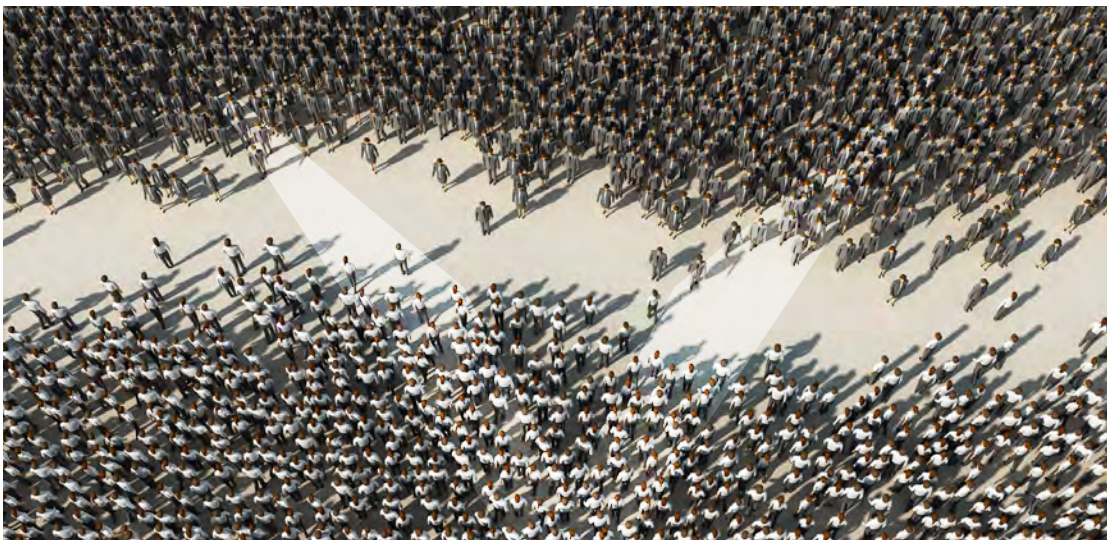
Countering Insider Threat in a Fractious Society – a View from Australia

Timothy V. Slattery

Insider threat is an ancient phenomenon. People who betray the trust of those around them have always existed as thieves, embezzlers, spies, saboteurs: the disgruntled. Also ancient is peoples' tendency to live and work in groups, evolving to operate as an ordered community – as a society. Within society, insider threat is written into Western cultural artefacts (for example, Judas' betrayal of Jesus) and is recorded across the canon of Western history. Insider threat is endemic to the human condition.[1]



Editor's note

The MIROR journal and its staff are staunch believers in personal dignity and the essential equality of people at the human level, regardless of any demographic affiliation. This article is written from a Western, Judeo-Christian perspective. The content does not denote nor connote the superiority of any set of values over another. It is the author's honest viewpoint, perspective and commentary offered here as a safe space for discussion and honest discourse that moves our community together toward a safer, more tolerant existence.

TIMOTHY V. SLATTERY

Tim Slattery served in Australia's army, intelligence and national security community for 37 years. Tim has operational and policy experience across defence, intelligence, law enforcement and protective security domains, including with Five Eyes partners. Tim retired from Australian federal government service in 2019, joining the consulting community in 2020 with focus on insider threat and broader personnel security issues across government, critical infrastructure and private sector clients. Tim co-founded of Pentagram Advisory Pty Ltd in 2024 to better focus his efforts to promote understanding and mitigation of insider threat.

Whilst the phenomenon is ancient, contemporary insider threat in Western societies is arguably more virulent and more consequential than ever before. Why? The flattening of societies resulting from omniscient technology correlates with a decay in the influence of traditional societal pillars in unifying the populace. The pillars of Western (European) society are generally taken to be: the *Judeo-Christian tradition, democracy* stemming from ancient Athens (5th century BC) linked to the Enlightenment (17th and 18th centuries), and *rationality* stemming from the time of Aristotle (4th century BC) and linked to the Renaissance (15th and 16th centuries) and Reformation (16th century) which enabled science. Decay, in this situation means a reduction in the potency of entrenched guiding principles for Western societies to influence (and unify) the populace. This reality, coupled with historically rapid and transformative technological advances, has promoted social fracture and large-scale 'othering'.[2] Societies are decreasingly coherent and hence less likely to offer people common purpose.

