process-based models of insider threat behaviour that takes into account interactions with elements of the environment (e.g., day-to-day social interactions with co-workers, superiors, and subordinates). Researchers could also search for other trait-based variables that have specifically been developed to explain the behaviours that are more relevant to insider threats. For instance, subclinical psychopathy has been examined as a better predictor than Big Five traits in the specific context of counterproductive work behaviours (Scherer, Baysinger, Zolynsky, & LeBreton, 2013). By examining more specific traits that incorporate psychological elements related to the environment of interest (rather than broad super-traits), savvy researchers would improve the external validity of their predictive models.

Certain personality elements, however, are relatively easier to quantify since they are likely to exhibit minimal change over time and/or are unlikely to fluctuate highly alongside micro-contextual variations. Some examples of these person-specific elements in Nurse et al.'s (2014) model which are relatively resistant to change – and thus more easy to assess and to include in an algorithmic predictive model – include historical behaviour and skill set.

Historical behaviour, particularly, could be an area where large knowledge increments can be accrued, and where improvements to modelling approaches can be made easily. For instance, in general, historical behaviour refers to a set of behaviours that the insider has engaged in during the immediate past, and which taken together suggest a consistent pattern of responses that are indicative of the insider's personality characteristics. Specifically, historical behaviours could include previous criminal acts, risky or addictive practices, and other serious rule violations that may or may not be classified as insider threat behaviours. These kinds of behaviours are all indicative of an underlying personality characteristic, which could arguably be described as anti-social tendency.

The idea of historical behaviours is conceptually equivalent to the habit construct in personality psychology. Habits are behaviours that are performed frequently in stable contexts (Hull, 1943; see

Wood & Neal, 2007). As a part of personality, habits are defined as "learned dispositions to repeat past responses. They are triggered by features of the context that have covaried frequently with past performance" (Wood & Neal, 2007, p. 843). Because a habit tends to be formed through the frequent, unintentional, and repeated occurrences of a response in a specific context, habits are often stable and resistant to long-term change. In situations that do not engender much deliberated action, habits guide behaviour rapidly and efficiently. Researchers interested in assessing historical behaviours and habits can easily do so by assessing frequencies of behaviours that are assumed to be related to insider threat[2].

Psychological State

In Nurse et al.'s (2014) model, the psychological state refers to the insider's short-term emotional and psychological state. This is the aspect that is perhaps the most difficult to assess and to quantify, because of the nature of emotional states being automatic, transient and rapidly cycling, as well as relatively inaccessible to conscious awareness. More research is needed in order to either develop relevant implicit measures of affect or to validate the use of standardised implicit measures of affect in psychological studies of cyber security and of insider attacks. The problem is that questionnaire measures of affect are reactive measures, in the sense that respondents often react to the act of taking the test, and this awareness of their responses is likely to cause them to subtly alter their responses. Most respondents of questionnaire measures would be reluctant to report extreme negative emotion, for example. Additionally, the possibility of response sets, for instance, the tendency to 'fake-good' or 'fake-bad' on Likert-type personality tests has been consistently demonstrated (cf. Bagby, Buis, & Nicholson, 1995). Hence, there is a need to select measures of emotion that are non-reactive. However, the good news is that non-reactive measures of affect and emotion are already readily available in psychological research, and can easily be transplanted for use in cyber security research. Examples of non-reactive measures of affect and emotion include the Implicit Positive and Negative Affect Test [IPANAT] (Quirin & Bode, 2014) and the Emotion Regulation Implicit Association Test [ER-IAT] (Mauss, Evers, Wilhelm, & Gross, 2006)[3].

Another interesting point about the study of emotional states of cyber-based insiders is the distinction between the actor's emotional content and his or her emotional style. This is a distinction (i.e., about emotions) that could be useful, but which is not commonly embraced by current researchers of cyber security. Specifically, while emotional content typically refers to the emotional state of an individual, which is susceptible to rapid moment-to-moment changes, emotional style refers to a stable characteristic way of reacting emotionally to events. Different emotional styles can be described, such as the tendency to react with positive emotions frequently and in response to ambiguous events (positive emotional style), or the tendency to react with negative emotions frequently and in response to ambiguous events (negative emotional style), or the tendency towards experiencing strong negative as well as strong positive emotions frequently and in response to ambiguous events (dialectical emotional style). While emotional content – currently commonly assessed in insider threat research – might differ dramatically from moment-to-moment, emotional style is relatively stable and influenced by other personality attributes as well as by culturally appropriate norms for emotional expressiveness (e.g., Miyamoto & Ryff, 2011).

Motivation to Attack

Motivation to attack refers to the specific reason for an insider attack. At present, most researchers of insider threat define motivation as the explicit reasons for the attack, which the attackers attribute to themselves or which investigators might attribute to the insiders, through extrapolation from personal circumstances and known external triggers of the attack. Common reasons include financial gain, revenge, political advantage, curiosity, boredom, etc. However, this way of looking at motivation (as self-attributed or other-declared reasons for the attack) primarily deals with the short-term motivational state of the offender, at the moment of the attack. These reasons for offending are state-like, most likely triggered by the circumstances, actors, and events in the immediate context, and hence difficult to assess before the fact. I would like to propose that, instead of studying state-based reasons for offending, researchers should turn their attention to trait-based notions of the motives of the offenders. In other words, individuals could be chronically motivated to fulfil certain needs. Moreover, there would be individual differences for these motives such that some people are perpetually more motivated than others by certain psychological needs. For instance, personality research suggests that people are differentially motivated by their need for power, affiliation, or achievement (McClelland, 1987).

Classic personality research shows that individual differences in these needs affect people's long-term goal-directed behaviour in important personal and social domains. Of particular relevance is power motivation: people motivated by their need for power are more likely to engage in antisocial and dominance-seeking aggressive behaviours. For instance, U.S. presidents with high power motivation tend to be more war mongering but are also more likely to be seen as effective leaders from a historical perspective (Winter, 1987). The level of power motivation between parties in a dyadic negotiation has also been shown to determine whether or not the conflict will escalate – an increase in power motivation of one party in the negotiation is typically followed by concomitant conflict-escalating behaviour of the other party (Winter, 2004). On the other hand, when communications between parties in a negotiation contain relatively more affiliation motive imagery than power motive imagery, the conflict tends to de-escalate. This and other research on motivation, illustrate the importance of accounting for the context when predicting behaviour from personality. Specifically, the motives of important others in the social interaction affect whether one's motives manifest in behaviour. Thus, motives are often seen as dynamic personality variables that wax and wane according to the degree to which environmental conditions encourage their expression.

