Journal of Military and Strategic Studies

VOLUME 23, ISSUE 2

"To Betray, You Must First Belong:" Psychological Pathways to Insider Threat and Radicalisation

Damian J. Terrill[1]*, Markos Trichas[2], Dave Bowden[1,2]

1 BAE Systems Plc, 6 Carlton Gardens, London, England.

2 BAE Systems Plc, 6 Carlton Gardens, London, England.

1,2 UK Ministry of Defence.

* **Correspondence:** Damian J. Terrill
damian.terrill@baesystems.com

Introduction

This paper examines the psychological processes and critical pathways that influence vulnerability to Insider Threat (IT) and radicalisation. Consideration of the

ISSN : 1488-559X

structural similarities between these concepts will enable practitioners to identify areas of concern and mitigate the threats associated with malicious internal activity. Although a universal agreement is yet to be reached on the definitive structures or processes which underpin IT or radicalisation,[1] it appears that the individual(s) in either circumstance have experienced a conflicted interpersonal perspective which led them to betray a group, society, or ideological system with which they had shared connections.

Given the complexities associated with discussions of ideology, self-perspective, and interpersonal psychological phenomena, it is essential to establish the key terms from the outset. Despite the similarities between the terms *risk* and *vulnerability,* they must not be employed interchangeably. Commenting on the relationship between extremism, radicalisation and mental health, Al-Attar.[2]clarifies the risk-vulnerability position. Al-Attar[3] observes that whilst risk and vulnerability are both concerned with the analysis and mitigation of harm, the former attends to known or verifiable factors (such as those psychological principles associated with the commission of crime); whereas, the latter focuses upon potential circumstances affecting persons with little or indeed no criminal history.[4] Although vulnerability and risk are routinely assessed systematically and at the individual level, Nogueira et al.[5] propose vulnerability

[1] A.R. Marbut & P.D. Harms, "Fiends and fools: A narrative review and neo-socioanalytic perspective on personality and insider threats," *Journal of Business and Psychology,* DOI: https://doi.org/10.1007/s10869-023-09885-9; M.A. Jensen, A. Atwell & P.A. James (2020), "Radicalization to violence: A pathway approach to studying extremism," *Terrorism and Political Violence* 32, 5 (2020): pp. 1067-1090.

[2] Z. Al-Attar, "Extremism, Radicalisation & Mental Health: Handbook for Practitioners," Brussels European Commission/RAN, 2019, europa.eu.

[3] ibid.

[4] Al-Attar, *Extremism, Radicalisation & Mental Health,p. 5.*

[5] M. O'Rourke, G. Bailes, & J. Davies, "Risk Assessment and Management," British Psychological Society, 2006, https://explore.bps.org.uk/content/report-guideline/bpsrep.2006.rep44; M. Lloyd, & C. Dean "ERG 22+ Structured Professional Guidelines for Assessing Risk of Extremist Offending," Ministry of Justice, 2011; A. Silke, "Risk assessment of terrorist and extremist prisoners," in *Prisons, Terrorism and Extremism: Critical Issues in Management, Radicalisation and Reform,* ed. A. Silke (New York, NY: Routledge, 2014), pp. 108-121; S. Bryans, P. Barzanò, & P. Meissner, *Handbook on the Management of Violent*

assessments are concerned with belief structures that render an individual less able to manage life challenges. O'Rourke et al., Lloyd and Dean, Silke and Bryans et al.[6] describe effective criminogenic risk assessment as dependent upon the practitioner's application of professional judgment to a range of variables. Crighton[7] asserts that whilst risk assessment cannot definitively ascertain who will offend or at precisely what moment; the correct application of credible risk assessment should allow practitioners to (i) identify specific hazards and outcomes and (ii) quantify both the probability and severity of these outcomes.Borum et al.[8] insist both threat and risk assessments typically adopt a person-specific focus to interpret the likelihood of a certain outcome. Citing Fein et al, Meloy and O'Toole[9] emphasise the importance of structured professional judgment when formulating an opinion on the details of the threat posed. Unlike the more holistic foundation of risk assessment, Meloy and O'Toole[10] and Simons and

Extremist Prisoners and the Prevention of Radicalization to Violence in Prisons. (Vienna: United Nations, 2016), unodc.org/pdf/criminal_justice/Handbook_on_VEPs.pdf

[6] M. O'Rourke, G. Bailes, & J. Davies, "Risk Assessment and Management," British Psychological Society, 2006, https://explore.bps.org.uk/content/report-guideline/bpsrep.2006.rep44; M. Lloyd, & C. Dean "ERG 22+ Structured Professional Guidelines for Assessing Risk of Extremist Offending," Ministry of Justice, 2011; A. Silke, "Risk assessment of terrorist and extremist prisoners," in *Prisons, Terrorism and Extremism: Critical Issues in Management, Radicalisation and Reform,* ed. A. Silke (New York, NY: Routledge, 2014), pp. 108-121; S. Bryans, P. Barzanò, & P. Meissner, *Handbook on the Management of Violent Extremist Prisoners and the Prevention of Radicalization to Violence in Prisons*. (Vienna: United Nations, 2016), unodc.org/pdf/criminal_justice/Handbook_on_VEPs.pdf

[7] D.A. Crighton, "Risk assessment," in *Forensic Psychology* 2nd ed. eds. D.A. Crighton & G.J. Towl, (Oxon: Wiley & Son, 2015), pp. 97-111.

[8] R. Borum, R. Fein, B. Vossekuil, & J. Berglund, "Threat assessment: Defining an approach to assessing risk for targeted violence," *Behavioral Sciences and the Law* 17, 3 (1999): pp. 323-337.

[9] J.R. Meloy, & M.E. O'Toole, "The concept of leakage in threat assessment," *Behavioral Sciences and the Law* 29, 4 (2011): pp. 513-527.

[10] ibid.

Meloy[11] insist threat assessment concentrates upon the application of deliberately targeted, premeditated, instrumental violence. Echoing the limitations observed in risk assessment, Simons and Meloy[12] maintain the assessor is unable to conclusively determine if or when the individual will engage in the targeted act.

Numerous points raised in the context of forensic risk assessment are consistent with the narrative surrounding IT vulnerability. Where risk assessments can be tailored to address the likelihood of a specified outcome, vulnerability is a diverse concept often called upon to inform explicit risk factors[13]. In an IT context the interpretation of *threat* incorporates, but extends beyond, the commission of premeditated violence, encompassing myriad harmful behaviours and deleterious outcomes. The discussion herein seeks to highlight the consistencies in patterns of vulnerability between IT and radicalisation to help facilitate analytical inquiry. It is hoped that by attending to these domains, practitioners will be better equipped to mitigate potential vulnerability and support interdisciplinary harm management outcomes.

Insider Threat (IT)

[11] A. Simons & J.R. Meloy, "Foundations of threat assessment and management," in *Handbook of Behavioral Criminology*, eds. V.B. Van Hasselt & M.L. Bourke, (New York, NY: Springer, 2017), pp. 627-644.

[12] ibid.

[13] B.G. Sellers, S.L. Desmarais, & M.W. Hanger, "Measurement of change in dynamic factors using the START:AV," *Journal of Forensic Psychology Research and Practice* 17, 3 (2017): pp. 198-215; A. Paetscha, T.W.P. van Osb, N.A.C. Troquetea, & R.H.S. van den Brinka, "Single-item predictive validity of the Short-Term Assessment of Risk and Treatability (START) for violent behavior in outpatient forensic psychiatry," *The Journal of Forensic Psychiatry and Psychology* 30 ,4 (2019): pp. 630-641; R.A. Knudsen, "Between vulnerability and risk? Mental health in UK counter-terrorism," *Behavioral Sciences of Terrorism and Political Aggression*, https://doi.org/10.1080/19434472.2019.1703782

IT encompasses a range of hostile actions. Whilst the outcomes of IT are significant and well-documented, the processes which give rise to them are only partially understood[14]. Similarly, Kont et al.[15] assert IT is comprehensively discussed, yet poorly defined. For clarity, IT is defined as "… the danger posed by an individual who possesses legitimate access and occupies a position of trust in or with the infrastructure or institution being targeted"[16]'. Furthering Catrantzos, Kont et al. define the *insider* as a member of an organisation who is *authenticated* to perform certain tasks[17]. Equally, Kont et al. and Alexander [18] recognise ITs can be orchestrated by unauthorised persons, such as former or current employees, fraudulently accessing systems - either through self-directed malice or the influence of external pressure. While threats from unintentional insiders (defined as an individual whose actions, although lacking malevolent intent, negatively impact an organisation's security'[19]) should not be discounted,[20] this paper focuses on the ideological and psychological processes which underpin premeditated attacks.

[14] R.C. Brackney, & R.H. Anderson, "*Understanding the Insider Threat: Proceedings of a March 2004 Workshop*". (Santa Monica, CA: RAND, 2004), rand.org/content/dam/rand/pubs/conf_proceedings/2005/RAND_CF196.pdf; Q. Yaseen, & B. Panda, "Insider threat mitigation: Preventing unauthorized knowledge acquisition," *International Journal of Information Security* 11, 4 (2012): 269-280; M. Bunn & S. Sagan, "Introduction: Inside the Insider Threat," in *Insider Threats,* eds. M. Bunn & S. Sagan, (Ithaca, NY: Cornell University Press, 2016), pp. 1-9; D. BaMaung, D. McIlhatton, M. MacDonald & R. Beattie, "The enemy within? The connection between insider threat and terrorism," *Studies in Conflict and Terrorism* 41, 2 (2018): pp, 133-150.

[15] M. Kont, M. Pihelgas, J. Wojtkowiak, L. Trinberg & A-M Osula, "*Insider Threat Detection Study*". (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015), p. 12.

[16] N. Catrantzos, *Managing the Threat: No Dark Corners,* (London: CRC Press, 2012), p. 4.

[17] Kont, M. Pihelgas, Wojtkowiak, Trinberg & Osula, "*Insider Threat Detection Study*", p. 12.

[18] ibid.; M. Alexander, "Protect, detect and correct methodology to mitigate incidents: Insider threats," *ISACA Journal* 3 (2018):pp.1-7.

[19] Kont, Pihelgas, Wojtkowiak, Trinberg A-M Osula, "*Insider Threat Detection Study*", p. 18.

[20] Brackney & Anderson, "*Understanding the Insider Threat*"; Kont, M. Pihelgas, Wojtkowiak, Trinberg & Osula, "*Insider Threat Detection Study*".

Although contemporary IT discussions are largely concerned with the cyber environment, Bunn and Sagan[21] insist ITs comprise three district domains: Passive – those who release information concerning their organisation's security protocols to an outside agency; active – those who provide physical access to a hostile actor and violent – those who are prepared to use force against their colleagues. Similarly, Kont et al.[22] promote five IT profiles: sabotage, theft (of intellectual property), fraud, espionage, and unintentional insiders.

Given the range of profiles and activities associated with IT, it is important to consider the frequency with which they are recorded and acknowledge their implications. Acknowledging the Kremlin's uncompromising policy of "symbolic assassination" for defectors,[23] and the Chinese Communist Party's (CCP) hardline approach to internal corruption and disloyalty,[24] IT in many countries and organisations is notoriously underreported.[25]

In a Western context, underreporting is often attributed to organisational concerns around perceived difficulties in identifying the details of an incident and

[21] Bunn & Sagan, *Insider Threats*, p. 4.

[22] Kont, M. Pihelgas, Wojtkowiak, Trinberg & Osula, "*Insider Threat Detection Study*, p. 3.

[23] D. V. Gioe, M.S. Goodman & D.S. Frey "Unforgiven: Russian Intelligence vengeance as political theater and strategic messaging," *Intelligence & National Security*, (2019):pp. 1-15, https://doi.org/10.1080/02684527.2019.1573537.

[24] M. Purbrick, "All the President's men – corruption in the Xi Jinping era," *China Brief* 22, 17 (2022), https://jamestown.org/program/all-the-presidents-men-corruption-in-the-xi-jinping-era/

[25] M.R. Randazzo, M.M. Keeney, E.F. Kowalski, D.M. Cappelli & A.P. Moore, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector* (Pittsburgh, P.A: Carnegie Mellon University, 2005), http://www.sei.cmu.edu/reports/04tr021.pdf; E.D. Shaw & H.V. Stock, *Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall* (Mountain View, CA: Symantec, 2011), https://zadereyko.info/downloads/Malicious_Insider.pdf; M. Massberg, J. Warren & N. Lang Beebe, "The Dark Side of the Insider: Detecting the Insider Threat Through Examination of Dark Triad Personality Traits," (paper presented at 48th Hawaii International Conference on System Science, Kauai, Hawaii, January 2015).

securing prosecutions, as well as the potential for reputational damage.[26] Of note, the National Counterintelligence and Security Center (NCSC),[27] insists the threat of trusted insiders disclosing sensitive information is likely to remain significant. Similarly, Alexander[28] concluded IT is both the second largest cause of data loss worldwide and the leading cause of global protected health information data breaches.

Although behaviours that would, almost certainly, be considered IT by today's standards date back to the ancient world[29] the contemporary study of IT can be traced to a US Government's counterintelligence activity *Project Slammer* that ran throughout the late 1980s.[30] Historical IT data is detail-rich. It benefits greatly from accurate descriptions of specific events and theoretical formulations regarding likely motivational antecedents. It is, however, limited both in terms of statistical analysis concerning potential trends, as well as commentary on the overall incidence of IT in a given period or setting.[31] More recently, Ponemon Institute revealed a 15% increase in global malicious insider attacks between 2017-2018, with an average annual cost of

[26] O. Brdiczka, "Insider Threats – how they affect US companies. What risk factors do US companies face? And how should they respond to insider threats?" *Computer World* (2014), https://www.computerworld.com/article/2691620/insider-threats-how-they-affect-us-companies.html; J.J. Kathuria & A. Bhardwaj, "Insider threat: The dangers within" *Mandiant* (2022), https://www.mandiant.com/resources/blog/insider-threat-dangers-within.

[27] National Counterintelligence and Security Center (NCSC) *Strategic Plan: 2018-2020*. (Washington, DC: NCSC, n.d.).

[28] Alexander, "Protect, detect and correct methodology to mitigate incidents."

[29] N. Powers, "What history teaches us about today's insider threats," *Delta Risk* (2017), https://deltarisk.com/blog/what-history-teaches-us-about-todays-insider-threats/.