This reduction in coherence—or unity—contributes to fracture within our society and provides the space for insider threats to take root, to propagate, to succeed, and cause catastrophic damage.

> *Leaders and managers must proactively counter contemporary insider threat to secure the asset or capability for which they are responsible. Leaders are charged with this duty in the face of a workforce drawn from a fractious society which encourages focus on self rather than the goals of the enterprise, to the detriment of society.*

Historical Context

Recent times have represented a set of historically unparallelled changes in society, occurring at an ever-increasing pace driven by technology. Stimulated by the Cold War, the United States' military-industrial complex continued a peacetime version of the societal mobilisation ignited in World War II. The United Kingdom underwent a scaled-down version of the US military-industrial complex. The U.S. yoked the needs of national security to the national economy serving its society, for example civil nuclear electricity production coupled to nuclear-powered and nuclear-armed submarines. The collaboration between government, business, science and society shaped by war delivered victory, the engine for ongoing security and significant benefits for society. Australia has maintained little such military-industrial capacity.

Also, in the wake of World War II, societies became less conservative, less constrained by norms that existed in the first part of the 20th century (there were glimpses of this in the 1920s post World War I). Growing post-war economies promoted consumerism, public health and expanded programmes of secondary and tertiary education which, by the 1960s, stimulated popular interrogation of societal pillars by people in Western democracies including Australia, the U.S. and the UK. *Post-modernism* developed in the 1960s amongst the humanities departments of Western academe and evolved to be a movement questioning the 'traditional': Christianity, ideologies such as Marxism, social class, science, and the pillars of post-Enlightenment Western democracy.[3]

Challenges to 20th century's societal pillars have left them weakened, and even replaced in some cases. Long-held viewpoints of the efficacy of democratic government, probity of Christian faiths and institutions, the honesty of banks and big business, the credibility of leadership hold less sway over members of society. Popular disquiet over the costs and morality attributed to national security has led many to find government to be questionable and untrustworthy.

Pillar beliefs that once made society strong became discredited. Innovative capitalism gave way to the 'greed is good' 1980s, a phrase attributed to the U.S. stock trader Ivan Boesky who was jailed in the 1980s for insider trading, with the phrase also recited by the character Gordon Gekko in Oliver Stone's 1987 film Wall Street,

> **Contemporary insider threat in Western societies is arguably more virulent and more consequential than ever before.**

emphasised materialism and the centrality of the individual, and when coupled with the social and economic globalisation of the 1990s ultimately eroded many people's trust in those pillars. Western blue-collar jobs were offshored and with them national security-relevant capabilities (military, industrial, scientific, information technology) were diminished as the end-of-the-Cold-War 'peace dividend' was harvested.

With the dust still settling from the fall of the Berlin Wall in 1989, the introduction of public internet in 1993 democratised access to information which, when coupled to the advances in consumer electronics (for example, 21 iterations of Apple iPhones 2007-2023), became a seminal historical conjunction enabling and empowering the individual over the state as never before in human history. This unbridled information access enabled individuals to contend with and potentially overcome the nation state and its societal institutions. Financial shocks in the 2000s and the recent COVID pandemic further untethered Western societies from established pillars because people could now, by virtue of powerful technology including home computing, entertainment and personal portable electronic devices, modify elements of their reality by 'on-demand' consumption of news, entertainment and information aligned to their desires and curated beliefs. Empowering research through quick access to vast troves of information nesting on the internet became available to all. Individuals have access in their hand to capabilities, such as overhead imagery and geolocation, that were the exclusive purview of select nation states a few decades before. Over the last 60 years people became tooled, and predisposed, to be activistic in their personal and work lives – almost untethered from the established pillars of society on which their forebears had relied – with consequences for their political, social, criminal, and tribal activities.