A major problem for using self-attributed, short-term reasons to understand the motivation behind insider attacks, is that measures of these reasons are typically self-report, questionnaire measures. Once again, the issue of respondent reactivity applies. Moreover, people are notoriously unreliable in reporting their motives since motives tend to operate at an implicit level, largely away from conscious cognition (cf. McClelland, Koestner, & Weinberger, 1989). As discussed later, in personality research, non-reactive measures of chronic dispositions like motives for power, affiliation, and achievement are readily available (e.g., Schultheiss & Pang, 2007), and could be used for future investigations of motivations behind insider threat.

MOORE ET AL.'S (2011) MODEL OF INSIDER IP THEFT

IP theft, a major category of insider cyber attacks, refers to "crimes in which current or former employees, contractors, or business partners intentionally exceeded or misused an authorised level of access to networks, systems, or data to steal confidential or proprietary information from the organisation" (Moore et al., 2011, p. 1). Moore et al.'s work comes from the well-known CERT program at Carnegie Mellon University, whose aim is to gather data on and analyse malicious insider incidents. The CERT Insider

Threat Center collaborates with the U.S. Department of Homeland Security, and is primarily involved in using system dynamics modelling to characterise and study insider threats (see Cappelli, Moore, & Trzeciak, 2012, for a more detailed description of CERT). Although the group at Carnegie Mellon has published work on other examples of insider threat (e.g., IT sabotage and fraud; Moore et al., 2008; Rich et al., 2005), the 2011 paper is the first one that uses a primarily personological approach, emphasising within-person specific characteristics more than the attack characteristics.

CERT's research is partially funded by the U.S. Army Research Office. Thus, the group at CERT had access to, and analysed hundreds of cases of insider threat, which were gathered from various sources across different United States infrastructure sectors. Moore et al. (2011) conducted follow-up work on 48 cases of IP theft using detailed group modelling procedures. Through this work, Moore et al. (2011) developed dynamics systems models for two major profiles of attackers for IP theft, specifically, the 'entitled independent' and the 'ambitious leader'.

The entitled independent refers to an insider who acts alone in order to obtain proprietary information that is beneficial to his or her personal interests in a new job or for a side business. The entitled independent is mainly characterised by his/her feeling of entitlement to access the information, and it is this sense of entitlement that justifies his/her actions. Typically, these offenders steal information that they were at least partially responsible for developing or safeguarding, and this partial investment of energy, time, and resources contributes to a sense of ownership of the information, which in turn feeds the feeling of entitlement. An example of an entitled independent individual might be a software programmer who leaves a virtual 'back door' to programs that he/she created. These programs could be portions of a larger system of infrastructure that is proprietary to the organisation, and the 'back door' serves as a threat to cyber security because it enables the programmer to obtain privileged but unsanctioned and/or unregulated access.

On the other hand, the ambitious leader recruits other insiders in order to obtain proprietary information to serve some larger purpose, such as the interests of a competing organisation or a foreign government. There are at least two ways to interpret the underlying motives of the ambitious leader type of cyber-criminals – they could see their role as a facilitator for the machinations of a larger power such as the competitor company that they are aiding and aligning with, or the ambitious leaders could see the outside company as a tool for obtaining greater power for themselves. However, these distinctions are not discussed in Moore et al.'s (2011) typology. What matters in Moore et al.'s (2011) model is that the act of betrayal is in service of an external organisation that will give the ambitious leader access to greater power.

Personality Differences between Ambitious Leader-type versus Entitled Independent-type Insiders

There are two major differences between the ambitious leader model and the entitled independent model for IP theft. First, insider attacks by entitled independents are typically preceded by the attackers experiencing dissatisfaction with their organisations, whereas such dissatisfaction is absent in ambitious leaders. Second, the attacks by ambitious leaders are executed with a great amount of prior planning that typically involve the recruitment of other insiders as well as the use of deception in order to obscure the theft. In contrast, attacks by entitled independents typically involve little planning or deception.

Although Moore and colleagues (2011) take a typological approach by essentially constructing profiles of different types of offenders, what is most interesting about their categorisation of IP theft attacks is that it reveals some common dimensions with which different types of insider attackers can be distinguished.

The first dimension is the presence and degree of negative emotionality. In the entitled independent model, the insider experiences some sort of triggering event (e.g., loss of a promotion opportunity), which leads him or her to experience dissatisfaction with the organisation. It is this dissatisfaction that provides the motivation for the act of disloyalty in stealing proprietary information. However, in the ambitious leader model, the attacker's decision to commit IP theft is motivated by the insider's commitment to an entity (another organisation) or a cause (a political agenda) other than the insider's organisation. This sense of commitment is not typically accompanied by negative emotion. In fact, there is a very deliberate, carefully thought-out plan to execute the theft, which suggests a low level of emotionality. Thus, one might describe the distinction between entitled independents' and ambitious leaders' motives as the difference between 'hot' and 'cold' – on one hand, entitled independents' actions are accompanied by arousing negative emotions of dissatisfaction and disgruntlement, while ambitious leaders actions are calculated and dispassionate.

The second dimension is the level of organisation of the attack. The ambitious leader undertakes a complex, well-planned, and drawn-out process of recruiting and coordinating other insiders into his or her cause, whereas the entitled independent executes the IP theft typically within a short period of time after the precipitating event, and without much prior planning or coordination.

Since Moore et al. (2011) take a system dynamics perspective, their model assumes that each offender is predisposed to engage in IP theft, but only acts on this propensity once there is some kind of triggering event. In the case of the entitled independent, the catalyst is an event that leads him or her to feel undervalued by the organisation (e.g., being passed over for promotion) and to start to shift his or her loyalties to a new organisation. In the case of the ambitious leader, a proposal by a competing cause or organisation leads him or her to form a plan for the attack in service of the competing organisation. Regardless, both scenarios work on a principle commonly referred to in clinical psychology as the diathesis-stress model. In the diathesis-stress model, individuals have internal attributes (diathesis – e.g., hormone dysregulation) that act as risk factors for certain conditions. The predisposing internal attributes, which could be due to biological, societal, or cultural causes, put the individual at risk for developing the conditions (of illness or clinical symptoms – e.g., anxiety disorders) but only under certain resource-demanding environmental context (stress). In Moore et al.'s (2011) model, both types of insiders are assumed to have predisposing characteristics (diathesis) that lead them to be susceptible to triggering events (stress) such as the loss of a promotion or the proposal from a competing company, which in turn leads to the insider attack.

Furthermore, the principle of differential susceptibility (Belsky, 1997) states that individuals differ in the degree to which they are susceptible to the effects of stressful events. That is, there are varying degrees of risk (diathesis) in a population, such that for certain individuals with greater risk factors (e.g., low socioeconomic status combined with cultural norms for depression, combined with biological vulnerability), the likelihood of developing symptoms are higher than for those individuals with fewer risk factors.