[30] M. Weir & R. A. Nettles, "Introduction: Insider Threat and the Malicious Insider Threat – Analyze. Deter. Discover. Prevent. Respond." *CSIAC Journal of Cyber Security and Information Systems* 6, 1 (2018):pp. 4-5.

[31] This is exemplified in the Project Slammer files, accessible via: https://www.cia.gov/readingroom/docs/CIA-RDP87-00812R000200070011-7.pdf

$1,621,075 per organisation.[32] Ponemon Institute reported an 8% rise in malicious insider threat incidents between 2020 and 2022, with an average cost of $701,500 per malicious incident.[33] Having analysed a range of international multisector data breaches, Verizon asserts Public Administration suffered the greatest number of confirmed data breaches in 2021 (584, out of a total of 3,273 incidents).[34] Of the incidents, 30% were attributed to internal actors, with personal information being the most compromised data set.[35] In addition, a 2019 study incorporating more than 500 information technology leaders (senior managers) and 4000 employees from the UK and the US indicated 61% of information technology leaders believed their previously loyal employees had maliciously harmed their organisations between 2018-2019. A further 46 percent of organisations expect to suffer a malicious insider breach in the preceding twelve months[36]. For many employees, it appears organisational loyalty is limited to their period of employment. egress reports 23 percent revealed information concerning their former organisations when starting a new position.[37]

In addition to being an underreported phenomenon, the development and implications of IT share many similarities whilst also remaining qualitatively distinct. According to Verizon, 83 percent of international data breaches are attributed to external threat actors (typically criminal organisations) seeking financial gain.[38] Verizon affirms that 74 percent of international data breaches involve a human component – a

[32] Ponemon Institute, "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. Unlocking the Value of Improved Cybersecurity Protection," (2019), https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

[33] Ponemon, *Cost of Insider Risks. Global Report 2023* (Michigan: Ponemon Institute, 2023), p. 23.

[34] Verizon, *DBIR 2023 Data Breach Investigations Report* (Verizon Business, 2023).

[35] ibid.p. 63.

[36] egress, "CIOs and Employees Differ on Data Ethics, Ownership and Root Causes of Insider Breaches," (2019), https://www.egress.com/en-US/news/insider-data-breach-survey-2019-na.

[37] ibid.

[38] Verizon, *DBIR 2023 Data Breach Investigations Report, p. 8.*

9.8 percent decrease from 2022.[39] Verizon identifies a critical intersection between external threat actors, insiders and, in certain cases, business partners,[40] Referencing breaches in the professional, scientific and technical sectors, Verizon refers to this human-centric threat interaction as ”multi-actor breaches,” which typically involve the recruitment of an internal actor (or partner) by an external entity.[41] Verizon attributes this threat interaction to a form of *social engineering*, which they define as “A psychological compromise of a person that alters their behaviour into taking an action or breaching confidentiality.[42]” Verizon suggests that social exploitation in this psychological compromise may result from deception, manipulation, or intimidation of personnel.[43]

Information concerning the effects of social engineering on IT is in short supply. However, Verizon insists social engineering helps conceal security breaches, thus making the threat harder to detect.[44] It may also contribute to the *privilege misuse* that Verizon aligns with IT[45]. Given the potential implications of social engineering upon an organisation’s security, further research into its origins, development and application is likely to prove advantageous.

IT activities conducted in the cyber or technical domains share similarities with those in the physical world – as the individual’s intent is carefully masked throughout the period leading up to (and, in some cases, post) the commission of the act(s). In the context of physical IT, however, the individual’s motivation and modus operandi are instrumental in determining the degree to which his/her actions remain concealed. For certain malicious insiders, success is contingent upon the sustained maintenance of

[39] ibid.

[40] Verizon, *DBIR Data Breach Investigations Report 2008-2022* (Verizon Business, 2022), https://www.verizon.com/business/resources/reports/dbir/.

[41] ibid., p. 70.

[42] ibid., p. 24.

[43] ibid., p. 14.

[44] Verizon, *DBIR 2023 Data Breach Investigations Report*; Verizon, *DBIR Data Breach Investigations Report 2008-2022.*

[45] Verizon, *DBIR Data Breach Investigations Report 2008-2022, pp,47-48.*

discretion, interpersonal deception, and secrecy; for others, it is underwritten by a sudden elevation in profile. In either case, once revealed, the conduct of a physical IT is likely to attract media attention and marked speculation concerning his/her motive(s), state(s) of mind and ideological commitment(s).

The undertakings of the Royal Canadian Mounted Police (RCMP) former senior intelligence officer Cameron Ortis, who is alleged to have supplied sensitive material to a 'foreign entity' or "terrorist organisation"[46] exemplify the slow-burn low-profile approach to IT. Conversely, the actions of the late Germanwings Pilot, Andreas Lubitz, highlight the catastrophic impact of a deliberately orchestrated singular malicious event.[47] Similarly, the US Army Psychiatrist Nidal Hasan,[48] and Saudi Air Force member Ahmed Mohammed al-Shamrani,[49] demonstrated their underlying commitment to extremist Islamic ideals through highly conspicuous one-off projections of lethal force against the US Government[50]. Of concern for His Majesty's Government (HMG) is the case of the former Royal Marine Commando, Ciaran Maxwell. Convicted

[46] D. Lao, "3 more charges laid against former RCMP official Cameron Ortis," Global News, 27 January 2020, https://globalnews.ca/news/6469618/cameron-ortis-charges-rcmp/.

[47] J.M. Clark, "Assuring safer skies?: A survey of aeromedical issues post-Germanwings," *Journal of Air Law and Commerce* 81, 3 (2016): 351-375; K. Hoffman, "The psychology of the lone terrorist: Identification with the aggressor in individuals and in societies," *International Forum of Psychoanalysis* 26, 4 (2017): pp. 200-206.

[48] Responsible for killing thirteen and wounding a further forty-three US Department of Defence employees at Fort Hood in 2009 (R. Schouten, "NC3 Insider Threats," Nautilus Institute for Security and Sustainability, 14 November 2019, https://nautilus.org/napsnet/napsnet-special-reports/nc3-insider-threats/).

[49] Responsible for killing three US sailors at Naval Air Station Pensacola in 2019 (D. Barrett & M. Zapotosky, "Pensacola shooting was an act of terrorism, attorney general says," Washington Post, 13 January 2020, https://www.washingtonpost.com/national-security/pensacola-shooting-was-an-act-of-terrorism-attorney-general-says/2020/01/13/34dbed8e-3629-11ea-bf30-ad313e4ec754_story.html.

[50] Bunn & Sagan, *Insider Threats;* K. M Sarma, "Risk assessment and the prevention of radicalization from nonviolence into terrorism," *American Psychologist* 72, 3 (2017): pp. 278-288; BaMaung, McIlhatton, MacDonald & Beattie, "The enemy within?"; Schouten, "NC3 Insider Threats"; Barrett & Zapotosky, "Pensacola shooting".

for terrorism and associated offences involving Dissident Republican groups in Northern Ireland, Maxwell was sentenced to eighteen years imprisonment in 2017, with an additional five years on licence[51]. In sentencing, Mr. Justice Sweeney commented unequivocally on Maxwell's motivation, emphasising his "… Dissident Republican sympathies and hostility to the United Kingdom …[52]".

Discussing the IT challenges of the nation-state defines IT as: 'The threat that an insider may harm, intentionally or unintentionally, national security. This threat can include damage through fratricide, espionage, terrorism, unauthorised disclosure of information or through loss or degradation of resources or capabilities.[53] MoD categorises IT as *non-traditional*, with the capacity to reduce strategic intent and undermine cohesive relationships.[54] Acknowledging the likelihood of direct, physical IT attacks occurring in situations or environments regarded as *safe* (for example, a forward operating base[55]), and involving local national allies, MoD emphasises the value of effective risk mitigation – for example, robust force protection measures. Additionally, MoD highlights the perennial need to understand local cultural atmospherics. In his analysis of *Green on Blue* IT attacks against Western personnel in Afghanistan (defined as Attacks by the Afghan National Army, Afghan, National Police, Afghan Air Force, and Afghan Local Police (*Green*), on US and NATO troops and civilian personnel (*Blue*)), Ahmad affirms the cross-cultural interpersonal dimensions of

[51] PSNI, "Ciaran Maxwell: Royal Marine bomb maker given 18 years," BBC News, 31 July 2017, https://www.bbc.co.uk/news/uk-northern-ireland-40774233.

[52] V. Dodd & J. Grierson, "Royal Marine who supplied arms for Irish republican attacks jailed for 18 years," The Guardian, 31 July 2017, https://www.theguardian.com/uk-news/2017/jul/31/royal-marine-ciaran-maxwell-arms-irish-republican-attacks-jailed.

[53] Ministry of Defence, "JDN 1/14" (not ratified), quoted in Ministry of Defence (MoD), *Joint Doctrine Publication 0-01.1 UK Terminology Supplement to NATOTerm: Joint Doctrine Publication (JDP) 0-01.1,* Edition A. (Swindon: Development, Concepts and Doctrine Centre (DCDC), 2019), p. 23.

[54] Ministry of Defence (MoD), *Allied Joint Doctrine for Force Protection Edition A Version 1: Allied Joint Publication (JDP) -3.14.* (Swindon: Development, Concepts and Doctrine Centre (DCDC), 2015), pp. 4-10.

[55] ibid. 1-1

insider attacks made them a "cultural weapon" which, for a considerable period, represented the "preferred warfighting tactic of the Taliban."[56]

The individualised, culturally nuanced characteristics of IT represent a consistent theme and a point of grave concern. These dynamics can be understood more clearly by adopting an idiographic perspective that examines the interpretive lens through which the person perceives him/herself relative to others and subsequently determines his/her place in the world. Thus, the ideological, situational, and psychological dimensions of IT require careful attention.

Ideological, Psychological and Situational Dimensions of Insider Threat

With his professional and social pedigree firmly rooted in the British upperclass, the Old Etonian and Cambridge graduate Harold A.R. *Kim* Philby was, by outward appearances, the consummate British civil servant. Regarded as one of the most successful penetration agents to have lived;[57] when asked in 1963 to explain his defection to the Soviet Union, Philby offered a poignant disclosure: "To betray, you must first belong … I never belonged."[58] Philby's aphoristic candour not only delivers a brief, crucial glimpse into his inner world, but it provides an essential clue as to the prominent driving forces behind IT: Self-perspective, ideology, and psychological discord. Although care must be taken when generalising from specific case studies,[59]

[56] J. Ahmad, *Dress Like Allies, Kill Like Enemies: An Analysis of 'Insider Attacks' in Afghanistan,* (West Point, NY: West Point, 2017), pp. 3-4.

[57] B. Macintyre, *A Spy Among Friends: Kim Philby and the Great Betrayal,* (New York, NY: Broadway Books, 2014).

[58] *Oxford Essential Quotations* 6th ed. ed. S. Ratcliffe (Oxon: Oxford University Press, 2018), p. 150.
D.A. Crighton, "Risk Assessment," in *Forensic Psychology* 2nd ed. eds. D.A. Crighton & G.J. Towl, (Oxon: Wiley & Son, 2015), pp. 97-111.

[59] R. Gomm, M. Hammersley & P. Foster, "Case study and generalisation," in *Case Study Method* eds. R. Gomm, M. Hammersley & P. Foster (New York, NY: Sage, 2009), pp. 98-115.

Philby embodies the extensive insider threat posed by a highly motivated actor with an entrenched ideological view.

Philby's ideological bond with socialism began during his early days at Cambridge in 1929,[60] Harbouring a determination to dedicate himself to the communist cause, Philby joined Britain's Secret Intelligence Service (MI6) in 1940 "with the meticulously concealed intent of spying for the Soviets – as he recalls," '… a prior total commitment to the Soviet Union …'[61]. Once established, Philby held numerous senior posts, whilst at the same time developing ever-closer connections with the KGB[62]

Although the extent of his actions ensures Philby remains an *outlier* in IT circles, his mastery of deception highlights several critical points for (Counter) Intelligence (CI) professionals; one of the more notable being the importance of continually re-examining one's perceptions of a person's decision to betray. Contemporary analysts largely agreed the decision to undertake malicious internal activity is the result of an intricate psychosocial process. In most Western contexts, however, malicious insiders do not join their respective organisations with a pre-existing intent to cause harm.[63] It is essential, therefore, to examine the ideological, situational, and psychological dimensions that influence their respective betrayals.

Throughout the latter part of the Twentieth century, IT was typically evaluated through the prism of individual weaknesses or personal vulnerabilities. This is exemplified in the acronym MICE (Money, Ideology, Coercion/Compromise and Ego[64]),

[60] K. Philby, *My Silent War. The Autobiography of a Spy.* (London: Arrow Books, 1968/2018).

[61] ibid., p.xxix.

[62] ibid; E.D.R. Harrison, "More thoughts on Kim Philby's *My Silent War," Intelligence and National Security* 10, 3 (1995): pp 514-525; B. Macintyre, *A Spy Among Friends.*

[63] G. K. Gronvall, "Managing the insider threat in high-containment laboratories," in *A Crossroads in Biosecurity: Steps to Strengthen U.S. Preparedness* ed. M.B. Hansen (Baltimore, MD: Center for Biosecurity of UPMC, 2011), pp.13-16; INSA, *Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation.* (Arlington, VA: INSA, 2017).

[64]R. Burkett, "An alternative Framework for Agent Recruitment: From MICE to RASCLS," *Studies in Intelligence* 57, 1 (2013): pp. 7-17; A. Vashisth & A. Kumar, "Corporate espionage: The insider threat,"

which remains an anecdotal reference point for many contemporary CI professionals. Despite the utility of the MICE model in framing IT discussions and highlighting the essential consideration that “motive precedes opportunity,"[65] IT commentators affirm MICE should not be regarded as a stand-alone explanatory paradigm of IT risk.[66] Likewise, the role of ideology as a driver for IT attracts considerable debate.

According to Burkett, ideology is a potent weapon in IT, with ideologically motivated ITs, representing a grave concern for CI officers,[67] This view is endorsed by a UK-based multisite study of 120 IT events which cites ideology as a primary motivator in 20% of cases (the other motivational factors include financial incentive (47 percent), a desire for recognition (14 percent), loyalty to friends/family/country (14percent), and revenge (6%)).[68] Similarly, Ahmad observes ideological factors can influence IT internally - as a source of friction between partners who hold divergent cultural views, and externally - as a means of exerting pressure upon an individual by a malignant third party.[69] Conversely, Barron, Levchenko and Fischer acknowledge the relevance of ideological factors in the recruitment of agents during the Cold War but question their contemporary efficacy.[70] As a potential consequence of these conflicting views, risk-centric discussions of ideology occupy limited space in the IT literature. As IT is a profoundly human problem, a failure to engage with the potential ideological-

Business Information Review 30, 2 (2013): pp. 83–90; K.A. Kennedy “Management and mitigation of insider threats,” in *Handbook of Behavioural Criminology:* pp, 485-500.