> *Leaders and managers need to understand recent history (many in their workforce won't) – the 'how we arrived at the current situation' – to provide context for the decisions they need to make today about the secure operation of their enterprise. To identify risk stemming from insider threat the enterprises' unique operating environment—including historical context—must be appreciated.*[4]

Changes in Society

The powerful changes in society, coupled with the explosion of technology-fueled rapid and chaotic change in Western societies, spawned an ever-dividing (increasingly fractious) society: a form of social meiosis based on differences. A lexicon has evolved to encompass a range of social inequalities and identity politics. Such terms became shorthand social descriptors generally relating to racial or social injustice,

in time evolving to diffuse political movements whose adherents embrace and identify with as strongly as a religiously devout person might have embraced their faith during the Western Protestant Reformation of the 1500s. Such terms merged with Postmodernism to derive the term *Social Justice scholarship*[5] which is a feature of Western democratic societies today, especially prevalent in universities.

In recent years, researchers and authors have explored the foundations and evolution of the features and consequences of personal beliefs that align generally to critical race theory, post-colonialism, social justice and identity. Two such books, *The Madness of Crowds: Gender, Race and Identity* by Douglas Murray (2019) and T*he Coddling of the American Mind* by Greg Lukianoff and Jonathan Haidt (2018) explore the topic and offer some confronting conclusions. Whilst any analysis such as these can be decried, the fact is the sentiments explored in these books are prevalent in large swaths of Western democratic societies, influencing the behaviours of many people to be focused on their view and wellbeing – potentially seeing themselves as victims - to the exclusion of them seeing themselves as part of a broader society.

Recognising the state of societal flux at the beginning of 2024 – war in the Middle East and Europe, nation-state competition including the threat of nuclear war, the tenets of globalisation and free market erosion, the challenging politics and economics of climate change, economic and personal financial stress – there is a need for people to act in concert for preservation. The reality is that people, as individuals, are historically empowered and more critical (and commensurately more vulnerable to misinformation), less tethered to societal pillars, more focused on their individual self and related discrete identity grouping rather than participating constructively in broader society of which they have diminished trust. How can we maintain the efficacy and effectiveness of society in the face of ever-increasing demands by individuals and tribes resulting in diminishing cohesion? How can we protect the effective operation of government and business for the benefit of the societies they serve?

Amongst the consequences of these changes in characterization of society, of change in societal mores,[6] are many individuals' diminished trust and loyalty in the institutions and leaders that have historically guided societies.

> *How far should leaders and managers be prepared to go, how accommodating should they be, to give comfort to changes in society, which promote asserted individual rights, at the potential expense of performance and security of their enterprise? In being so accommodating are they enabling insider threat in the enterprise?*

> [The] reduction in social coherence—or unity—contributes to fracture within our society and provides the space for insider threats to take root, to propagate, to succeed, and cause catastrophic damage.

Trust

A key element of the changes in society is the concept of trust.[7] In discussing insider threat, it is those who have legitimate access to an enterprise's assets and operations who are most relevant. Our current environment is comprised of people with diminished trust in the pillars of society. In the context of their lives, the 'who' and 'what' sources of information they trust are less predictable than in the past. There is a trend to refer to one's *lived experience*[8] of how these pillars have impacted one's life, rather than people holding a broader view of themselves as part of a society willing to rely on consuming and trusting information that others provide. This view repudiates empirical fact in favour of 'fact' being shaped by one's experience and perception – everyone is empowered to create their own 'facts'. The pillars they might have trusted to guide their thinking and inform their position are weakened or redundant leading to a deficit of trust in significant proportions of Western societies, and hence in our workplaces.