Specifically, according to Moore et al. (2011), the entitled independent has a predisposition that leads him or her to become more easily entitled. However, Moore and colleagues do not go on to discuss what these predispositions might be.

Following the principles of diathesis-stress and differential susceptibility, one might argue that entitled independents possess key personality and person-specific factors that are different from those of ambitious leaders, and that these person-specific factors make entitled independents particularly susceptible to feeling entitled but dissatisfied at work, and to act on their dissatisfaction in ways that are harmful to their organisations. Accordingly, ambitious leaders should also be more likely to possess personality attributes that are different from those of entitled independents, and these attributes should make ambitious leader types more susceptible to counter-proposals from competing organisations, and more willing to engage in deceptive behaviour in service of those competing organisations.

For instance, as argued above, the entitled independent model of IP theft is distinguished from the ambitious leader model by the presence of negative emotionality. This suggests that individuals who are more likely to fall into the role of entitled independent are more reactive to negative emotions, or perhaps are more emotionally unstable. It could be argued that these individuals are less adept at the emotion-regulation aspect of coping with emotionally aversive events. Conversely, individuals who have relatively fewer negative emotions on average, or who have fewer fluctuations in their emotions on a daily basis, or have greater resources for coping with negative emotions would be more likely to be resilient to triggering incidents at work (e.g., being passed over for a promotion, a perception of a lack of respect or injustice in the organisation) that could threaten their loyalty to the organisation. Of course, there is an alternative explanation of events, in which the entitled independent is not necessarily more prone to negative emotionality, but where they have been repeatedly thwarted in their work efforts and general agency by systematic factors, such as an unequitable remuneration or promotion system, exploitative or unappreciative bosses, or corporate indifference. In these cases, however, there would still be mean level differences in negative emotionality between loyal employees and disgruntled ones, albeit differences caused by the immediate work context. Regardless of whether there is a dispositional style towards negative emotionality or there are higher-than normal context-dependent levels of negative emotionality, it seems likely that entitled independents would exhibit higher mean levels than their colleagues.

On the other hand, the ambitious leader model is distinguished by the presence of a high level of organisation. Accordingly, insiders who are emotionally stable, possess sufficient organisational and coordination skills, have a certain degree of influence in the organisation in order to recruit other insiders, and who enjoy the process of planning covert and complicated operations, would be more likely to fall under the ambitious leader model than their more neurotic, less skilled, less organised, and less socially-influential counterparts.

Literature in a wide range of related fields such as that of organisational citizenship behaviours, counterproductive work behaviours, personality psychology, forensic psychology, and business ethics is replete with evidence for profiles of criminal behaviour. These lines of research, while not being directly related to cyber security and/or insider threat might help researchers interested in insider attacks that take place in cyber arenas, particularly when the work includes related insider activities such as fraud and industrial sabotage. For instance, Murphy and Dacin (2011) illustrate the value of constructing overarching dimensions to organise the decision-making processes of perpetrators of fraud. In their framework, individuals first have to become aware that certain behaviours constitute as fraud. Next, the insider needs to make a judgment about whether the fraudulent act is an acceptable behaviour, according to the norms of the organisation. Next, the insider needs to evaluate the relative costs and risks versus the benefits of the fraudulent action. Finally, the insider needs to decide how to deal with the negative emotions (e.g., guilt, shame) that accompany the fraud. If the fraudsters are able to rationalise their actions in a way that minimises personal responsibility for any negative consequences or in a way that diminishes their moral culpability, then they are likely to continue engaging in the fraudulent behaviour.

Murphy and Dacin's (2011) paper reveals some common personality and person-specific dimensions that help to differentiate between different perpetrators of insider attacks. These dimensions are:

- **Awareness**: First, individuals who engage in insider attacks typically possess some minimum degree of social acumen, such that they have awareness of the social norms regarding ethical behaviour within their organisation, as well as the boundaries of acceptable work behaviour. This necessitates a certain level of social, emotional, and analytical intelligence. Furthermore, every organisation's normative culture is idiosyncratic and developed from a combination of the micro-level group dynamics and daily work culture, the larger institutional demands and goals, and macro-level moral, ethical, and social codes within the proximal geographical context. These ethical norms for acceptable work behaviour would be generally endorsed by insiders at all levels of the organisation, implicitly known to all the members of the organisation, and finally, transmitted quickly to any new uninitiated members of the organisation – even though they would not be communicated or immediately obvious to outsiders. As a result, researchers seeking to understand norms for ethical behaviour in an organisation would need to survey a large number of insiders of the organisation from different levels of the organisation structure in order to determine the level of awareness a true insider would need to possess.
- **Value System**: Second, individuals who engage in insider attacks tend to possess a value system that allows them to overlook the goals of their organisation in order to serve their own needs and/or the needs of a competing organisation. Two scenarios could occur. Either the insiders possess a set of values that causes them to place their personal interests above the interests of others (e.g., the value of ambition), or the insiders possess a set of values which conflicts with the normative value system of the organisation (i.e., culturally sanctioned values). Specifically, in the first scenario, employees of an organisation who value personal ambition over communal growth would be more willing to engage in insider activities that damage the interests of their organisation. In the second scenario, employees who possess work goals which conflict with the goals of their work-group would feel alienated from their colleagues, and this alienation could lessen the insiders' allegiance to their group and to their organisation.
- **Negative Emotionality**: Third, as mentioned earlier, insiders who engage in insider attacks are likely to be more susceptible to negative emotions. In personality psychology, generally the disposition to be more reactive to negative emotions such as anxiety, shame, and depression, can either be described by the personality trait of neuroticism (e.g., as assessed by the NEO-FFI; McCrae & Costa, 2004), or by the temperament of negative emotionality. Negative emotionality is assumed to be a stable emotional style that is present at a very young age, even before early socialisation and before the development of language. Hence, personality assessments for negative emotionality and related constructs (e.g., irritability – Stringaris et al., 2012; rumination – Nolen-Hoeksema, 1998; NEO-PI assessed neuroticism – Reise, Smith, & Furr, 2001) could easily be adapted for use in cyber security research.
- **Rationalisation/Moral Disengagement**: Finally, individuals who initiate an insider attack are likely to possess a personality characteristic that allows them to rationalise their actions in a way that absolves them of personal responsibility for any wrongdoing. A candidate personality variable that describes such a process is the dispositional propensity for moral disengagement. Specifically,

people differ in the degree to which they disengage from morally dubious outcomes. Insiders who engage in insider attacks could be high in moral disengagement, which lessens their moral culpability for their actions, and this in turn makes it easier for them to continue their attacks. Moore et al. (2012) have developed an 8-item measure of the propensity for moral disengagement that has been used to predict unethical organisational behaviour. Accordingly, this and other conceptually equivalent measures of moral disengagement could be included in screening and personnel assessments. Of relevance are personality profiles of individuals who are more likely to engage in moral disengagement. For instance, individuals who score highly on measures for the 'dark triad' characteristics of psychopathy, Machiavellianism, and narcissism have been found to be more likely to morally disengage and to endorse unethical consumer attitudes (Egan, Hughes, & Palmer, 2015). Certainly, more research is needed on how individual differences in the propensity to morally disengage affect social interactions. Of particular interest would be whether ethical decision-making processes are predicted by the greater tendency to morally disengage, and whether the mode of interaction – face-to-face versus computer-mediated – would moderate these relationships.