[65] C.F. Noonan, *Spy the Lie: Detecting Malicious Insiders*. (Richland, WA: U.S. Department of Energy, 2018), 2.9.

[66] Burkett, “An alternative Framework for Agent Recruitment”; Alexander, “Protect, detect and correct"; Noonan, *Spy the Lie.*

[67] Burkett, “An alternative Framework for Agent Recruitment”, p. 10.

[68] CPNI, *CPNI Insider Data Collection Study: Report of Main Findings*. (London: CPNI, 2013), p. 9.

[69] Ahmad, *Dress Like Allies, Kill Like Enemies*.

[70] J. Barron, *KGB Today: The Hidden Hand*. (New York, NY: Berkley Books, 1985); S. Levchenko, *On the Wrong Side: My Life in the KGB*. (New York, NY: Pergamon, 1988); L.F. Fischer, *Espionage: Why Does it Happen?* (2000), https://usnwc.libguides.com/c.php?g=661096&p=4721274.

psychological crossover raises concern over the successful identification and management of individual vulnerability.

An effective response must recognise that IT inhabits the interactional or 'transitional' space,[71] between the individual and his/her surroundings. Thereafter, it is essential to acknowledge IT is influenced by myriad interpersonal connections and brought to bear through a matrix of personal interpretive frameworks and ideological channels. A reconstituted approach to ideology is likely to foster a more detailed understanding of its unique risks, whilst simultaneously highlighting its latent protective qualities. To capitalise upon the predictive accuracy of ideology in IT assessment, it is necessary to consider its principal features and dynamic nature.

Bryans et al. and Kennedy describe ideology in terms of an individual's commitment to a nationalist, political, religious or supremacist belief system and, on occasion, the use of violence to further their group's objectives.[72] The validity of this position is hard to discount. Charney and Irvin concur with the proposition that ideology represents a shared belief system; however, they apply an idiographic view, by emphasising the degree to which it is governed by a series of unique psychological factors.[73] Charney and Irvin maintain ideology becomes the conduit through which the person confirms and, in certain cases, enacts, his/her worldviews.[74] Likewise, Burkett stresses the need for intelligence practitioners to recognise the web of interpersonal loyalties that coalesce – and occasionally conflict - to influence the person's ideological perspectives and decision-making.[75] For Burkett, the complexity of ideologically driven decision-making processes is magnified when the person risks severe consequences by

[71] D.W. Winnicott, "Transitional objects and transitional phenomena." *International Journal of Psychoanalysis* 34, 2 (1953): pp. 89-97.

[72] Bryans, Barzanò & Meissner, *Handbook on the Management of Violent Extremist Prisoners;* Kennedy "Management and mitigation of insider threats."

[73] D.L. Charney & J.A. Irvin, "The psychology of espionage," *Intelligencer: Journal of U.S. Intelligence Studies* 22, 1 (2016): pp. 71-77.

[74] ibid. 72.

[75] Burkett, "An alternative Framework for Agent Recruitment."

turning against established peers or colleagues.[76] Commentators insist the ambiguity surrounding a person's ideological worldview can be better understood by applying a psychological rationale.[77] It is essential, therefore, to consider both the psychological traits and psychosocial pathways that increase the likelihood of a person engaging in IT.[78]

Whilst Pfleeger, Charney, and INSA affirm it would be erroneous to propose rigid psychological traits or a "psychological profile" predispose an individual to IT,[79] INSA draw upon Post et al. to highlight a 'cluster model' (Figure 1) involving five personality disorders which appear indicative of information technology-based IT risks.[80] According to Shaw et al. and INSA, Cluster One - Avoidant and Schizoid typologies show a heightened interest in computer systems; whereas, Cluster Two -

[76] ibid.

[77] R. Borum, "Understanding the terrorist mindset." *FBI Law Enforcement Bulletin* 72, 7 (2003): pp. 7–10; M.T. Miliora, "The psychology and ideology of an Islamic terrorist leader: Usama bin Laden." *International Journal of Applied Psychoanalytic Studies* 1, 2 (2004): pp. 121-139; F.M. Moghaddam, "The staircase to terrorism: A psychological exploration." *American Psychologist* 60, 2 (2005): pp. 161-169; J.T. Jost, B.A. Nosek & S.D. Gosling, "Ideology: Its resurgence in social, personality, and political psychology." *Perspectives on Psychological Science* 3, 2 (2008): pp. 126-136; Z. Al-Attar, "Interviewing terrorism suspects and offenders with an Autism Spectrum Disorder." *International Journal of Forensic Mental Health* 17 4 (2018): pp. 321-337; G. Rifkind, *The Psychology of Political Extremism: What Would Sigmund Freud have Thought About Islamic State?* (Oxon: Routledge, 2018); R.H. Hamden, *Psychology of Terrorists: Profiling and CounterAction.* (London: CRC Press/Taylor & Francis, 2019).

[78] E.D. Shaw, K.G. Ruby & J.M. Post, "The insider threat to information systems: The psychology of the dangerous insider." *Security Awareness Bulletin* 2, 1998, http://www.pol-psych.com/sab.pdf; E. Shaw & L. Sellers, "Application of the critical-path method to evaluate insider risks." *Studies in Intelligence* 59, 2, 2015, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies

[79] C.P. Pfleeger, "Reflections on the insider threat," in *Insider Attack and Cyber Security: Advances in Information Security,* ed. S.J. Stolfo, S.M. Bellovin, A.D. Keromytis, S. Hershkop, S.W, Smith, & S. Sinclair (Boston, MA: Springer), 5-15; D.L. Charney, "True psychology of the insider spy." *Intelligencer: Journal of U.S. Intelligence Studies* Fall/Winter (2010): 47-54; INSA, "Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation."

[80] INSA, "Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation."

Anti-social, Narcissistic and Paranoid typologies demonstrate behaviours indicative of entitlement, reduced loyalty and ethical flexibility and were prominent in an espionage context.[81] Notably, social, and personal frustration and limited empathy were consistent across both clusters.[82]

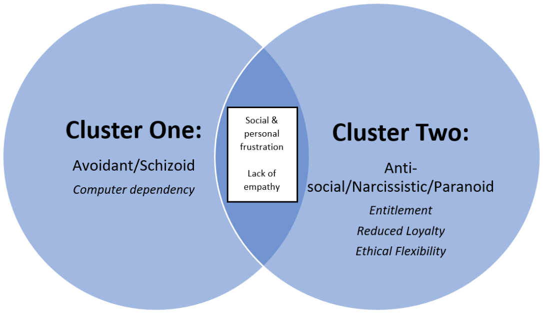

Figure 1 - personality clusters and information technology-based IT risks (adapted from INSA[83]).

Claycomb et al.; Greitzer et al.; Maasberg et al.; Shaw and Sellers; Dupuis and Khadeer, and Wilder attend to those traits which may increase individual vulnerability to IT.[84] Although numerous personality models are promoted within the social

[81] Shaw, Ruby & Post, "The insider threat to information systems"; INSA, "Assessing the Mind of the Malicious Insider," pp. 3-4.

[82] ibid.

[83] INSA, *Assessing the Mind of the Malicious Insider*, 3.

[84] W.R. Claycomb, C.L. Huth, L. Flynn, D.M. McIntire & T.B. Lewellen, "Chronological examination of insider threat sabotage: Preliminary observations," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 3, 4 (2012): pp. 4-20; F.L. Greitzer, L.J. Kangas, C.F. Noonan, C.R. Brown & T. Ferryman, "Psychosocial modelling of insider threat risk based on behavioral and word use analysis," *E-Service Journal* 3, 1 (2013): pp. 106-141; Massberg, Warren & Lang Beebe, "The Dark Side of the Insider"; Shaw & Sellers, "Application of the critical-path method to evaluate insider risks."; M. Dupuis & S. Khadeer, "Curiosity Killed the Organisation: A Psychological Comparison between Malicious and Non-malicious Insiders and the Insider Threat," *Proceedings of the 5th Annual Conference on Research in Information Technology* (September 2016), 35-40; U.M. Wilder, "Why spy now? The psychology of espionage and leaking in the digital age," *Studies in Intelligence* 61, 2 (2017): pp. 1-36.

sciences, the Five-Factor Model (FFM) is widely accepted.[85] Advocating the analysis of personality through five interrelated domains (extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience), the relevance of the FFM within an IT context has been studiously critiqued.[86] Although Brdiczka et al. and Axelrad et al. discuss the benefits of the FFM in studying the static personality dimensions associated with IT, Massberg et al. and Noonan identify shortcomings in the FFM approach, especially, a limited focus on antisocial and malevolent behavioural characteristics.[87]

Massberg et al. and Noonan and Myers and Trent advocate consideration of the 'dark triad (Psychopathy, Narcissism and Machiavellianism)[88] of personality traits in IT analysis.[89] Massberg et al. affirm whilst dark triad characteristics should not be deemed

[85]A.E. Poropat, "A meta-analysis of the five-factor model of personality and academic performance," *Psychological Bulletin* 135, 2 (2009): pp. 322-338; T.A. Widiger, W.L. Gore, C. Crego, S.L. Rojas & J.R. Oltmanns, "Five-Factor Model and Personality Disorder" in *The Oxford Handbook of the Five Factor Model of Personality* ed. T.A. Widiger (Oxford Handbooks Online), DOI: 10.1093/oxfordhb/9780199352487.013.4 (2016).

[86] O. Brdiczka, B. Price, J. Shen, A. Patil, R. Chow, E. Bart & N. Ducheneaut, "Proactive insider threat detection through graph learning and psychological context," *SPW '12: Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops* (2012), DOI 10.1109/SPW.2012.29; Massberg, Warren & Lang Beebe, "The Dark Side of the Insider"; Noonan, *Spy the Lie*.

[87]Brdiczka, Price, Shen, Patil, Chow, Bart & Ducheneaut, "Proactive insider threat detection"; E.T. Axelrad, P.J. Sticha, O. Brdiczka & J. Shen, "A Bayesian network model for predicting insider threats," *2013 IEEE Security and Privacy Workshops* (2013), DOI 10.1109/SPW.2013.35; Massberg, Warren & Lang Beebe, "The Dark Side of the Insider"; Noonan, *Spy the Lie*.

[88] Psychopathy – formulated upon three core facets: Arrogant and deceitful interpersonal style, limited affect, and impulsive, irresponsible behaviours. Narcissism – behaviours indicating persistent attention-seeking, high levels of vanity, excessive self-focus, and the pursuit of exploitative interpersonal relationships. Machiavellianism – a preference for interpersonal strategies grounded in self-interest, deception, and manipulation (S. Jakobwitz & V. Egan, "The dark triad and normal personality traits" *Personality and Individual Differences* 40, 2 (2006): pp, 332-333).

[89] Massberg, Warren & Lang Beebe, "The Dark Side of the Insider"; Noonan, *Spy the Lie*; C. Myers & A. Trent, "Operational psychology in insider threat," in *Operational Psychology: A New Field to Support*

explanatory, their inclusion enables a detailed understanding of the malevolent character traits and interpersonal deviance associated with IT, especially when examined in parallel with an individual's mood and stress responses.[90] It is important to note that the comprehensive assessment of a person's psychological disposition carries myriad time-related, ethical, and financial implications. Nevertheless, Dupuis and Khadeer highlight the relevance of the dark triad in assessing potential vulnerability to IT, whilst emphasising the value of simultaneously examining both negative affect and malicious intent.[91] Dupuis and Khadeer contend the potential risks associated with the dark triad are magnified when the individual experiences consistent periods of negative affect, such as fear, doubt, or uncertainty. They caution that should these emotions remain unaddressed, the individual is at greater risk of feeling overlooked or undervalued; thereby, triggering a decline in organisational commitment and the potential onset of malicious worldviews.[92] Acknowledging opportunities to enhance IT mitigation, Noonan advocates the development of the dark triad model.[93] Noonan promotes the addition of a fourth trait – Sadism,[94] thus, suggesting analysis by means of a "dark tetrad."[95] Although further research is needed into the role of the dark tetrad in IT, Wilder describes it as relevant amongst individuals who engage in online trolling behaviours[96].

The overemphasis on personality-based approaches to IT vulnerability risks imposing analytical limitations by downplaying the significance of situational factors. Charney, Brdiczka et al., Greitzer et al.; Legg et al.; Massberg et al.; Shaw and Sellers;

National Security and Public Safety eds. M.A. Stall & S.C. Harvey (Santa Barbara, CA: ABC-CLIO, 2019), pp. 157-184.

[90] Massberg, Warren & Lang Beebe, "The Dark Side of the Insider."

[91] Dupuis & Khadeer, "Curiosity Killed the Organisation."

[92] ibid.

[93] Noonan, *Spy the Lie*.

[94] Sadism - 'the derivation of pleasure through cruelty and inflicting pain, humiliation, and other forms of suffering on individuals' (APA), "Sadism," in *APA Dictionary of Psychology* (2018), https://dictionary.apa.org/sadism

[95] Noonan, *Spy the Lie*, 2.10.

[96] Wilder, "Why spy now?".

Dupuis and Khadeer, and Myers and Trent, promote a dynamic, contextually sensitive view of IT identification[97]. One such approach is Massberg et al's Capability Motive Opportunity (CMO) model[98].

The CMO model is intended to interpret IT vulnerability and support the development of countermeasures[99]. Acknowledging IT attacks are typically planned in detail, the CMO model is grounded in a rational choice perspective[100]. It adopts a psychosocial position that aligns the individual's internal logic with the interpersonal circumstances and external events affecting his/her rationale. Massberg et al. and Elmrabit et al. propose that for an IT event to occur the motivated individual must possess the necessary motive(s) to act and, having identified a clear opportunity, he/she must have confidence in his/her capability to succeed[101].