The *2023 Edelman Trust Barometer,* in its 23rd year of production, surveyed more than 32,000 people in 28 countries[9] in the period 1 – 28 November 2022. The theme for its 2023 report is *Navigating a Polarised World*, and in its Australia-focused analysis cites 'four forces that have Australia on the path to polarisation', those forces being:

- **Economic Anxieties –** Economic optimism is collapsing around the world, with 24 of 28 countries seeing all-time lows in the number of people who think their families will be better off in five years.
- **Institutional Imbalance –** Business is now the sole institution seen as competent and ethical; government is viewed as unethical and incompetent. Business is under pressure to step into the void left by government.
- **Mass-Class Divide –** People in the top quartile of income live in a different trust reality than those in the bottom quartile, with 20+ point gaps in Thailand, the United States, and Saudi Arabia.
- **The Battle for Truth –** A shared media environment has given way to echo chambers, making it harder to collaboratively solve problems. Media is not trusted, with especially low trust in social media.

Key points from the report include:

- Trust Index (the average percentage trust in NGOs, business, government and media) in a comparison between 2022 and 2023 reports saw Australia decrease trust (second worst result) whereas the U.S. had the biggest increase in trust.
- All Australian governments are distrusted.
- In Australia, business remains the only institution seen as competent and ethical.
- The key workforce demographics of Gen Z (born 1997-2012) distrust government and media with neutral levels of trust in business and NGOs.
- Millennials (born 1981 to 1996) distrust government and media and have neutral trust in business and NGOs.
- Institutional leaders are distrusted, with co-workers the most trusted.

For the Australia, United Kingdom, United States (AUKUS) security partners, with respect to global distrust threatening to polarise societies, Australia is assessed as moderately polarised. By comparison, the UK is assessed of being in danger of severe polarisation and the U.S. is assessed as now being severely polarised.

In exploring Australia's social fabric, 61% of Australian respondents cited 'the lack of civility and mutual respect is the worst I have ever seen' and 54% said that 'the social fabric that once held this country together has grown too weak to serve as a foundation for unity and common purpose'.

The report offers ideas to correct course in an increasingly polarised world by:

- **Supporting your home base –** The data has been very clear in the need for business to prioritise those in their own backyard by directly addressing their anxieties and working to reassure. It will be important to listen to your workforce to effectively drive change that is meaningful and impactful to the workforce.
- **Collaborating with government –** The best results come when business and government work together, not independently. Look for opportunities to build consensus and collaborate on policies and standards to deliver results that encourage a more just, secure, and thriving society.
- **Empower Gen Z –** It will be critical to better understand Gen Z as they engage with and value things very differently to those before them. Gen Z is driving a generational shift in trust which will be critical to address on the pathway to change, to set a new tone for the future.
- **Courage to take a stand –** A grim economic view is both a driver and outcome of polarisation that fuels distrust. Have the courage to take a stand on key issues that unify and hold divisive forces accountable.

This report describes a deteriorating society, a trust deficit, and indicates that people are looking for sources of trust – polarisation is not inevitable and may be reversible. People are more likely to trust business rather than government.

The challenge is to reconcile people's general lack of trust in the pillars of society, and their consequential move away from those in favour of a myriad of other societal groupings, and the opportunity for leaders and managers to capitalise on the workforce's willingness, even need, to trust the enterprise they are employed in.,

Turning to research[10] about trust, a long-term study investigating people's neurological responses to 'trust' concluded that building a culture of trust is what makes a meaningful difference to individuals relationship with work and hence to the enterprise they are part of. The research indicates that people in 'high-trust' enterprises are more productive, have more energy at work, collaborate better with colleagues, and stay with their employers longer. This high trust environment meets their needs as a person. The study offers eight management behaviours that can foster employee trust. The study offers that leaders and managers are the fundamental enabler to grow trust: leaders must provide the conditions for success – clear direction and suitable resources – then allow people to get on with the task, supervised (coached) but not micromanaged. I contend that a person is less likely to become an insider threat to an enterprise which offers them a culture of trust within which they are emotionally rewarded and socially enriched.

> *There is an opportunity for enterprises, especially private sector, to meet a fundamental employee need though creating a workplace culture based on knowing and communicating what the enterprise does and the contribution it makes to society. Culture of this type is likely to engender trust – to meet peoples' need to trust – as they feel a sense of supportive belonging which their tribe or broader society does not satisfy.*

Loyalty

Dr Kris Veenstra has written[11] on the topic of loyalty, social identity and insider threat. Whilst the research focused on suitability for employment in a high security government agency in the United States or Australia, in the context of insider threat and using Edward Snowden[12] as the exemplar the findings are relevant to any enterprise.