RELATING CYBER-BASED INSIDER THREAT AND THREATS FROM RADICALISATION

Broadly speaking, radicalisation refers to the process of individuals becoming increasingly committed to attitudes and behaviours that are judged by larger society as non-normative (Bhui, Warfa, & Jones, 2014; cf. Kruglanski et al., 2014). As Silke (2008) has argued, while the recent burgeoning interest in radicalisation can be attributed to its link to terrorism, not all individuals who become radicalised will eventually engage in terrorist acts. As such, radicalised attitudes and behaviours can include – besides terrorism – extreme criminal activity, participation in religious cults, self-harming behaviour, suicidal ideation, and substance and behavioural addiction, amongst others. When conceptualised in this manner, it is clear that some perpetrators of cyber-based insider criminal activity could be radicalised individuals who see cyberspace as a suitable avenue for accomplishing their focal goals.

As such, as long as there is an accompanying process of personal and/or political transformation into an identity that deviates from the norm and which leads to commitment to intergroup conflict in order to protect the beliefs of the group to which these non-normative ideals are ascribed (cf. Christmann, 2012), the insider threat issue can be viewed using the same lens as the issue of the threat of radicalisation. Using Moore et al.'s (2011) terminology, radicalised insiders would qualify as ambitious leader-types who perpetrate the insider attack in support of some larger organisation. In this case, the 'organisation' refers to the group to which these non-normative ideologies or identities are attributed.

A key finding in radicalisation research is that certain person-specific demographic factors seem to emerge robustly as correlates of radical behaviour – although there is considerable inter-individual variation, broadly speaking, these individuals tend to be male, young (under 25 years old), and highly educated (or at least have some degree of intellectual aptitude in order to contemplate doctrine and ideology) (cf. Young, Rooze, & Holsappel, 2015). The significance of the under-25 age factor is likely due to the possibility that individuals in this age group are actively developing their personal identities, thus this is a sensitive period of life where youth might be more susceptible to the extreme political, social, or theological ideologies that underpin radicalised criminal or terrorist activity. Additionally, the emotional skill set of young males in this age group are also likely to still be developing, which contributes to their vulnerability to the persuasive potential of extremist messages that are often couched in emotionally evocative language.

Besides documenting some of these important person-specific, socioeconomic variables, recent research has also produced some psychologically grounded models of the process of developing radicalised identities (e.g., Doosje & de Wolf, 2010; Moghadam, 2005) that might also present some points of relevance for the present discussion. For instance, in Doosje and de Wolf's (2010) model, the radicalisation process is structured around six levels of increasing radicalisation, in which the earlier levels (0, 1, 2) contain socio-psychological processes tied to how an individual process his/her environment, and the middle and higher levels (3, 4, 5, 6) involve increasing degrees of influence of the group and social context, and the associated ideologies, actors, and mores of the group. In this model, some factors that exist at the lowest levels are directly relevant to personality. For instance, on the ground floor of Doosje and de Wolf's (2010) model, the prominent psychological factors governing entry into a radicalisation process are the individuals' frustration at being deprived or discriminated by society, their feelings of personal uncertainty, either about their identities or their social status, and finally their degree of openness towards the influence of close others.

There are established personality measures for assessing individual differences in the levels of frustration (e.g., Harrington, 2005), in subscription to prevailing social norms and values and degree of identification with the prevailing cultural identity (e.g., Hu, Wang, & Li, 2014; Wan & Chew, 2013), and non-hypnotic or imaginative suggestibility (e.g., Braffman & Kirsch, 2001) which could be useful to researchers interested in assessing individual differences in susceptibility to radicalisation. Furthermore, it is likely that these feelings of deprivation and discrimination, feelings of uncertainty, and an unstable identity accompanied by the intellectual openness would lead insiders to become vulnerable to feelings of entitlement and/or a loss of identification with the organisation to which they belong, and hence be vulnerable to the orchestrations of malicious outsiders who might exploit these insiders' access.

There is a fragmented but highly relevant set of literature on personality, anti-sociality, extremism, and radicalisation that researchers interested in building psychological and personality based models of cyber-based insider threat can refer to. Case studies are particularly useful in this regard (e.g., Mastors & Siers, 2014), as are a wide variety of papers that examine different individual motives for extremism and/or terrorism. For instance, promising examples of constructs examined in these literatures include moral disengagement (cf. Bandura, 2004), frustration and anger (cf. Davie, 1973), honour-based notions of aggression (Nisbett & Cohen, 1996), personal injustice (Moghaddam, 2007), personal uncertainty (Doosje, Loseman, & van de Bos, 2013), need for closure (Kruglanski, Pierro, Mannetti, & de Grada, 2006), self-deception (von Hippel & Trivers, 2011), terror management theory (Pyszczynski, Rothschild, & Abdollahi, 2008), psychopathy and associated traits such as callous-unemotional traits (Kimonis et al., 2008), and anti-social tendencies such as the so-called dark triad (Paulhus, 2014).

To illustrate the relevance of these literatures, let us turn to Kruglanski et al. (2014) who argued that the underlying personal motivation for radicalised individuals is an underlying need for personal significance. This search for personal significance is reminiscent of classic constructs in personality psychology that speak to an intrinsic and universal need for building a sense of self-worth; for example, Maslow's (1943) needs for self-esteem and self-actualisation, Frankl's (2000) *Being* need, and Deci and Ryan's (2000) basic need for competence. In relation to cyber-based insider crime, this quest for personal significance could also drive some individuals belonging to Moore et al.'s (2011) ambitious leader type. Specifically, when the work environment does not contain the necessary means for individuals to feel effective in their environment or to achieve personal meaning, these individuals might become more susceptible to external influences and ideologies that provide a larger significance to their lives, and hence embark on a process of radicalisation.

Finally, as mentioned earlier, case studies of radicalised individuals are particularly useful for theory generation, especially in establishing early detection models, provided that there is enough information about the personal histories of these individuals. These cases studies provide the benefit of determining – albeit retrospectively – trajectories, and examining the dynamic interaction of various personality and person-specific factors in an integrative manner.