Defining motive as 'a predictor of intent,' Massberg et al. describe the individual's motive(s) to engage in malicious activity as influencing his/her state of mind, whilst operating in conjunction with various external factors (opportunity and capability).[102] Having outlined those personality-based factors commonly associated with malicious insider activity, it is imperative to consider the external elements of the process. Massberg et al. describe opportunity as the scope or means by which the individual can manipulate organisational vulnerabilities, for example, gaining access

[97] Charney, "True psychology of the insider spy"; Brdiczka, Price, Shen, Patil, Chow, Bart & Ducheneaut, "Proactive insider threat detection"; Greitzer, Kangas, Noonan, Brown & Ferryman, "Psychosocial modeling of insider threat risk"; P. Legg, N. Moffat, J.R.C. Nurse, J. Happa, I. Agrafiotis, M. Goldsmith & S. Creese *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 4, 4 (2013): 20-37; Massberg, Warren & Lang Beebe, "The Dark Side of the Insider"; Shaw & Sellers, "Application of the critical-path method to evaluate insider risks"; Dupuis & Khadeer, "Curiosity Killed the Organisation"; Myers & Trent, "Operational psychology in insider threat".

[98] Massberg, Warren & Lang Beebe, "The Dark Side of the Insider".

[99] ibid.

[100] Shaw & Sellers, "Application of the critical-path method to evaluate insider risks".

[101] Massberg, Warren & Lang Beebe, "The Dark Side of the Insider"; N. Elmrabit, S-H. Yang & L. Yang, "Insider threats in information security categories and approaches" *21st International Conference on Automation and Computing (ICAC)* (2015), DOI: 10.1109/IConAC.2015.7313979.

[102] Massberg, Warren & Lang Beebe, "The Dark Side of the Insider," p. 3522.

through dated, ineffective, or absent security protocols, poor screening of potential employees, intermittent role auditing, limited task rotation and the retention of security clearances by former employees.[103] Massberg et al. affirm capability represent the individual's knowledge of organisational protocols and his/her skill at manipulating them.[104] Citing Willison and Siponen, Massberg et al. maintain the level of potential harm a dishonest employee represents is largely determined by the skills and knowledge he/she has obtained from inside the organisation.[105] Massberg et al. hypothesise opportunity and capability increase the likelihood of an individual developing malicious intent and committing an IT incident.[106] Additionally, Massberg et al. emphasise the need to understand those specific trigger(s) that initiate the incident; they achieve this by examining the critical pathway(s) connecting opportunity and capability with the IT incident.[107]

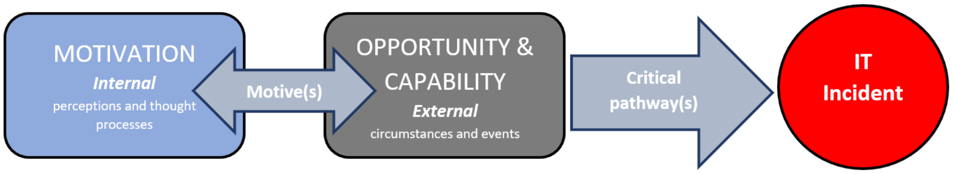

Figure 2 - CMO model and critical pathway(s)

Catrantzos; US Department of Homeland Security (DHS); Bunn and Sagan; INSA, and Wilder affirm individuals follow a "critical pathway" in the process of

[103] ibid.
[104] ibid.
[105] ibid., p. 3253.
[106] Massberg, Warren & Lang Beebe, "The Dark Side of the Insider."
[107] ibid.

becoming an IT.[108] Shaw and Sellers' criticalpath approach.[109]is one of the more widely discussed IT paradigms.[110]

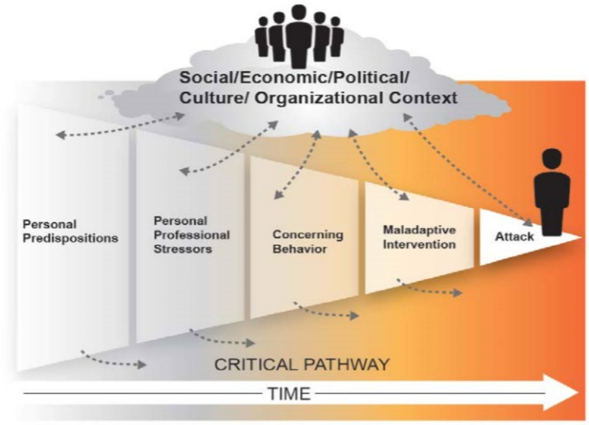

Figure 3 – critical pathway to IT attack (Noonan[111])

The pathway begins by examining the individual's psychological predispositions. Paralleling many of the traits discussed – whilst also considering factors such as alcoholism and compromising interpersonal relationships the individual's psychological predispositions are exacerbated by personal and professional stressors, including familial pressures and/or financial difficulties.[112] Personal and professional life stressors are comprehensively discussed within the IT community. Charney promotes a developmental perspective which examines the individual's self-

[108] Catrantzos, *Managing the Threat: No Dark Corners*; US Department of Homeland Security, National Cybersecurity and Communications Integration Center, "Combating the Insider Threat." (2 May 2014), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cisa.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf; Bunn & Sagan, *Insider Threats*; INSA, *Assessing the Mind of the Malicious Insider*; Wilder, "Why spy now?"

[109] Shaw & Sellers, "Application of the critical-path method to evaluate insider risks."

[110] Noonan, *Spy the Lie*; Myers & Trent, "Operational psychology in insider threat."

[111] Noonan, *Spy the Lie, pp.* 4.35.

[112] Shaw & Sellers, "Application of the critical-path method to evaluate insider risks."

perspective alongside ten life stages and three existential challenges.[113] Similarly, Fischer; CPNI; INSA, and Brinksman et al. discuss the influence of age-related stressors on IT vulnerability.[114]

Fischer insists the bulk of military-related espionage offences are committed prior to the individual's thirtieth birthday; she notes, that this may be partially explained by the high proportion of under-thirties routinely exposed to sensitive information in military environments.[115] Brinksman et al. accentuate the challenges surrounding Millennials[116] with access to classified material. Brinksman et al. conclude that despite encountering similar risk factors as previous generations, Millennials undertake IT attacks at a lower frequency. Nevertheless, they highlight a series of generationally nuanced risks–such as lower levels of job satisfaction and excessive debt, as well as a heavy dependency upon technology and virtual relationships–as primary concerns for Millennials.[117]

CPNI and INSA affirm middle age represents a marked period of vulnerability.[118] INSA suggests people typically re-evaluate their lives during a "mid-life transition period" (between the ages of thirty-five and forty). They propose that at this point a 'symbiotic relationship' unfolds between an individual's work and personal life, wherein difficulties in one domain converge with the other.[119] The resultant elevation in stress appears to increase the likelihood of a person engaging in malicious activities. Similarly, CPNI observed almost half of the insider cases they identified were committed by persons aged between thirty-one and forty-five. CPNI reports the majority (76 percent) were *self-initiated* and attributable to a combination of financial,

[113] Charney, "True psychology of the insider spy."

[114] Fischer, *Espionage*; CPNI, *Insider Data Collection Study*; INSA, *Assessing the Mind of the Malicious Insider*; I. Brinksman, M. Christian, D. Johnston *et al.*, *Millennial Considerations on Insider Threat: Are We A Threat Or An Opportunity?* (Washington, DC: Georgetown University, 2019).

[115] Fischer, *Espionage.*

[116] Persons born between 1980 and 2000 (Brinksman *et al.*, *Millennial Considerations on Insider Threat, p.* 7).

[117] Brinksman *et al.*, *Millennial Considerations on Insider Threat.*

[118] CPNI, *Insider Data Collection Study*; INSA, *Assessing the Mind of the Malicious Insider*.

[119] ibid. p. 4.

ideological, and existential factors (such as a desire for recognition, conflicted loyalties, and revenge).[120]

Aligning the existential demands of middle age with gender, Charney and CPNI observe the bulk of malicious insider activity is committed by males.[121] Charney ascribes the gender imbalance to vulnerabilities in "male psychology" associated with a damaged ego and attributes these vulnerabilities to the painful recognition of a failure to manage life challenges and maintain a coherent sense of worth.[122] Thereafter, he outlines a sequence of "existential dilemmas" which initiate a spiralling loss of control and trigger those deep fissures in the "bedrock of personal pride" that precipitate IT events.[123]

Although not identifying a significant gender disparity, INSA affirms a perceived lack of control amplifies negative affect and feelings of injustice; thereby, increasing the likelihood of the person engaging in those counterproductive work behaviours associated with IT.[124] This parallels Dupuis and Khadeer's observations concerning the influence of negative mood upon dark triad personality traits in the context of IT risk[125] The root cause(s) of gender discrepancy in IT may benefit from ongoing analysis. Nevertheless, it is beneficial to recognise the influence of age-related factors upon IT, whilst simultaneously acknowledging the risks associated with the malevolent activity are further magnified when the individual feels overlooked or undervalued and experiences "an intolerable sense of personal failure."[126]

According to Noonan's (2018) critical path approach, aberrant behaviour (including IT), is a common reaction to chronic psychological distress.[127] It follows, that the third phase of Shaw and Sellers' critical-path method highlights a series of

[120] CPNI, *Insider Data Collection Study*; INSA, *Assessing the Mind of the Malicious Insider*, p. 9.
[121] Charney, "True psychology of the insider spy"; CPNI, *Insider Data Collection Study*.
[122] Charney, "True psychology of the insider spy", p. 48.
[123] ibid. p. 52.
[124] INSA, *Assessing the Mind of the Malicious Insider*.
[125] Dupuis & Khadeer, "Curiosity Killed the Organisation".
[126] Charney, "True psychology of the insider spy", p. 48.
[127] Noonan, *Spy the Lie*, 4.34.

concerning behaviours typically demonstrated by the malicious insider prior to committing the principal event.[128] Evaluative IT studies such as CPNI; DHS; Noonan, and INSA, concur that rebellious, combative, or hostile behaviours, betrayals of trust and the alienation of colleagues are especially concerning.[129] Likewise, Myers and Trent, suggest early-stage malicious insiders often engage in preparatory behaviours to assess the fortitude of organisational security protocols. They insist these behaviours can be used to identify potential hostile acts before they occur. Given the complexities surrounding IT, effective responses must balance rigorous investigative methodologies with respect for the suspect.[130]

Interpersonal stressors associated with the early stages of the critical path may be aggravated by poor organisational practices[131] and/or maladaptive organisational interventions. Ill-considered responses to a suspected IT event are ineffective in containing immediate risks and may accelerate malicious activities.[132] For Shaw and Sellers, effective interventions are purposefully structured, remaining proactive without becoming heavy-handed, humiliating, or aggressive.[133] Yaseen and Panda; CPNI; Bunn and Sagan; DHS; Brinksman et al., and NCSC recommend various strategies to aid in the identification and management of malicious activities.[134] When considering potential risk mitigation, it is helpful to note the critical-path model of IT vulnerability shares several convergent properties with those psychosocial processes that appear to underpin radicalisation.

[128] Shaw & Sellers, "Application of the critical-path method to evaluate insider risks".

[129] CPNI, *Insider Data Collection Study*; US Department of Homeland Security, National Cybersecurity and Communications Integration Center, "Combating the Insider Threat"; Noonan, *Spy the Lie;* INSA, *Assessing the Mind of the Malicious Insider*.

[130] Myers & Trent, "Operational psychology in insider threat".

[131] CPNI, *Insider Data Collection Study*, p. 13.

[132] Shaw & Sellers, "Application of the critical-path method to evaluate insider risks".

[133] ibid.

[134] Yaseen & Panda, "Insider threat mitigation"; CPNI, *Insider Data Collection Study*; Bunn & Sagan, *Insider Threats*; US Department of Homeland Security, National Cybersecurity and Communications Integration Center, "Combating the Insider Threat"; Brinksman *et al., "Millennial Considerations on Insider Threat";* National Counterintelligence and Security Center (NCSC) *Strategic Plan: 2018-2020.*

Radicalisation

The following discussion considers those aspects of the self and the associated psychosocial processes that may increase a person's vulnerability to extremist narratives and, potentially, terrorist activities. For many, this process is encapsulated under the term *radicalisation*. Despite attracting multinational interdisciplinary attention, a universally endorsed definition of radicalisation remains elusive.[135] Consequently, Schmid and Coolsaet caution widespread use of the term *radicalisation* oversimplifies an intricate diverse phenomenon.[136] Similarly, Schmid; Miller and Chauhan, and Sarma urge caution in the tendency to view radicalisation as a process that invariably leads to violence.[137] Whilst sustained critical analysis remains a cornerstone of theoretical advancement, the inability to reach an agreement on the defining characteristics of radicalisation risks limiting contemporary understanding and may forestall the development of effective response strategies.[138] Unsurprisingly,

[135] T. Veldhuis & J. Staun, *Islamic Radicalisation: A Root Cause Model* (The Hague: Netherlands Institute of International Relations Clingendael, 2009); A. P. Schmid, "Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review," (ICCT Research Paper, The Hague: International Centre for Counter-Terrorism, March 2013); A.P. Schmid, "Research on radicalization: Topics and themes," *Perspectives on Terrorism* 10, 3 (2016): pp. 26-32; M. Lloyd & C. Dean, "The development of structured guidelines for assessing risk in extremist offenders," *Journal of Threat Assessment and Management* 2, 1 (2015): pp. 40-52..

[136] Schmid, "Radicalisation, De-Radicalisation, Counter-Radicalisation," ; R Coolsaet, "Radicalization: The origins and limits of a contested concept," in *Radicalization in Belgium and the Netherlands: Critical Perspective on Violence and Security* eds. N. Fadil, M. de Konig & F. Ragazzi (London: I.B. Tauris, 2019), pp. 29-30.

[137] Schmid, "Radicalisation, De-Radicalisation, Counter-Radicalisation," C. Miller & L.S. Chauhan, "Radical beliefs and violent behavior," in *De-radicalization': Scientific insights for policy* ed. L. Colaert (Brussels: Flemish Peace Institute, 2017), pp. 23-46; K. M Sarma, "Risk assessment and the prevention of radicalization".

[138] S. Harris-Hogan, K. Barrelle & A. "Zammit, What is countering violent extremism? Exploring CVE policy and practice in Australia." *Behavioural Sciences of Terrorism and Political Aggression* 8, 1 (2016): pp. 6-

commentators describe research in the radicalisation field as being in a developmental stage.[139]

Although Lloyd and Dean and Abbas affirm radicalisation holds the distinct position of being both a process and an outcome,[140] this paper is principally concerned with the former and attempts to deconstruct the psychosocial and ideological interactions therein. Silke and Brown insist the use of the term *radicalisation* to describe a process of deepening commitment to violent causes or activism is a recent phenomenon[141]. Nevertheless, *radical* behaviours which escalate to the point of political activism, violence and, in certain cases, terrorism, have appeared as waves of political intent throughout history[142] and continue with alarming regularity.[143]

Referencing "secularized societal disengagement" (i.e., the rejection of Western democracy) in jihadist radicalisation, Klausen et al. suggest indications of extremist

24; N. Irwin, "The complexity of responding to home-grown terrorism: Radicalisation, de-radicalization and disengagement," *Journal of Policing, Intelligence, and Counter Terrorism* 10, 2 (2016):pp. 166-175.

[139] D. Pisoui & R. Ahmed, *Radicalisation Research – Gap Analysis.* (Amsterdam: RAN Centre of Excellence, 2016); Miller & Chauhan, "Radical beliefs and violent behavior".

[140] Lloyd & Dean, "The development of structured guidelines for assessing risk in extremist offenders"; T. Abbas, "Ethnicity and politics in contextualising far right and Islamist extremism," *Perspectives on Terrorism* 11, 3 (2017): pp. 54-61.

[141] A. Silke & K. Brown, "Radicalisation: The transformation of modern understanding of terrorist origins, psychology and motivation," in *State, Society, and National Security: Challenges and Opportunities in the 21st Century* ed. S. Jayakumar (Singapore: World Scientific Publishing, 2016), p. 129.

[142] E. Brighi, "The mimetic politics of lone-wolf terrorism," *Journal of International Political Theory* 11, 1, (2015): p. 145-164; A.P. Schmid, "Research on radicalization: Topics and themes," *Perspectives on Terrorism* 10, 3 (2016): pp. 26-32.

[143] UNDP, *Preventing Violent Extremism Through Promoting Inclusive Development, Tolerance and Respect for Diversity. A Development Response to Addressing Radicalization and Violent Extremism.* (New York, NY: United Nations Development Programme, 2016); CST, *Hate Fuel: The Hidden Online World Fuelling Far Right Terror.* (London: Community Security Trust, 2020).

positioning may go unreported or unnoticed in the immediate social context.[144] Additionally, Abbas cautions that despite recurrent episodes of far-right and Islamophobic violence - especially amongst so-called ”lone actor” terrorists - in North America and Europe, analysis in this field is hampered by reporting errors.[145] Attempts to interpret the causal factors of radicalisation or mitigate its potential consequences must take into consideration its deeply ingrained political roots. Thereafter, it is imperative to recognise the multitude of pathways into and through radicalisation, acknowledging individuals are attracted by the appeal of radical perspectives through a range of personal, interpersonal and/or sociocultural drivers – each coloured by shades of ideological nuance.

Ideological, Psychological and Situational Dimensions of Radicalisation

Commentators are largely agreed individual vulnerability to radicalisation and engagement in terrorism cannot be definitively "profiled."[146] Equally, the complex interplay between societal, ideological and, in certain cases, criminological dimensions of radicalisation suggest it constitutes an evolving process intimately connected with

[144] J. Klausen, R. Libretti, R., B.W.K. Hung & A.P. Jayasumana, "Radicalization trajectories: An evidence-based computational approach to dynamic risk assessment of "homegrown" Jihadists," *Studies in Conflict & Terrorism* 43, 7 (2020): p. 605.

[145] Abbas, "Ethnicity and politics in contextualising far right and Islamist extremism".

[146] J. G. Horgan, "From profiles to *pathways* and roots to *routes*: Perspectives from psychology on radicalization into terrorism," *The ANNALS of the American Academy of Political and Social Sciences* 618 (2008): 80-94; J.G. Horgan, *Walking Away from Terrorism: Accounts of Disengagement from Radical and Extremist Movements.* (New York, NY: Routledge, 2009); Veldhuis & Staun, *Islamic Radicalisation: A Root Cause Model; C.* McCauley & S. Moskalenko "Toward a profile of lone wolf terrorists: What moves an individual from radical opinion to radical action," *Terrorism and Political Violence* 26, 1 (2014): pp. 69-85; Royal College of Psychiatrists (RCP), *Counter-terrorism and Psychiatry: Position Statement PS04/16.* (London: Royal College of Psychiatrists, 2016); R.A. Knudsen, "Measuring radicalization: Risk assessment conceptualisations and practice in England and Wales," *Behavioral Sciences of Terrorism and Political Aggression* 12, 1 (2020b): pp. 37-54.

extremist thinking[147]; resolute political and/or ideological opposition[148] and, on occasions, increased willingness to commit acts of terrorism.[149]

To establish a person-centred view of radicalisation, it is helpful to consider the previous observation that self-perspective develops in an obscure *transitional* space.[150]between the person's internal (psychological) world and his/her broader social interactions; noting, furthermore, that these interactions are largely influenced by the person's ideological standpoint(s). This proposition is summarised by Schmid, who highlights the "ideological socialisation" of persons as they experience radicalisation.[151] Schmid maintains that in addition to its political dimensions, radicalisation may constitute the basis of a manipulative "recruitment campaign," or a 'conversion process' through which the individual's self-perspective transitions from an egocentric position to one of a collectivist nature.[152] Furthering this position, Moghaddam and Borum emphasise the interpersonal nature of a psychosocial process which unfolds sequentially in the transitional space between the individual and his/her social world.[153] Highlighting limitations in the radicalisation discourse, Miller and Chauhan assert radicalisation involves myriad interpersonal factors and may affect the individual in ways he/she does not consciously recognise[154].

[147] O. Lynch, "Understanding radicalization: Implications for criminal justice practitioners," *Irish Probation Journal* 14 (2017): 78-91; European Commission, *High-Level Commission Expert Group on Radicalisation (HLCEG-R).* (Luxembourg: European Union, 2018); N. Sterkenburg, *RAN Factbook. Far-right Extremism: A Practical Introduction* (Amsterdam: RAN Centre of Excellence, 2019).

[148] Schmid, "Research on radicalization"; Silke & Brown, "Radicalisation: The transformation of modern understanding".

[149] HM Government, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*. (London: Her Majesty's Stationery Office, 2018).

[150] Winnicott, "Transitional objects and transitional phenomena."

[151] Schmid, "Research on radicalization," p. 27.

[152] ibid.

[153] Moghaddam, "The staircase to terrorism"; R. Borum, "Radicalisation into violent extremism II: A review of conceptual models and empirical research," *Journal of Strategic Security* 4, 4 (2011): pp. 37–62.

[154] Miller & Chauhan, "Radical beliefs and violent behavior."

Given the extensive debate regarding the profiles and motivational drivers of radicalisation, Veldhuis and Staun; González et al., and Ingram and Groppi critique the strategic or rational choice paradigm.[155] The choice is considered *rational* if the individual has selected the most suitable course of action based on his/her preferences and beliefs.[156] Groppi insists rational choice was less predictive of Islamist radicalisation in an Italian context than a desire to punish wrongdoing or pursue ideological commitment to Islamist governance.[157] Similarly, Veldhuis and Staun propose rational choice theory offers a partial explanation of radicalisation.[158] Reinforcing the need to distinguish radicalisation from terrorism, Veldhuis and Staun insist where terrorism constitutes a tool or instrument deliberately employed in pursuit of specific political goals, radicalisation remains a "(transforming) state of mind" encompassing a more general change in a person's thoughts and behaviours[159]. Building upon this position, Ingram insists IS's purposeful pairing of rational and identity-choice, through the Dabiq magazine, was integral to its extraordinarily successful recruitment strategy.[160] Comparably, González et al. explore a gendered position of rationality, by highlighting the need for women to be perceived as *agents* (not *victims*) of terrorist recruitment, suggesting they may participate in violence through a sense of socially reinforced empowerment.[161]

Ensuring the individual remains central to the analytical framework, Horgan, Altier et al. and Horgan et al. affirm the person's radicalisation journey is most

[155] Veldhuis & Staun, *Islamic Radicalisation: A Root Cause Model*; A.L. González, J.D. Freilich & S.M. Chermak, "How women engage homegrown terrorism," *Feminist Criminology* 9, 4 (2014): pp. 344-366; H.J. Ingram, "An analysis of Islamic State's Dabiq magazine," *Australian Journal of Political Science* 51, 3 (2016): pp. 458-477; M. Groppi, "An empirical analysis of causes of Islamist radicalization: Italian case study," *Perspectives on Terrorism* 11, 1 (2017): pp. 68-76.

[156] D. Satz & J. Ferejohn, "Rational choice and social theory," *The Journal of Philosophy* 91, 2 (1994): p. 71.

[157] Groppi, "An empirical analysis of causes of Islamist radicalization".

[158] Veldhuis & Staun, *Islamic Radicalisation: A Root Cause Model*.

[159] ibid. p. 59.

[160] Ingram, "An analysis of Islamic State's Dabiq magazine".

[161] González, Freilich & Chermak, "How women engage homegrown terrorism", p. 348.

accurately interpreted via a series of interconnected stages.[162] Horgan identifies three as particularly salient: becoming involved, being involved, and disengaging[163]. Noting how a range of vulnerabilities or 'influences' underpin each stage, Horgan insists the individual's journey is gradual, psychosocial in nature and determined by elements of rational choice.[164] Horgan maintains efforts to interpret and manage the likelihood of a person engaging in terrorism must focus upon the process itself, whilst paying attention to the meaning and engagement he/she forms therein.[165]

A more complete understanding of the pursuit of individual meaning, the search for a secure sense of self and engagement with radical discourse may be achieved by considering the potential existential drivers of radicalisation. As discussed, existential concerns can have a marked impact on the person's ideological position, self-perspective, and sense of belonging.[166] According to Gøtzsche-Astrup pronounced psychological uncertainty and a lack of meaning contribute markedly to radicalisation processes,[167] Likewise, Kruglanski et al.; González et al., and Sparke insist an existential crisis increases the likelihood of a person electing martyrdom to attain feelings of ultimate control over his/her fate, whilst advancing the group cause.[168]

[162] Horgan, "From profiles to *pathways* and roots to *routes*; Horgan, *Walking Away from Terrorism*; M.B. Altier, C.N. Thoroughgood & J.G. Horgan, "Turning away from terrorism: Lessons from psychology, sociology, and criminology," *Journal of Peace Research* 51, 5 (2014); pp. 647-661; J.G. Horgan, M. Taylor, M. Bloom & C. Winter, "From cubs to lions: A six-stage model of child socialization into the Islamic State," *Studies in Conflict & Terrorism* 14, 7 (2017): pp. 645-664.

[163] Horgan, "From profiles to *pathways* and roots to *routes*.

[164] ibid. p. 85.

[165] ibid.

[166] Charney, "True psychology of the insider spy"; INSA, *Assessing the Mind of the Malicious Insider*.

[167] O. Gøtzsche-Astrup, "The time for causal designs: Review and evaluation of empirical support for mechanisms of political radicalization," *Aggression and Violent Behavior* 39 (2018): pp. 90-99.

[168] A.W. Kruglanski, X. Chen, M. Dechesne, S. Fishman & E. Orehek, "Fully committed: Suicide bombers' motivation and the quest for personal significance," *Political Psychology* 30, 3 (2009): pp. 331-357; González, Freilich & Chermak, "How women engage homegrown terrorism"; B. Sparke, "The religious vs. social radicalization debate: Current understandings and effects on policy," *Journal of Policing, Intelligence and Counter Terrorism* 14, 1 (2019): pp. 82-96.

It appears the drive for group belonging represents a potent motif, with Schmid; Silke and Brown; Jones, and Gøtzsche-Astrup suggesting camaraderie and group belonging increase the appeal of radical groups and help calcify attachment bonds.[169] Doosje and van Eerten maintain radical group belonging is particularly appealing for persons seeking identity, meaning/significance, justice and/or adventure/sensation.[170] The drive for group belonging is further emphasised by a sense of collective marginalisation or threat from an identifiable *other*. Commenting on various Muslim minority and immigrant communities in Europe, Sirseloudi and Coolsaet assert elevated levels of discrimination and rejection, alongside an inconsistent sense of cultural identity, leave the individual vulnerable to radical, potentially extremist, ideologies which are often formulated around a *good versus bad* dichotomous worldview.[171] Simultaneously, Kallis et al. and Sterkenburg highlight the desire for uniformity, collective identity, and comradeship - which is typically enhanced through a shared experience of violence - as central to the appeal of extremist European right-wing movements.[172]

The identity-related, collectivist parallels between Islamist and right-wing radicalisation are further evident in discussions around gender and the evolving influence of women in extremist groups. Although research into gender-sensitive

[169] K. Bhui, "Radicalisation and mental health," *Nordic Journal of Psychiatry* 72, S1 (2018): pp. S16-S19; Schmid, "Radicalisation, De-Radicalisation, Counter-Radicalisation"; Silke & Brown, "Radicalisation: The transformation of modern understanding"; E. Jones, "The reception of broadcast terrorism: Recruitment and radicalization," *International Review of Psychiatry* 29, 4 (2017): pp. 320-326; O. Gøtzsche-Astrup, "The time for causal designs".

[170] B. Doosje, & J.J. van Eerten, "Counter narrative' against violent extremism," in *'De-radicalization': Scientific insights for policy* ed. L. Colaert (Brussels: Flemish Peace Institute, 2017), p. 86.

[171] M. Sirseloudi, "The meaning of religion and identity for the violent radicalization of the Turkish diaspora in Germany," *Terrorism and Political Violence* 24, 5 (2012): pp. 807-824; Coolsaet, "Radicalization: The origins and limits of a contested concept".

[172] A. Kallis, S. Zeiger & B. Öztürk, "Executive summary and recommendations," in *Violent Radicalisation & Far-right Extremism in Europe* eds. A. Kallis, S. Zeiger, & B Öztürk (Ankara: SETA Publications, 2018), 13-17; Sterkenburg, *RAN Factbook.*

aspects of extremism is comparatively limited[173] (González et al.; CTED), Kelly asserts greater attention has been paid to the involvement of European women in Islamic extremism than extremist right-wing groups[174]. Referencing DAESH, CTED suggests the drivers of female radicalisation are infused with regional nuance, yet encompass economic, political, psychological, and personal grievances – especially human rights abuses and gendered violence. Likewise, Pearson and Winterbotham highlight belonging, empowerment and identity as central to DAESH recruitment narratives; thereby, suggesting women are drawn to extremist groups for similar reasons as men.[175] Despite these shared grievances, Cook and Vale report women represent a smaller percentage of DAESH recruits than men and whilst it is not possible to 'profile' female DAESH recruits, in many cases their rationale for joining was influenced by significant males.[176] Conversely, Stinton highlights the findings of Nair and Chong to challenge the perception that subservient women are passively recruited into DAESH by dominant males.[177] Stinton maintains female DAESH recruits often formulate their own (radical) interpretation of Islam.[178] Paralleling the conclusions of Cook and Vale,[179]

[173] González, Freilich & Chermak, "How women engage homegrown terrorism"; CTED, *Gender Dimensions of the Response to Returning Foreign Terrorist Fighters: Research Perspectives*. (New York, NY: UN Security Council, 2019).