Some examples of high profile cases that involved cyber-based insider activity include Edward Snowden, Bradley/Chelsea Manning, and Robert Hanssen. Although none of these individuals mentioned involved violent acts of terrorism and hence are not extreme radicals, I would argue that they could be described as radicalised, given that they all committed their acts of data theft and espionage in the service of an external organisation (the Soviet Union for Hanssen) or identity (transgender identity for Manning; larger American society for Snowden), and possessed varying degrees of feelings of perceived injustice or discrimination (in the case of Snowden, the perceptions of the United States intelligence community's failure to preserve global privacy, and in Manning's case, perceptions of discrimination based on sexual orientation), or deprivation (monetary in Hanssen's case) in their interaction with the institutions (the CIA and NSA for Snowden, the FBI for Hanssen, and the U.S. Army for Manning) to which they belonged, and subsequently betrayed.

For instance, Bradley/Chelsea Manning was a U.S. Army intelligence officer who provided classified military information to the whistle-blower website, WikiLeaks. Written accounts of Manning's case revealed that she was unhappy with having to hide her homosexuality and her transgendered identity given the 'Don't Ask Don't Tell' policy of the U.S. Army, and its hyper-masculine social landscape. Additionally, she perceived some discrimination and injustices in her work life that drove her to become increasingly isolated from other soldiers in her unit. As such, it might be helpful for researchers to study these cases for commonalities in personality and other person-specific characteristics.

GUIDELINES FOR INVESTIGATING CYBER-BASED INSIDER THREAT FROM A PERSONALITY PERSPECTIVE

As personality psychologists interested in cyber-based insider threat, we are in the midst of a field of research that must keep up with a moving target composed of an expanding and rapidly changing group of qualified insiders who are increasingly familiar with information technology, with cyberspace, and the ways to exploit it. Additionally, low bases rates for cyber-based insider activity pose a major challenge to developing models for personality precursors of insider threat behaviour before rather than after an attack. Finally, environments in which cyber-based insider activity occurs are often restricted-access, high-stakes, and low-transparency environments, such as the higher levels in the hierarchy of a multinational corporation or in national security contexts. As a result, it is often difficult to obtain access to insiders, and even after access is granted, there is a strong likelihood that self-presentational concerns would jeopardise the veridicality of self-report measures of personality. In some cases, peer ratings, direct observations, and other non-self-report measures may require more invasive access into the subject's life than he or she is willing or able to accommodate. Clearly, there are a myriad of difficulties when undertaking research with a personality or person-based perspective on cyber-based insider threat.

In the following section, I discuss three major guidelines for personality based research that might help researchers interested in insider threat and cyber security to improve the psychological realism, and the reliability and validity of their models.

Incorporating the Person-Situation Interaction into Analyses

In order to understand processes related to cyber-based insider attacks from a personality and person-specific perspective, researchers need to develop a more contextualised research approach to understanding the influence of personality variables on behavioural and social outcomes. Specifically, because insider attacks happen usually as a result of a triggering event, the immediate context has a large influence on the initiation as well as maintenance of behaviour that would lead to insider attacks and threats to cyber security. Research that assesses personality variables or demographic factors related to questions of cyber security tends to underemphasise the interaction between the person and the situation as a source of the threat. Specifically, research on offender profiling (e.g., Kapardis & Krambia-Kapardis, 2004; Knapp, Smith, & Sprinkle, 2014) tends to generate types of offenders based on a combination of personality (e.g., traits, motives, cognitive indicators) and person-specific characteristics (e.g., gender, work role, duration with organisation), and uses these combinations of personality dimensions directly as single predictors of insider attacks.

However, as argued above, the integration of the context into understanding the effect of personality on insider attacks is particularly important in cyber-based attacks, since cyber-environments evolve more rapidly than physical environments. The key is to be mindful of the context when applying personality and dispositional measures in predictive models. Given the dynamic interplay between person-factors and the environment, it is unlikely that researchers would be able to comprehensively measure all the relevant dispositional and demographic variables; nonetheless, researchers should still apply prudence and sensitivity when adapting personality based explanations and personality precursors from the research to the immediate context.

Developing Culturally Informed Explanations

Related to the above point, there is a need for more specialised explanations of cyber-based insider threats, particularly explanations that take the local cultural norms, conventions, and values into account. Due to the low base rates for insider attacks and the difficulty of gaining access to insider information within many corporate organisations, extant research has relied heavily on national defence-related sectors for funding and for sources of data on insider attacks (e.g., CERT, CPNI). However, this creates explanations and models that are heavily rooted in the cultural and social mores for acceptable work-related behaviour and for personal ethics. Frequently, as can be seen from Moore et al.'s (2011) work, the insiders create a sense of self-entitlement in order to justify their actions, suggesting that they are at least appreciative of the possible ethical transgressions of their actions. Thus, before using personality to predict behaviour, researchers should take care to establish the meaning of the behaviour, as ascribed to it by significant others within the immediate social context. Researchers should lay the groundwork for every research program by first assessing the norms for acceptable work behaviour, the consensus view of clear transgressions within the organisation, as well as the core ethical principles within the organisation and for the larger cultural milieu.

Moving Away from Correlation-based Research that uses only Reactive Measures of Personality

As discussed above, most research on insider threat and cyber security uses questionnaire measures of personality variables, which are highly susceptible to response biases, self-monitoring and self-presentational concerns, amongst other problems. There are already many well-established measures of personality that are non-self-report – e.g., for motives and for emotions. Researchers would do well to utilise these and other similar instruments. This is not to say that researchers should do away with self-report or questionnaire measures altogether, but to caution against solely relying on self-report data, especially in a sensitive area of study that generates wariness in participants. In general, an approach that uses multiple sources of data (e.g., self, observers, subordinates, superiors, peers), multiple methods of inquiry (e.g., experimental, modelling, content analysis of freely generated text documents, correlational analyses of survey data, behavioural coding) and that relies on interdisciplinary (e.g., mathematical, computer science, information science, psychology, sociology) collaborations should be encouraged.

For instance, the popular corporate practice of having 360-degree assessments of performance appraisal has addressed some of the concerns of self-report, questionnaire, and retrospective assessment. Briefly, the 360-degree assessment method relies on using competence-based survey instruments to solicit confidential evaluations from the full range of working relationships a worker encounters. At minimum, these relationships include those with subordinates, peers, and supervisors. Each targeted individual in turn receives a numerical as well as a descriptive assessment of his/her capability to effectively demonstrate specific competences based on the perceptions of those people with whom he/she closely works with. By relying on the testimonies of the network of close associates, and by triangulating measurement across different sources and perspectives of the work-group (each source involved in different physical or knowledge-based aspects of the production process), the 360-degree approach is able to decrease data distortions due to reporting biases and thus improve the validity and reliability of performance measurement (see Toegel & Conger, 2003, for a more comprehensive discussion of the pros and cons of adopting this assessment method). In the same spirit, there are many merits to incorporate a multi-source approach to personality and psychometric assessment, while still preserving the convenience and ease of administration of questionnaire-based measures.