[174] L. Kelly, *Overview of Research on Far Right Extremism in the Western Balkans. K4D Helpdesk Report* (Brighton, UK: Institute of Development Studies, 2019), https://assets.publishing.service.gov.uk/media/5d309f7aed915d2fe9ea6aec/620_Western_Balkans_far_Right.pdf

[175] E. Pearson & E. Winterbotham, "Women, gender and daesh radicalization: A milieu approach," *The RUSI Journal* 162, 3 (2017): pp. 60-72.

[176] J. Cook & G. Vale, *From Daesh to 'diaspora': Tracing the women and minors of Islamic State*. (London: ICSR, 2018).

[177] C. Stinton, "Combining the aberrant with the ordinary: The role of white supremacy in the far-right radicalization of women," *Journal of Applied Psychology and Social Science* 5, 1 (2019): pp. 86-115.

[178] ibid.

[179] Cook & Vale, *From Daesh to 'diaspora'*.

Stinton asserts these interpretations involve the endorsement of and, on occasion, direct participation in violence.[180]

Blee records variation in the backgrounds and motivational drivers of women involved in white supremacist organisations.[181] Moreover, Mattheis asserts far-right women are often deeply committed to their organisation's beliefs and practices and highly attuned to their identity.[182] Crucially, CTED emphasise the judicial implications of gendered perspectives of extremist vulnerability, observing males have been perceived as commanding greater individual agency and, therefore, received a more robust judicial response.[183] CTED insist women are routinely infantilised by judicial systems which fail to recognise the extent or complexity of their risks.[184]

The influence of personal agency, feelings of empowerment and notions of belonging upon female vulnerability to extremism demands consideration. Khan describes religious extremism as harmful to female agency and detrimental to a woman's capacity for free choice[185]. Contemporaneously, Bacchetta insists obtaining an accurate understanding of female agency in right-wing contexts is notoriously difficult.[186] Nevertheless, González et al. affirm females commonly display rationality and deliberateness in their decision to engage with terrorist networks.[187] González et al. assert rational thought is evident in women's pursuit of individual and collective

[180] Stinton, "Combining the aberrant with the ordinary".

[181] K. M. Blee, *Inside Organized Racism: Women in the Hate Movement*. (Los Angeles, CA: University of California Press, 2002).

[182] A.A Mattheis, "Shieldmaidens of whiteness: (Alt) maternalism and women recruiting for the far/alt-right," *Journal for Deradicalization Winter* 2018/19, 17 (2018): pp. 128-162.

[183] CTED, *Gender Dimensions of the Response to Returning Foreign Terrorist Fighters.*

[184] ibid.

[185] M.B. Khan, "How religious extremism compromises women's security, agency and mental health: Conversation with Sarah Eltantawi," *Agenda* 3 (2016): pp. 11-17.

[186] P. Bacchetta, "Hindu nationalist women imagine spatialities/imagine themselves: Reflections on gender-supplemental-agency," in *Right Wing Women: From Conservatives to Extremists Around the World* eds. P. Bacchetta & M. Power. (New York, NY: Routledge, 2002), 43-56.

[187] González, Freilich & Chermak, "How women engage homegrown terrorism".

empowerment, with many contemplating martyrdom as a means of (re)claiming their autonomy.[188] Unsurprisingly, the value of understanding gender-sensitive recruitment campaigns has not escaped the attention of groups such as DAESH.[189] CTED, and Pearson and Winterbotham stress that whilst attempting to capitalise upon a range of psychosocial issues in an intricate, highly nuanced manner, the DAESH approach to gendered recruitment relied upon generalisations that accentuated traditional power structures.[190] DAESH's female-centric rhetoric stresses the position that Muslim women are disempowered by Western worldviews; contemporaneously, DAESH's male-oriented recruitment dialogue promotes a view of the passive female to reinforce conventional masculinity paradigms. Notably, Pearson and Winterbotham, insist young people, young women in particular, who felt disinclined to the dominant perspectives and behaviours of their nations or social groups - and in certain cases estranged from the attitudes of their family members - were attracted by DAESH's promises of a land dedicated to religious piety and the solidarity of likeminded kinship.[191]

Although unquestionably relevant in certain cases, de Leede and CTED urge caution in the tendency to overemphasise clichéd recruitment tropes such as the pious journey and the 'Jihadi bride' phenomenon.[192] According to CTED, these perspectives risk devaluing the potency of women's grievances and female agencies in the recruitment process, thus producing deep fissures in the security response.[193] González

[188] ibid.

[189] Pearson & Winterbotham, "Women, gender and daesh radicalization"; S. de Leede, "Western women supporting IS/DAESH in Syria and Iraq – An exploration of their motivations," *International Annals of Criminology* 56, 1-2 (2018): 43–54; M. Loken & A. Zelenz "Explaining extremism: Western women in DAESH," *European Journal of International Security* 3, 1 (2018): 45-68; CTED, *Gender Dimensions of the Response to Returning Foreign Terrorist Fighters.*

[190] CTED, *Gender Dimensions of the Response to Returning Foreign Terrorist Fighters*; Pearson & Winterbotham, "Women, gender and daesh radicalization".

[191] ibid.

[192] de Leede, "Western women supporting IS/DAESH in Syria and Iraq; CTED, *Gender Dimensions of the Response to Returning Foreign Terrorist Fighters*; Pearson

[193] ibid.

et al. and Sterkenburg recognise intimate relationships and social networks are central to female recruitment.[194] Nevertheless, Sterkenburg acknowledges that whilst many women become affiliated with right-wing groups through their male partners, a considerable number approached them independently.[195] Equally, Pilkington observes women frequently established robust connections with the English Defence League without the influence of a male partner.[196] Despite attracting criticism from numerous quarters, commentators such as Eatwell and Leek suggest narratives of female self-determination amongst right-wing groups are not a recent phenomenon, pointing out themes of empowerment and the efficacy of certain women amongst 1930s Nazi rhetoric.[197] Recognising a paucity of data concerning women's motivation to join left-wing extremist or terrorist organisations, Koehler identifies four person-centred themes as significant: i. living authentically as a political warrior; ii. alignment with rebellion; iii. a sense of moral superiority, and iv. unethical judicial practices.[198]

Once recruited, women's roles in extremist groups are broad and diverse. Cook and Vale, insist women hold powerful symbolic and practical value for DAESH.[199] Moreover, it appears women have become increasingly active in right-wing extremist circles over the past thirty years. CTED; González et al., and Sterkenburg highlight the strategic capacity of female members.[200] They accentuate the essential contributions of female recruits to the rhetoric and philosophical agenda of their respective

[194] González, Freilich & Chermak, "How women engage homegrown terrorism"; Sterkenburg, *RAN Factbook.*

[195] ibid.

[196] H. Pilkington, *Loud and Proud: Passion and Politics in the English Defence League.* (Manchester: Manchester University Press, 2016).

[197] R. Eatwell, "Towards a new model of the rise of right-wing extremism," *German Politics* 6, 3 (1997):pp. 166-184; R. Leek, "Conservative empowerment and the gender of Nazism: Paradigms of power and complicity in German women's history," *Journal of Women's History* 12, 2 (2000): pp. 147-169.

[198] D. Koehler, "The fighting made me feel alive": Women's motivations for engaging in left-wing terrorism: A thematic analysis," *Terrorism and Political Violence* 35, 3 (2023): pp. 553-568.

[199] Cook & Vale, *From Daesh to 'diaspora.'"*

[200] CTED, *Gender Dimensions of the Response to Returning Foreign Terrorist Fighters;* González, Freilich & Chermak, "How women engage homegrown terrorism"; Sterkenburg, *RAN Factbook.*

organisations, acknowledging their pivotal role in safeguarding intra-group cohesion. Likewise, Stinton affirms women are especially active online, both in right-wing and Islamist extremist contexts.[201] Building on this position, Pearson and Winterbotham; Cook and Vale, and CTED report women occupy an array of roles within DAESH including recruiters, promoters, educators, facilitators and, to a lesser extent, direct perpetrators of violence.[202] Responding to the nuances of female involvement in extremist networks, González et al. invoke Agnew's (1992) General Strain Theory and highlight the emotional challenges women typically encounter through membership in a violent extremist group.[203] González et al. propose women are more likely to endure emotional strain and lowered mood as they contend with their original grievance, whilst simultaneously processing the unique stressors associated with their role(s) within the group.[204] Adopting a cautionary tone, González et al. assert women frequently channel negative, angry emotions inward, and are, therefore, at greater risk of engaging in personally destructive behaviours.[205] Further to the findings of Pearson and Winterbotham, González et al. contend women's experiences of "strained collectivity" (i.e., weak social ties with the dominant group), increase the appeal of homegrown terrorism [206].

Although frequently overlooked, the gender-sensitive dimensions of vulnerability to terrorism and violent extremism provide insight into the congested field of radicalisation analysis. Having outlined myriad layers of interpersonal complexity associated with the enumerable radicalisation pathways, it is essential to examine His Majesty's Government's contemporary response. HMG has been confronting terrorism, insurgency and conduct that is now categorised as "violent

[201] Stinton, "Combining the aberrant with the ordinary".

[202] Pearson & Winterbotham, "Women, gender and daesh radicalization"; Cook & Vale, *From Daesh to 'diaspora'"*; CTED, *Gender Dimensions of the Response to Returning Foreign Terrorist Fighters*;

[203] González, Freilich & Chermak, "How women engage homegrown terrorism".

[204] ibid.

[205] ibid.

[206] Pearson & Winterbotham, "Women, gender and daesh radicalization"; González, Freilich & Chermak, "How women engage homegrown terrorism", p. 348.

extremism," for centuries.[207] Knudsen describes the UK as a leading European contributor to counter-terrorism policies and practices.[208] Moreover, as a permanent member of the United Nations Security Council (UNSC), the UK is legally mandated to employ evidence-based risk assessment in the management of criminal or terrorist activities.[209]

HMG's contemporary evidence-based approach favours the analysis of radicalisation through the Prevent principle of the CONTEST Strategy.[210] Prevent draws upon three overarching dimensions: engagement (with a group, cause, or ideology), intent and capability (to cause harm), and to assess radicalisation risks[211]. These dimensions are operationalised in a variety of approaches, one of the more notable being the Extremism Risk Guidance 22+ (ERG 22+),[212] which explicitly assesses the risks and needs of persons convicted of an extremist offence.[213]

Although the ERG offers a credible response to the psychosocial challenges surrounding extremist offending, Lindekilde, and Knudsen affirm radicalisation assessment is in an early stage and remains fraught with difficulty.[214] Lynch suggests current restrictions are exacerbated by a limited ability to interpret the relationship

[207] D. French, *The British Way in Counter-Insurgency, 1945-1967.* (Oxon: Oxford University Press, 2011); C. Honeywood, "Britain's approach to balancing counter-terrorism laws with human rights," *Journal of Strategic Security* 9, 3 (2016): pp. 28-48.

[208] Knudsen, "Between vulnerability and risk?"; R.A. Knudsen, "Measuring radicalization: Risk assessment conceptualisations and practice in England and Wales," *Behavioral Sciences of Terrorism and Political Aggression* 12, 1 (2020b): pp. 37-54.

[209] UNSC, *Resolution 2396 (2017)* (2017), https://undocs.org/en/S/RES/2396(2017).

[210] HM Government, *CONTEST.*

[211] HM Government, *Channel: Vulnerability Assessment Framework.* (London: Home Office, 2012).

[212] Hereafter referred to as the ERG.

[213] M. Lloyd, *Extremism Risk Assessment: A Directory.* (UK: CREST, 2019).

[214] Lloyd, *Extremism Risk Assessment*; B. Powis, K. Randhawa-Horne & D. Bishopp, *The Structural Properties of the Extremism Risk Guidelines (ERG22+): A Structured Formulation Tool for Extremist Offenders.* (London. Ministry of Justice, 2019); L. Lindekilde, "Introduction: Assessing the effectiveness of counter-radicalization policies in northwestern Europe," *Critical Studies on Terrorism* 5, 3 (2012) pp. 335-344; Knudsen, "Measuring radicalization".

between dangerousness and ideology, as well as the low base rates for the most serious radicalisation outcomes.[215] Described as a Structured Professional Judgment (SPJ) tool that "… analyses the personal and contextual factors and circumstances that contributed to an individual's engagement in an extremist group, cause and/or ideology, and offending," [216] Powis et al., and Lloyd and Dean emphasise the ERG's contribution to the management of extremism.[217]

The ambiguity surrounding radicalisation and notions of individual vulnerability has remained a core feature of ERG discussions. When designing the ERG, Lloyd and Dean purposefully omitted the term "radicalisation."[218] Given its evidence-based approach, Herzog-Evans insists the ERG is not intended to quantify potential vulnerability to extremism[219]. Conversely, Knudsen affirms the ERG is principally concerned with identifying persons at risk of radicalisation.[220] Likewise, van der Heide et al. maintain the ERG structure helps illuminate those psychological features which are instrumental in determining radicalisation pathways.[221] Having been employed by Her Majesty's Prison and Probation Service since 2011,[222] it may be argued that by focusing on the potential psychosocial pathways to extremist offending, the ERG offers valuable perspectives on the more serious implications of radicalisation.

As its full title suggests, the ERG 22+ examines twenty-two factors which align with the three dimensions outlined in the Prevent strategy's Channel program:

[215] Lynch, "Understanding radicalization".

[216] Powis, Randhawa-Horne & Bishopp, *The Structural Properties of the Extremism Risk Guidelines, p. p. 5.*

[217] ibid.; Lloyd & Dean, "The development of structured guidelines for assessing risk in extremist offenders".

[218] ibid.

[219] M. Herzog-Evans, "A comparison of two structured professional judgment tools for violent extremism and their relevance in the French context," *European Journal of Probation* 10, 1 (2018): p. 13.

[220] Knudsen, "Measuring radicalization".

[221] L. van der Heide, M. van der Zwan & M. van Leyenhorst, *The Practitioner's Guide to the Galaxy - A Comparison of Risk Assessment Tools for Violent Extremism.* (The Hague: ICCT, 2019): p. 8.

[222] S. Webster, J. Kerr & C. Tompkins, *A Process Evaluation of the Structured Risk Guidance for Extremist Offenders*. (London: OGL. 2017); Powis, Randhawa-Horne & Bishopp, *The Structural Properties of the Extremism Risk Guidelines.*

engagement, intent, and capability (see Figure 4).[223] Lloyd cautions the ERG is dependent upon the assessor's application of SPJ [224]. Defined as "… the professional appraisal of the risk factors ,"[225] SPJ enables the assessor to develop a holistic picture of the individual by acting as a scaffold for key risk indicators.[226] Silke maintains the SPJ element of the ERG considers aspects of the individual's circumstances which may not be captured by the twenty-two factors, thereby accounting for the +.[227] Acknowledging the value of the ERG as a risk management tool that focuses upon identity-related matters concerning extremism; Herzog-Evans, clarifies the ERG does not provide a specific risk score, nor is it intended to determine precisely who will re-offend, or when an offence will occur.[228]

[223] J. Rushchenko, *Prison Management of Terrorism-Related Offenders: Is Separation Effective?* (London: The Henry Jackson Society, 2018): pp. 33-34.

[224] Lloyd, *Extremism Risk Assessment*.

[225] C. Logan, "Structured professional judgment: Applications to sexual offender risk assessment and management," in *Sexual Offending: Predisposing Antecedents, Assessments and Management* eds. A. Phenix & H.M. Hoberman (New York, NY: Springer, 2016),p. 572.

[226] Lloyd, *Extremism Risk Assessment*, p. 7.

[227] Silke, "Risk assessment of terrorist and extremist prisoners".

[228] Herzog-Evans, "A comparison of two structured professional judgment tools".

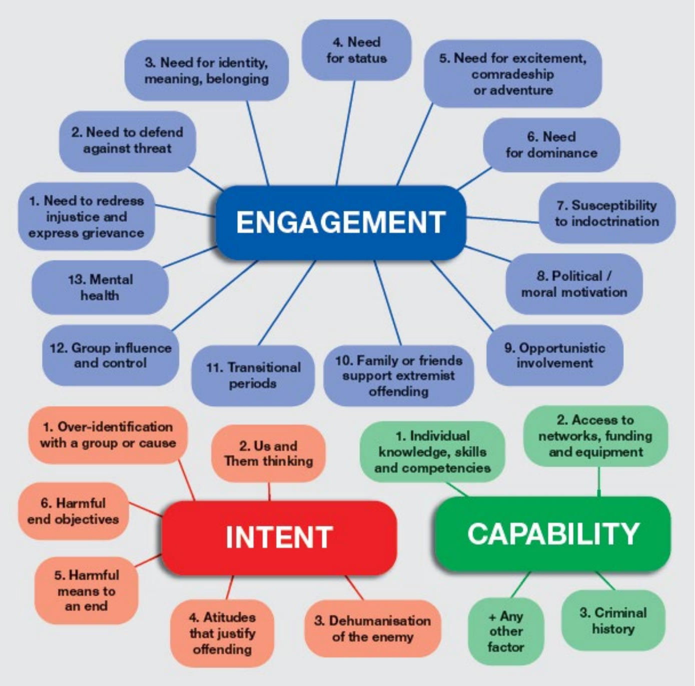
3. Need for identity, meaning, belonging
4. Need for status
5. Need for excitement, comradeship or adventure
2. Need to defend against threat
6. Need for dominance
1. Need to redress injustice and express grievance
ENGAGEMENT
7. Susceptibility to indoctrination
13. Mental health
8. Political / moral motivation
12. Group influence and control
11. Transitional periods
10. Family or friends support extremist offending
9. Opportunistic involvement
1. Over-identification with a group or cause
2. Us and Them thinking
1. Individual knowledge, skills and competencies
2. Access to networks, funding and equipment
6. Harmful end objectives
INTENT
CAPABILITY
5. Harmful means to an end
4. Atitudes that justify offending
3. Dehumanisation of the enemy
+ Any other factor
3. Criminal history

Figure 4 – dimensions and factors of the ERG 22.+[229]

Although the ERG is founded upon unpublished material[230] and research into its background and development is limited,[231] Powis et al. assert the ERG '… shows promise as a risk and need formulation tool for extremist offenders .'[232] Following a detailed statistical analysis of the twenty-two factors, Powis et al. highlight Identity and External Influence, Motivation and Ideology, Capability, Criminality, Status and Personal Influence as salient,[233] Nevertheless, Powis et al. report the ERG is yet to be validated against a non-Islamist extremist population, whilst also acknowledging

[229] Rushchenko "Prison Management of Terrorism-Related Offenders: Is Separation Effective?" *p.* 34.

[230] Lloyd & Dean "ERG 22+ Structured Professional Guidelines for Assessing Risk of Extremist Offending,"

[231] A. Scaracella, R. Page & V. Furtado, "Terrorism, radicalization, extremism, authoritarianism and fundamentalism: A systematic review of the quality and psychometric properties of assessments," *Plos One* 11, 12 (2016), doi.org/10.1371/journal.pone.0166947.

[232] Powis, Randhawa-Horne & Bishopp, *The Structural Properties of the Extremism Risk Guidelines (ERG22+)*, 1.

[233] ibid.

female extremists constituted a marginal subset of the cohort who may demonstrate differing needs from men. Powis et al. maintain further refinement is required in two dimensions: mental health and excitement, comradeship, or adventure.[234]

For Sarma, it is essential that practitioners remain cognisant of limitations in the individualised assessment of terrorism pathways, whilst remaining undeterred in the furtherance of best practice.[235] Thus, assessments of violent extremism and/or terrorism must align with and enhance those protocols and measures intended to counter their harmful effects. The equivocation surrounding radicalisation and the uncertainty regarding its potential outcomes, has contributed to poor practice by those organisations tasked with preventing violent extremism, thereby damaging cross-cultural relationships.[236] Consequently, Koehler and Fiebig stress the need for sustained coordination between the academic and applied approaches to countering violent extremism, particularly in training, professional development, and mentoring.[237] Despite layers of ambiguity, the radicalisation and IT literature identify the value of considering vulnerability and, in certain cases, the influence of discreet risk factors from the perspective of an individually nuanced psychosocial pathway. Therefore, an examination of those psychological threat domains which parallel IT and radicalisation may prove beneficial.

Parallel Threats: The IT-Radicalisation Crossover

Despite the increasing prevalence of IT and radicalisation and the apparent psychological crossover therein, research in these domains remains in a developmental

[234] Powis, Randhawa-Horne & Bishopp, *The Structural Properties of the Extremism Risk Guidelines (ERG22+)*,

[235] Sarma, "Risk assessment and the prevention of radicalization".

[236] D. Lowe, "Prevent strategies: The problems associated in defining Extremism: The case of the United Kingdom," *Studies in Conflict & Terrorism*, 40, 11 (2017): pp. 917-933; D. Parker, D. Chapot, J. Davis, "The Prevent Strategy's impact on social relations: A report on work in two local authorities," *Feminist Dissent* 4 (2019):pp. 160-193.

[237] D. Koehler & V. Fiebig, "Knowing what to do: Academic and practitioner understanding of how to counter violent radicalization," *Perspectives on Terrorism* 13, 3 (2016): pp. 44-62.

stage[238]. Consequently, the penultimate section of this paper seeks to promote analytical developments in IT and radicalisation by discussing the psychosocial parallels in their respective pathways.

Charney, Axelrad et al.; Massberg et al.; Shaw and Sellers; Dupuis and Khadeer; INSA; Noonan; Brinksman et al., and Myers and Trent emphasise the need to examine an individual's psychological traits when considering his/her potential vulnerability to IT[239]. Likewise, Bryans et al., RCP, Feddes and Al-Attar reiterate the importance of interpreting person-specific psychological factors when analysing potential susceptibility to radicalisation.[240] Unlike conventional risk assessment frameworks, however, the risk of an individual engaging in violent extremism cannot be comprehensively determined through the aggregation of empirically validated criminogenic factors.[241] Moreover, it appears, that the analysis of psychopathology may be better suited to terrorist subgroups, such as lone actors.[242] Given the complex, dynamic states of being which define the human condition, an accurate evaluation of a

[238] Horgan, "From profiles to *pathways* and roots to *routes*"; Greitzer, Kangas, Noonan, Brown & Ferryman, "Psychosocial modelling of insider threat risk; Silke, "Risk assessment of terrorist and extremist prisoners"; Shaw & Sellers, "Application of the critical-path method to evaluate insider risks"; Al-Attar, *Extremism, Radicalisation & Mental Health,*; van der Heide, van der Zwan & van Leyenhorst, *The Practitioner's Guide to the Galaxy.*

[239] Charney, "True psychology of the insider spy"; Axelrad, Sticha, Brdiczka & Shen, "A Bayesian network model for predicting insider threats"; Massberg, Warren & Lang Beebe, "The Dark Side of the Insider"; Shaw & Sellers, "Application of the critical-path method to evaluate insider risks"; Dupuis & Khadeer, "Curiosity Killed the Organisation."; INSA, "Assessing the Mind of the Malicious Insider"; Noonan, *Spy the Lie;* Brinksman *et al., "Millennial Considerations on Insider Threat"*; Myers & Trent, "Operational psychology in insider threat".

[240] Bryans, Barzanò, & Meissner, *Handbook on the Management of Violent Extremist Prisoners*; RCP, *Counter-terrorism and Psychiatry*; A. R. Feddes, "Risk assessment in integral security policy" in *'De-radicalization': Scientific Insights for Policy* ed. L. Colaert (Brussels: Flemish Peace Institute, 2017), pp.47-62; Al-Attar, *Extremism, Radicalisation & Mental Health.*

[241] van der Heide, van der Zwan & van Leyenhorst, *The Practitioner's Guide to the Galaxy.*

[242] J.W. Coid, K. Bhui, D. MacManus, C. Kallis, P. Bebbington, & S. Ullrich, "Extremism, religion and psychiatric morbidity in a population-based sample of young men," *The British Journal of Psychiatry p.* 209, 6, (2016): pp. 491-497; RCP, *Counter-terrorism and Psychiatry*; . Feddes, "Risk assessment in integral security policy".

person's vulnerability to extremist ideologies necessitates a holistic evidence-based case formulation approach.[243]

According to Al-Attar, accurate case formulation delivers an evidence-based analysis of an individual's current mental state and the impact this may have on his/her vulnerability to extremism.[244] As such, case formulation is largely informed by the individual's subjective experiences and remains heavily influenced by his/her encounters with the social world.[245] It follows, that when considering vulnerability to extremist thinking, a nuanced, contextually sensitive approach that recognises the interaction between political inclinations, social context and psychological perspectives is required[246]. This view is echoed by leading radicalisation and IT scholars, who maintain a person's decision to engage in IT or align themselves with an extremist organisation originates from a range of motivational dimensions.[247] As such, it is essential to recognise the potential influence of these factors on the individual's sense of self.

Referencing ideological extremism, yet mirroring fundamental elements of Charney's discussion around the existential drivers of IT, Dean and Rifkind describe identity as a subjective experience that mediates between the demands of an individual's internal reality and the pressures of his/her external world.[248]. Outlining

[243] Al-Attar, *Extremism, Radicalisation & Mental Health.*

[244] ibid,

[245] N. Tarrier, "An introduction to case formulation and its challenges," in *Case Formulation in Cognitive Behaviour Therapy: The Treatment of Challenging and Complex Cases* ed. N. Tarrier (Hove: Routledge, 2006): 1-11; Al-Attar, *Extremism, Radicalisation & Mental Health.*

[246]Coolsaet, "Radicalization: The origins and limits of a contested concept." CTED, *Gender Dimensions of the Response to Returning Foreign Terrorist Fighters*.

[247] Charney, "True psychology of the insider spy"; Silke, "Risk assessment of terrorist and extremist prisoners"; Shaw & Sellers, "Application of the critical-path method to evaluate insider risks"; BaMaung, McIlhatton, MacDonald & Beattie, "The enemy within?"; Noonan, *Spy the Lie.*

[248] Charney, "True psychology of the insider spy"; C. Dean, "The Healthy Identity Intervention: The UK's development of psychologically informed intervention to address extremist offending" in *Prisons, Terrorism and Extremism: Critical Issues in Management, Radicalisation and Reform* ed. A. Silke (New York, NY: Routledge, 2014): pp. 89-107; Rifkind, *The Psychology of Political Extremism.*

potential criminogenic implications therein, Dean asserts an impoverished sense of self-worth, a wish to be regarded as special and/or a dichotomous "us versus them" mindset frequently underpins the emotional drivers behind group-based offending.[249] This view is shared by numerous scholars. Ahmad draws on the experiences of Afghan suicide bombers to suggest the desire for a 'sense of purpose and a need to belong' increased the appeal of the extremist ideologies which underpinned their rationale[250]. Similarly, Schmid and Harpviken acknowledge an existential crisis linked to feelings of isolation and meaninglessness is likely to intensify the lure of *significance quests* - such as those offered by extremist groups.[251] In explanation, Rifkind contends the certainty of the extremist position offers a form of redemption which dissolves the insincerities, falsehoods, and contradictions of everyday life.[252] Incorporating the views of Junger, Rifkind maintains that, for some, a dichotomous mindset and the catharsis of a group bond escalate to a point where they would rather sacrifice themselves for the collective than exist in isolation.[253]

Examining psychological engagement with extremist groups, Dean makes two pertinent observations: firstly, engagement with a group's activities does not necessarily require the individual to identify with it on an intrinsic level; secondly, the intensity of a person's engagement is likely to evolve over time.[254] Speaking from a criminological perspective, Dean maintains an individual's involvement with organised criminal activity can be motivated primarily by social bonds and remain largely detached from the group's political or ideological motive(s).[255] Likewise, Horgan insists the nature or

[249] Dean, "The Healthy Identity Intervention," p. 96.

[250] Ahmad, *Dress Like Allies, Kill Like Enemies*, p. 19.

[251] Schmid, "Radicalisation, De-Radicalisation, Counter-Radicalisation," Harpviken, "Psychological vulnerabilities and extremism among Western youth: A literature review," *Adolescent Research Review* 5, 1 (2020): 1pp. -26; A. W. Kruglanski, M. J. Gelfand, J. J. Bélanger, A. Sheveland, M. Hetiarachchi & R. Gunaratna, "The psychology of radicalization and deradicalization: How significance quest impacts violent extremism," *Political Psychology* 35, S1 (2014): pp. 69–93.