Specific to the cyber-arena, researchers could also adopt methodologies that have been used by personality and social psychologists interested in social media platforms such as Facebook, Twitter, Instagram, etc. The area of work that is particularly relevant to non-reactive assessments of personality is based on the principle of assessing behavioural residues in naturally occurring verbal content on online social networking sites (see Gosling, Augustine, Vazire, Holtzman, & Gaddis, 2011, for a representative study on assessing personality traits from Facebook activity). Briefly, researchers assume that personality characteristics manifest themselves in behaviours that individuals engage in when participating on these social networking sites. In other words, there is a residue of the traits that is left behind in the observable remnants of online behaviours. Facebook posts, for instance, are a log of online activity and can be collected and analysed for varying degrees of trait-relevant content. This work on coding freely generated content for personality characteristics is not new – there is a long tradition of at-a-distance personality measurement (cf. Winter, 2005) of individuals who are not easily accessible (e.g., because they are historical figures or because they are socially prominent individuals for which access is difficult to obtain). For instance, researchers have conducted personality assessments of U.S. presidents – e.g., Winter's (2011) assessment of Barack Obama's personality.

Finally, validation of any theories and models should take place ideally by the collection of new data from realistic environments within a different organisation which belongs nonetheless to the same cultural context, rather than by way of simulations or re-analyses of data from the same organisation. This practice will improve the validity of models, as well as provide greater generalisability for the theories.

REFERENCES

Axelrad, E. T., Sticha, T. J., Brdiczka, O., & Shen, J. (2013). A Bayesian network model for predicting insider threats. In *IEEE Symposium on Security and Privacy Workshops*. San Francisco, CA: IEEE. doi:10.1109/SPW.2013.35

Bagby, R. M., Buis, T., & Nicholson, R. A. (1995). Relative effectiveness of the standard validity scales in detecting fake-bad and fake-good responding: Replication and extension. *Psychological Assessment*, *7*(1), 84–92. doi:10.1037/1040-3590.7.1.84

Bandura, A. (2004). The role of selective moral disengagement in terrorism and counterterrorism. In F. M. Moghaddam & A. J. Marsella (Eds.), *Understanding terrorism: Psychosocial roots, causes and consequences* (pp. 121–150). Washington, DC: American Psychological Association. doi:10.1037/10621-006

Belsky, J. (1997). Theory testing, effect-size evaluation, and differential susceptibility to rearing influence: The case of mothering and attachment. *Child Development*, *68*(4), 598–600. doi:10.2307/1132110

Bhui, K., Warfa, N., & Jones, E. (2014). Is violent radicalisation associated with poverty, migration, poor self-reported health and common mental disorders? *PLoS ONE*, *9*(3), 1–10. doi:10.1371/journal.pone.0090718

Braffman, W., & Kirsch, I. (2001). Reaction time as a predictor of imaginative suggestibility and hypnotizability. *Contemporary Hypnosis*, *18*(3), 107–119. doi:10.1002/ch.224

Cappelli, D., Moore, A., & Trzeciak, R. (2012). *The CERT guide to insider threats: How to Prevent, Detect, and Respond to Information Technology Crimes*. Boston, MA: Pearson Education, Inc.

Cervone, D., Shoda, Y., & Downey, G. (2007). Construing persons in context: On building a science of the individual. In Y. Shoda, D. Cervone, G. Downey, Y. Shoda, D. Cervone, & G. Downey (Eds.), *Persons in context: Building a science of the individual* (pp. 3–15). New York, NY: Guilford Press.

Chang, M., & Lim, Y. (2014). Late disclosure of insider trades: Who does it and why? *Journal of Business Ethics*, 1–13.

Christmann, K. (2012). *Preventing religious radicalisation and violent extremism: A systematic review of the research evidence*. London: Youth Justice Board.

Cooper, M. L., Barber, L. L., Zhaoyang, R., & Talley, A. E. (2011). Motivational pursuits in the context of human sexual relationships. *Journal of Personality*, *79*(6), 1031–1066. doi:10.1111/j.1467-6494.2010.00713.x

Costa, P. T. Jr, & McCrae, R. R. (1994). Stability and change in personality from adolescene through adulthood. In C. F. Halverson, G. A. Kohnstamm, & R. P. Martin (Eds.), *The developing structure of temperament and personality from infancy to adulthood* (pp. 139–150). Hillsdale, NJ: Erlbaum.

Davie, J. C. (1973). Aggression, violence, revolution and war. In J. N. Knutsen (Ed.), *Handbook of political psychology* (pp. 234–260). San Francisco, CA: Jossey-Bass.

Deci, E. L., & Ryan, R. M. (2000). The 'what' and 'why' of goal pursuits: Human needs and the self-determination of behaviour. *Psychological Inquiry*, *11*(4), 227–268. doi:10.1207/S15327965PLI1104_01

Doosje, B., & de Wolf, A. (2010). *Dealing with radicalism: A psychological analysis*. Amsterdam: SWP.

Doosje, B., Loseman, A., & van de Bos, K. (2013). Determinants of radicalization of Islamic youth in the Netherlands: Personal uncertainty, perceived injustice, and perceived group threat. *The Journal of Social Issues*, *69*(3), 586–604. doi:10.1111/josi.12030

Duggan, C. (2004). Does personality change and, if so, what changes? *Criminal Behaviour and Mental Health*, *14*(1), 5–16. doi:10.1002/cbm.556

Egan, V., Hughes, N., & Palmer, E. J. (2015). Moral disengagement, the dark triad, and unethical consumer attitudes. *Personality and Individual Differences*, *76*, 123–128. doi:10.1016/j.paid.2014.11.054

Fiedler, K., Messner, C., & Bluemke, M. (2006). Unresolved problems with the "I," the "A" and the "T": Logical and psychometric critique of the Implicit Association Test (IAT). *European Review of Social Psychology*, *17*(1), 74–147. doi:10.1080/10463280600681248

Frankl, V. (2000). *Recollections: An autobiography*. New York, NY: Perseus Books.

Gosling, S., Augustine, A. A., Vazire, S., Holtzman, N., & Gaddis, S. (2011). Manifestations of personality in online social networks: Self-reported Facebook-related behaviors and observable profile information. *Cyberpsychology, Behavior, and Social Networking*, *14*(9), 483–488. doi:10.1089/cyber.2010.0087

Graber, E. C., Laurenceau, J., & Carver, C. S. (2011). Integrating the dynamics of personality and close relationship processes: Methodological and data analytic implications. *Journal of Personality*, *79*(6), 1101–1137. doi:10.1111/j.1467-6494.2011.00725.x

Harrington, N. (2005). The frustration discomfort scale: Development and psychometric properties. *Clinical Psychology & Psychotherapy*, *12*(5), 374–387. doi:10.1002/cpp.465

Hu, F., Wang, P., & Li, L. (2014). Psychometric structure of the Chinese Multiethnic Adolescent Cultural Identity Questionnaire. *Psychological Assessment*, *26*(4), 1356–1368. doi:10.1037/a0037690

Hull, C. L. (1943). *Principles of behavior*. Oxford, England: Appleton-Century.

James, W. (1890). *The principles of psychology* (Vol. I). New York, NY, US: Henry Holt and Co. doi:10.1037/11059-000

John, O. P., & Srivastava, S. (1999). The Big Five trait taxonomy: History, measurement and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and Research* (pp. 102–138). New York, NY: The Guildford Press.

Kapardis, A., & Krambia-Kapardis, M. (2004). Enhancing fraud prevention and detection by profiling fraud offenders. *Criminal Behaviour and Mental Health*, *14*(3), 189–201. doi:10.1002/cbm.586

Kimonis, E. R., Frick, P. J., Skeem, J. L., Marsee, M. A., Cruise, K., Munoz, L. C., & Morris, A. S. et al. (2008). Assessing callous-unemotional traits in adolescent offenders: Validation of the inventory of callous-unemotional traits. *International Journal of Law and Psychiatry*, *31*(3), 241–252. doi:10.1016/j.ijlp.2008.04.002

Knapp, J. R., Smith, B. R., & Sprinkle, T. A. (2014). Clarifying the relational ties of organizational belonging: Understanding the roles of perceived insider status, psychological ownership, and organizational identification. *Journal of Leadership & Organizational Studies*, *21*(3), 273–285. doi:10.1177/1548051814529826

Kruglanski, A. W., Gelfand, M. J., Bélanger, J. J., Sheveland, A., Hetiarachchi, M., & Gunaratna, R. (2014). The psychology of radicalization and deradicalisation: How significance quest impacts violent extremism. *Political Psychology*, *35*(S1), 69–93. doi:10.1111/pops.12163

Kruglanski, A. W., Pierro, A., Mannetti, L., & de Grada, E. (2006). Groups as epistemic providers: Need for closure and the unfolding of group-centrism. *Psychological Review*, *113*(1), 84–100. doi:10.1037/0033-295X.113.1.84

Lilienfeld, S. O., Wood, J. M., & Garb, H. N. (2000). The scientific status of projective techniques. *Psychological Science in the Public Interest*, *1*, 27–66.

Lucas, R. E., & Donnellan, M. B. (2011). Personality development across the life span: Longitudinal analyses with a national sample from Germany. *Journal of Personality and Social Psychology*, *101*(4), 847–861. doi:10.1037/a0024298

Marcus, B., Lee, K., & Ashton, M. C. (2007). Personality dimensions explaining relationships between integrity tests and counterproductive behavior: Big five, or one in addition? *Personnel Psychology*, *60*(1), 1–34. doi:10.1111/j.1744-6570.2007.00063.x

Marcus, B., & Schuler, H. (2004). Antecedents of counterproductive behavior at work: A general perspective. *The Journal of Applied Psychology*, *89*(4), 647–660. doi:10.1037/0021-9010.89.4.647

Maslow, A. (1943). A theory of motivation. *Psychological Review*, *50*(4), 370–396. doi:10.1037/h0054346

Mastors, E., & Siers, R. (2014). Omar al-Hammami: A case study in radicalization. *Behavioral Sciences & the Law*, *32*(3), 377–388. doi:10.1002/bsl.2108

Mauss, I. B., Evers, C., Wilhelm, F. H., & Gross, J. J. (2006). How to bite your tongue without blowing your top: Implicit evaluation of emotion regulation predicts affective responding to anger provocation. *Personality and Social Psychology Bulletin*, *32*(5), 589–602. doi:10.1177/0146167205283841

McClelland, D. C. (1987). *Human motivation*. New York, NY: Cambridge University Press.

McClelland, D. C., Koestner, R., & Weinberger, J. (1989). How do self-attributed and implicit motives differ? *Psychological Review*, *96*(4), 690–702. doi:10.1037/0033-295X.96.4.690

McCrae, R. R., & Costa, P. J. Jr. (2004). A contemplated revision of the NEO Five-Factor Inventory. *Personality and Individual Differences*, *36*(3), 587–596. doi:10.1016/S0191-8869(03)00118-1

Miller, C. S., Kimonis, E. R., Otto, R. K., Kline, S. M., & Wasserman, A. L. (2012). Reliability of risk assessment measures used in sexually violent predator proceedings. *Psychological Assessment*, *24*(4), 944–953. doi:10.1037/a0028411

Mischel, W., & Shoda, Y. (1995). A cognitive-affective system theory of personality: Reconceptualizing situations, dispositions, dynamics, and invariance in personality structure. *Psychological Review*, *102*(2), 246–268. doi:10.1037/0033-295X.102.2.246

Miyamoto, Y., & Ryff, C. D. (2011). Cultural differences in the dialectical and non-dialectical emotional styles and their implications for health. *Cognition and Emotion*, *25*(1), 22–39. doi:10.1080/02699931003612114

Moghaddam, F. M. (2005). The staircase to terrorism: A psychological exploration. *The American Psychologist*, *60*(2), 161–169. doi:10.1037/0003-066X.60.2.161

Moghaddam, F. M. (2007). The staircase to terrorism: A psychological exploration. In B. Bongar, L. M. Brown, L. E., Beutler, J. N. Breckenridge, & P. G. Zimbardo (Eds.), Psychology of terrorism (pp. 69-80). New York, NY: Oxford University Press.

Moore, A. P., Cappelli, D. M., Caron, T. C., Shaw, E. D., Spooner, D., & Trzeciak, R. F. (2011). *A preliminary model of insider theft of intellectual property (Technical report: CMU/SEI-2011-TN-013)*. Pittsburgh, PA: Software Engineering Institute.

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). *The "Big Picture" of insider IT sabotage across U.S. critical infrastructures (Technical report: CMU/SEI-2008-TR-009)*. Pittsburgh, PA: Software Engineering Institute.

Moore, C., Detert, J. R., Treviño, L. K., Baker, V. L., & Mayer, D. M. (2012). Why employees do bad things: Moral disengagement and unethical organizational behavior. *Personnel Psychology*, *65*(1), 1–48. doi:10.1111/j.1744-6570.2011.01237.x

Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: Understanding and preventing fraud in organization. *Journal of Business Ethics*, *101*(4), 601–618. doi:10.1007/s10551-011-0741-0

Nisbett, R. E., & Cohen, D. (1996). *Culture of honor: The psychology of violence in the South*. Boulder, CO: Westview Press.