[252] Rifkind, *The Psychology of Political Extremism.*

[253] Junger, 2011, as cited in Rifkind, *The Psychology of Political Extremism*, p. 56.

[254] Dean, "The Healthy Identity Intervention."

[255] ibid.

extent of the individual’s engagement reveals important clues into a series of underlying psychosocial processes concerning self-perspective, belonging and group involvement.[256] Accordingly, Lloyd and Dean, and Herzog-Evans, insist extremist risk assessment must acknowledge that an individual may engage with a group, but have little or no intent and/or capability to cause harm.[257]

Given the intricate psychosocial processes which unite both vulnerabilities to radicalisation and IT, the nature of the individual’s ideological engagement represents an essential area for consideration. In both contexts, he/she is likely to be motivated by a range of psychosocial factors that unfold over a sustained, though undefined period. González et al. Pearson and Winterbotham and CTED observe how deep-seated beliefs of estrangement from family and social networks help facilitate radicalisation.[258] A comparable position is evident in Philby’s self-reported absence of belonging as central to his betrayal. In Philby’s case, it appears deep-seated ideological devotion to an overarching cause had a prominent effect on his willingness to deceive. Likewise, his capacity to continue doing so was maintained by his ever-deepening commitment. For other malicious insiders, the pathway through deception is less concerned with matters of belonging or ideological allegiance and more closely aligned with the immediate gratification of self-serving factors, such as the pursuit of material comforts or feelings of satisfaction.

Although the relative depth of the person’s ideological commitment attracts considerable discussion from radicalisation commentators, it receives markedly less attention in the IT domain. The limitations of case study analysis notwithstanding, the Philby situation reveals the intricate deception and extensive harms of a capable, highly motivated outwardly confident individual who, upon closer examination, seemed embroiled in ideologically rooted existential conflict. Philby appeared to occupy a

[256] Horgan, “From profiles to *pathways* and roots to *routes*.”
[257] Lloyd & Dean, “The development of structured guidelines for assessing risk in extremist offenders,” Herzog-Evans, “A comparison of two structured professional judgment tools.”
[258] González, Freilich & Chermak, “How women engage homegrown terrorism”; Pearson & Winterbotham, “Women, gender and daesh radicalization”; CTED, *Gender Dimensions of the Response to Returning Foreign Terrorist Fighters*.

discordant position between the decadence and personal advantage of his "old-boys' lifestyle and the collectivist ideals of the Soviet cause. Philby's assertion that when the proposition of joining the Soviet intelligence service was made 'I did not hesitate. One does not look twice at an offer of enrolment in an elite force,"[259] alongside the numerous reports of his desire for personal comforts.[260]and self-confessed conflict between personal and political allegiance,[261] suggest Philby occupied a uniquely incongruent dualistic position: the upper-class elitist striving for greater personal acclaim and material benefits, viz-a-viz the communist idealist committed to the empowerment of an exploited proletariat. Tellingly, Yuri Modin.[262]professed Philby "never revealed his true self" to anyone (emphasis added).[263] Modin's remarks raise the question of whether Philby was himself cognisant of his true self; or whether - as Laing might suggest - his self-perception was so acutely obscured by ontological insecurity as to confound the balanced integration necessary for authentic self-awareness.[264]

As discussed, susceptibility to malicious insider activity has been assessed largely through a reductionist paradigm that overemphasises individual vulnerability.[265] Paralleling the observations of Brinksman et al.; Burkett and Wilder insist a nuanced empirically grounded approach that is attuned to those specific threats and opportunities created by the increasing complexities of the time is needed.[266] Drawing on Cialdini's six influence factors,[267] Burkett highlights the importance of recognising patterns in social relationships, in particular, the tendency to pursue

[259] Philby, *My Silent War*, xxxii.

[260] Macintyre, *A Spy Among Friends*.

[261] T. Milne *Kim Philby: A Story of Friendship and Betrayal* (London: Biteback Publishing, 2015).

[262] KGB Handler of the Cambridge Five.

[263] Modin, n.d., as cited in Philby, *My Silent War*.

[264] R. D. Laing *The Divided Self: An Existential Study in Sanity and Madness with an Introduction by Anthony David.*, (London: Penguin Books, 1969/2010).

[265] Burkett, "An alternative Framework for Agent Recruitment"; Vashisth & Kumar, "Corporate espionage"; Kennedy "Management and mitigation of insider threats."

[266] .Brinksman, Christian, Johnston *et al.*, *Millennial Considerations on Insider Threat:* Burkett, "An alternative Framework for Agent Recruitment"; Wilder, "Why spy now?"

[267] Reciprocation, Authority, Scarcity, Commitment (and Consistency), Liking, and Social Proof (Cialdini, 1984, as cited in Burkett, "An alternative Framework for Agent Recruitment," p. 7.

shortcuts or 'fixed action patterns' to limit the cognitive stressors of an overstimulated mind, alongside the desire to establish harmonious collaborative relationships.[268] Paralleling the approach employed by individuals seeking to radicalise, Burkett affirms the skilled case officer may capitalise upon the six influence factors to build the level of trust required in swaying the individual into malicious internal action,[269] Burkett cautions that failure to appreciate the challenges and demands of modern society is highly likely to result in an inaccurate interpretation of IT vulnerability and limit the efficacy of an organisation's countermeasures.[270]

Shortcomings may also arise from a bias towards the traditional view that IT and radicalisation are largely male concerns and ostensibly driven by individual weakness. Acknowledging psychological stressors appear fundamental to critical IT pathways, Burkett advocates a comprehensive analytical position.[271] Likewise, gender-sensitive radicalisation research highlights the vigorous commitment and proactive mindset of many female recruits.

Although conceptual parallels can be drawn between the application of Cialdini's six influence factors in an IT context and the recruitment of vulnerable persons in radicalisation processes, research into this proposition is in markedly short supply. Despite this limitation, a notable area of convergence between IT and radicalisation has been found within the cyber domain. There is a wealth of literature discussing the online recruitment of individuals into extremist groups. For example, scholars highlight the importance of global reach, the relative ease of facilitating discussions and the strategic use of messaging to build social networks and shift social norms (to an acceptance of more extreme perspectives) as common themes.[272] Likewise,

[268] Burkett, "An alternative Framework for Agent Recruitment," p. 13.

[269] Burkett, "An alternative Framework for Agent Recruitment."

[270] ibid.

[271] ibid.

[272] J. Cole, "Radicalisation in virtual worlds: Second Life through the eyes of an avatar," *Journal of Policing, Intelligence and Counter Terrorism* 7, 1 (2012): 66-79; T. Reynolds, "Ethical and legal issues surrounding academic research into online radicalization: A UK experience, " *Critical Studies on Terrorism* 5, 3, (2012): 499-513; M. Caiani & L. Parenti, *European and American Extreme Right Groups and the Internet.*

Wilder, Alexander, Verizon and NCSC, underscore the importance of considering the cyber domain in an IT context, particularly in relation to the leaking of sensitive materials.[273] Wilder maintains that whilst substantial advances in online technology have improved the ease of day-to-day communication, they have both intensified existing security challenges and created myriad new opportunities for malicious activity.[274] Acknowledging developments in the cyber domain enable an individual's pre-existing psychosocial vulnerabilities, Wilder suggests those who are heavily dependent upon the internet to satisfy their "positive qualities" (including a desire for social relationships, intimacy, creativity, and a will to belong) and "negative qualities" (including a desire for power, control, and manipulation), are particularly susceptible to malicious insider activity.[275] Crucially, BaMaung et al. highlights the cyber domain as a prominent point of convergence between IT and terrorism, insisting nation-states and their affiliates are exploiting its vulnerabilities to conduct espionage with increasing regularity.[276] BaMaung et al. maintain the cyber domain is invaluable in turning a loyal employee, whilst also representing a potent means of conducting indirect attacks.[277] In response to the growing threat associated with IT, radicalisation, and *cyberterrorism*, BaMaung et al. call for an integrated security paradigm that aligns the human with the physical and cyber dimensions to establish effective countermeasures.[278]

(Oxon: Routledge, 2013); R. Torok, "Developing an explanatory model for the process of online radicalization and terrorism," *Security Informatics* 2, 6 (2013): DOI: https://doi.org/10.1186/2190-8532-2-6; G. Weimann, "The emerging role of social media in the recruitment of foreign fighters," in *Foreign Fighters under International Law and Beyond* eds. A. de Guttry A, F. Capone F & C. Paulussen (T.M.C. Asser Press: The Hague, 2016), 77-96; Pearson & Winterbotham, "Women, gender and daesh radicalization"; Alexander, "Protect, detect and correct methodology to mitigate incidents"; Verizon, *DBIR 2023 Data Breach Investigations Report;* National Counterintelligence and Security Center (NCSC) *Strategic Plan: 2018-2020.*

[273] Wilder, "Why spy now?"; Alexander, "Protect, detect and correct methodology to mitigate incidents"; Verizon, *DBIR 2023 Data Breach Investigations Report;* NCSC *Strategic Plan.*

[274] ibid.

[275] ibid. p. 2.

[276] BaMaung, McIlhatton, MacDonald & Beattie, "The enemy within?"

[277] ibid.

[278] ibid., p. 133.

Discussion

As notions of identity and the social connections that drive it become ever more complex, the inevitable interpersonal challenges these circumstances inspire are likely to be reflected in those psychosocial pathways that lead to IT and radicalisation. Whether established through a long-term deceptive presence (as evident in the conduct of Philby or Ortis), or a single high-impact event (such as demonstrated by Lubitz, or in Hasan's and al-Shamrani's blue/green on blue shootings), the psychosocial antecedents of IT must be critically examined. It would be erroneous to suggest direct parallels in the motivational states of persons who engage in IT or experience radicalisation, or to transpose IT vulnerability directly into the context of radicalisation. However, identifying and studying consistencies between the two domains will support practitioners in managing both IT and radicalisation today and into the evolving ambiguity of tomorrow's hyperconnected world.

IT and radicalisation are collective terms that elude matter-of-fact categorisation. Both reflect extensive cultural nuance and have come to symbolise interpersonal pathways which encompass a range of actions - some expressly hostile, others more benign, but all underpinned by layers of deception and born out of an amalgam of ideological perspective, psychosocial motives, and desired end states. This paper has attempted to identify the personal and professional circumstances which precipitate intentional malicious insider activity. Contemporaneously, it has adopted a dimensional perspective of radicalisation that perceives harm in relative terms. The radicalisation discussion explores the impact of nuanced interpersonal factors upon the individual's sense of self and interprets his/her desire for identity and belonging as a means of analysing and managing risk. Whilst these factors are instrumental in determining radicalisation processes, further research into the structure and influence of personal ideological interpretation is encouraged. When examined through a psychological lens, the convergence between individual vulnerability to malicious insider activity and radicalisation is palpable. The elucidation of psychological parallels between IT and radicalisation presents a unique opportunity to develop early identification and medium-long-term management strategies. It is hoped this perspective will advance the implementation of a broader preventative approach formulated upon awareness raising, evidence-based collaboration and the development of mutual trust.

Though hampered by potential misreporting, the increasing frequency and wide-reaching consequences of IT and radicalisation present opportunities for further investigation. There can be little doubt the psychological fabric of both is rooted in the interface between a person's internal state(s) of mind, those external conditions which affect his/her decision making and the influence of risk-elevating interpersonal pathways. For some, depth of ideological commitment is a prominent antecedent. Others are motivated by a preponderance of negative mood states, marked interpersonal difficulties and the lure of material benefits. While the precise degree of influence attributable to each factor will invariably differ; in the context of both IT and radicalisation, the individual's interpretive paradigm is underwritten by a sense of dissatisfaction and ideological dissonance - whether from the more restricted 'workplace community,' or the community per se. Once engaged in either process, the individual operates covertly within a host environment deemed antithetical to his/her pressing needs or desires and/or harmful to his/her ideological position.

The specific harms associated with IT and radicalisation are difficult to quantify. In the most serious cases (such as those involving large-scale or high-impact data breaches, the commission of violence and/or the loss of life), the effects are likely to resonate far beyond the immediate target. Thus, IT and radicalisation have the capacity to cast a noxious shadow of instability across the political, economic, physical, and psychological domains, thereby significantly impacting well-being at the individual and collective levels. Although a woeful truism, it is accurate to conclude that the severity of the harm incurred disproportionately outweighs the number of perpetrators.

The roots of IT and radicalisation vulnerability run deep. Thus, inattention to their ideological underpinnings is a grave concern and represents a notable limitation in an organisation's ability to identify and mitigate either circumstance to the greatest effect. Both the CMO and critical pathways models provide a structured framework to orientate an effective analytical approach to IT, whilst the Engagement, Intent and

Capability model emphasises psychosocial pathways into extremist offending. Despite their utility, these paradigms must not be regarded as definitive, actuarial risk assessment tools or frameworks for interpreting vulnerability. Rather, they are evidence-based complementary paradigms most effectively applied in conjunction with existing risk-related psychometrics to inform the management of harm. In an IT context, the CMO and critical pathways models are ideally placed to support the development of a nuanced individualised view of potential vulnerability. This approach may add value to discussions on the role of psychopathology in IT. Moreover, despite the identity-related foundation of the ERG, analytical discussions around radicalisation risk may be further nuanced through the continual re-examination of psychopathology. Although psychopathology remains a topic of debate in radicalisation research, commentary from an IT perspective is largely restricted to observations on stress and existential anxiety. Whilst these factors are of primary concern, a broadening of the psychopathology narrative represents an opportunity for additional IT research.

Given the harms associated with misguided or disproportionate responses to radicalisation and IT, early-stage enquiries are likely to be more effective when directed toward the identification of risk-related behaviours. Although a person-specific approach would be required, there is a risk of escalating both interpersonal and contextual risk factors if this is ill-timed. The development of effective responses to IT and radicalisation remains an area of interest for academics and practitioners alike. Thus, it is essential for organisations and communities to recognise the value of developing ideological commitment through individual empowerment. Authentic feelings of individual purpose and synergistic alignment with the broader collective are instrumental in mitigating the psychological and ideological uncertainties that underpin malicious IT activity and increase vulnerability to radicalisation. It follows that collaboration, unity, and a clear sense of belonging form the greatest safeguards against betrayal.

Acknowledgments

The authors wish to express their sincere gratitude to Dr Zainab Al-Attar for her insightful comments, and to Miss Kate Molan for her first-rate proofreading and editorial skills.