Nolen-Hoeksema, S. (1998). The other end of the continuum: The costs of rumination. *Psychological Inquiry*, *9*(3), 216–219. doi:10.1207/s15327965pli0903_5

Nurse, J. R. C., Buckley, O., Legg, P. H., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding insider threat: A framework for characterizing attacks. In *IEEE Computer Society Security and Privacy Workshops*. San Francisco, CA: IEEE. doi:10.1109/SPW.2014.38

Paulhus, D. L. (2014). Toward a taxonomy of dark personalities. *Current Directions in Psychological Science*, *23*(6), 421–426. doi:10.1177/0963721414547737

Probst, C. W., Hunker, J., Bishop, M., & Gollmann, D. (Eds.). (2010). *Insider threats in cyber security*. New York, NY: Springer. doi:10.1007/978-1-4419-7133-3

Pyszczynski, T., Rothschild, Z., & Abdollahi, A. (2008). Terrorism, violence, and hope for peace: A terror management perspective. *Current Directions in Psychological Science*, *17*(5), 318–322. doi:10.1111/j.1467-8721.2008.00598.x

Quirin, M., & Bode, R. C. (2014). An alternative to self-reports of trait and state affect: The Implicit Positive and Negative Affect Test (IPANAT). *European Journal of Psychological Assessment*, *30*(3), 231–237. doi:10.1027/1015-5759/a000190

Reise, S. P., Smith, L., & Furr, R. M. (2001). Invariance on the NEO PI-R neuroticism scale. *Multivariate Behavioral Research*, *36*(1), 83–110. doi:10.1207/S15327906MBR3601_04

Rich, E., Martinez-Moyano, I. J., Conrad, S., Cappelli, D. M., Moore, A. P., Shimeall, T. J., & Wilk, J. et al. (2005). Simulating insider cyber-threat risks: A model-based case and a case-based model. In *Proceedings of the 16th International Conference of the System Dynamics Society*. Quebec City, Canada: System Dynamics Society.

Sackett, P. R., Berry, C. M., Wiemann, S. A., & Laczo, R. M. (2006). Citizenship and counterproductive behavior: Clarifying relations between the two domains. *Human Performance*, *19*(4), 441–464. doi:10.1207/s15327043hup1904_7

Salgado, J. (2002). The Big Five personality dimensions and counterproductive behaviors. *International Journal of Selection and Assessment*, *10*(1-2), 117–125. doi:10.1111/1468-2389.00198

Scherer, K. T., Baysinger, M., Zolynsky, D., & LeBreton, J. M. (2013). Predicting counterproductive work behaviors with sub-clinical psychopathy: Beyond the Five Factor Model of personality. *Personality and Individual Differences*, *55*(3), 300–305. doi:10.1016/j.paid.2013.03.007

Schultheiss, O. C., & Pang, J. S. (2007). Measuring implicit motives. In R. W. Robins, R. C. Fraley, & R. Krueger (Eds.), *Handbook of research methods in personality psychology* (pp. 322–344). New York, NY: Guilford.

Silke, A. (2008). Holy warriors: Exploring the psychological processes of jihadi radicalisation. *European Journal of Criminology*, *5*(1), 99–123. doi:10.1177/1477370807084226

Stringaris, A., Goodman, R., Ferdinando, S., Razdan, V., Muhrer, E., Leibenluft, E., & Brotman, M. A. (2012). The Affective Reactivity Index: A concise irritability scale for clinical and research settings. *Journal of Child Psychology and Psychiatry, and Allied Disciplines*, *53*(11), 1109–1117. doi:10.1111/j.1469-7610.2012.02561.x

Toegel, G., & Conger, J. (2003). 360-degree feedback: Time for reinvention. *Academy of Management Learning & Education*, *2*(3), 297–311. doi:10.5465/AMLE.2003.10932156

von Hippel, W., & Trivers, R. (2011). The evolution and psychology of self-deception. *Behavioral and Brain Sciences*, *34*(1), 1–16. doi:10.1017/S0140525X10001354

Wan, C., & Chew, P. Y. (2013). Cultural knowledge, category label, and social connections: Components of cultural identity in the global, multicultural context. *Asian Journal of Social Psychology*, *16*(4), 247–259. doi:10.1111/ajsp.12029

Winter, D. G. (1987). Leader appeal, leader performance, and the motive profiles of leaders and followers: A study of American presidents and elections. *Journal of Personality and Social Psychology*, *52*(1), 196–202. doi:10.1037/0022-3514.52.1.196

Winter, D. G. (2004). Motivation and the escalation of conflict: Case studies of individual leaders. *Peace and Conflict*, *10*(4), 381–398. doi:10.1207/s15327949pac1004_8

Wood, W., & Neal, D. T. (2007). A new look at habits and the habit-goal interface. *Psychological Review*, *114*(4), 843–863. doi:10.1037/0033-295X.114.4.843

Young, H. F., Rooze, M., & Holsappel, J. (2015). Translating conceptualizations into practical suggestions: What the literature on radicalization can offer to practitioners. *Peace and Conflict*, *21*(2), 212–225. doi:10.1037/pac0000065

ENDNOTES

[1] The issue of personality stability, personality change, and personality coherence is a perennial topic for discussion, and one that has yet to be irrefutably resolved within the field. Whilst there is relatively high test-retest reliability and relatively high life-span stability for the Big Five personality traits (e.g., Lucas & Donnellan, 2011), contemporary personality psychologists understand that even these traits continue to develop and change over the lifespan and are also susceptible to short term changes due to demand characteristics and 'strong situation' context effects. The predominant view is that of dynamic interactionism, where individuals select, react to, and directly change the environments that they are in depending on their stable dispositional characteristics, and the resulting environments in turn affect the quantity and quality of the dispositional trait that the individuals are expressing.

[2] However, the sheer number of possible antecedents and habits makes this task tedious, laborious, and challenging. Research that takes the time to catalogue the habits relevant to cyber-based insider crime is surely something worthwhile exploring, but which is likely to be neglected by busy researchers, academics, and policy makers with competing demands and limited time and resources.

[3] Users of implicit measures of personality should be aware of some of the controversies of implicit measures. Since these are indirect measures of personality, they utilise less obvious measures of psychological constructs – such as reaction time or through content coding of imaginative material. Hence, there is healthy discussion amongst researchers about the psychometric properties of these measures (e.g., Fiedler, Messner, & Bluemke, 2006; Lilienfeld, Wood, & Garb, 2000).