> Dr Veenstra writes: *According to social identity principles, the social identity an individual holds (i.e., self-definition's derived from group memberships such as their employing agency) play a significant role in the way they see themselves and how they behave. When people think of themselves in terms of a social identity, particularly if it is one that is valued and important to them, their individual interests become entwined with those of the group. As a result, they are more inclined to conform to group norms and demonstrate loyalty. Furthermore, loyalty is an outcome of the identification process. The more strongly someone identifies with their employing agency, the more loyal they will be.*[13]

The topic of social identity appears to be relevant to the 2023 case of U.S. citizen Jack Teixeira, alleged responsible for leaking of a significant trove of U.S. intelligence material, which is a case of insider threat because Teixeira's employment with the U.S. Air National Guard afforded him access to classified information. Reports that Teixeira posted classified material on a website, on which he was well known under a pseudonym, to generate notoriety amongst website users is of particular interest in terms of where his loyalties rest. It seems his loyalty rested with himself and his virtual activities rather than with the institutions and people who had offered him trust and loyalty in the 'real world'.

Recent reporting[14] about Jack Teixeira noted that members of Teixeira's chain of command have been charged over his theft and posting of classified information. The official investigation identified at least four instances of Teixeira accessing intelligence for which he had no legitimate access with supervisors being aware but not reporting it. Similar lacklustre management and leadership was evident in the Edward Snowden case with his supervisors not acting on, nor reporting, aberrant insider threat behaviour.

> **"...the value of human-based mitigations – leadership, culture, communications, employee support – and the ability of leaders to understand the operating context are indispensable mitigations to meet insider threat, a human-based threat.**

Snowden and Teixeira are for me, based on published information, emblematic of the person who becomes an insider threat: they made a decision to reject the trust and loyalty extended to them by a group they have sought to be part of and had been accepted into. Further, Snowden and Teixeira showcase technology as both the enabler of their thefts and the means to satisfy their personal agenda by using technology to promulgate the information they stole.

In the 20th century, loyalty was rooted in nationalism bound to national security through pain of war and so was seemingly straightforward to discern – society's institutions provided social identity. Our understanding of loyalty has moved from analogue to digital – it's more complex now.

Peoples' connection points for their loyalty have eroded in the same way as societal pillars have. The internet opened vast frontiers for new types of social identity – of connection points for loyalty – to be created. This diffusion of loyalty points has rendered the concept of loyalty increasingly complex and more difficult to assess.

Needs of the Many and the Needs of the Few

In the 1982, Star Trek film The Wrath of Khan, Spock says "Logic clearly dictates that the needs of the many outweigh the needs of the few." To which Kirk answers, "Or the one." This dialogue, steeped in utilitarianism,[15] has remained with me through the years as I have seen changes in society, enabled by technology and postmodernist thinking, swing the pendulum from mid-20th century 'big society' – the many – to cross the equilibrium to favour smaller groupings – the few – and it seems some have pushed the pendulum even further – to the one. That said, Kirk's answer signals recognition of instances where a compassionate response by society, recognising that there are instances to prioritise resources for people in absolute need, such as those with a physical disability, are homeless or suffering a mental health condition. The 'many' can selectively support the 'few', or the 'one'.

People (employees and contractors) are generally an enterprise's greatest asset. People are needed to deliver the product or service which is the reason the enterprise exists, and work as a team to achieve this. People, therefore, can be the greatest risk to the enterprise because they are trusted by the leadership and, in return, leaders seek peoples' trust and anticipate their loyal behaviour.

> *Leaders and managers must deliberately balance the needs of the many, the few, and the one. This issue is particularly relevant to insider threat as we navigate the friction between maintaining security and purpose of the enterprise versus observing individual employee preferences, always respecting employee rights in law.*

Countering Insider Threat

There is an imperative for managers and leaders to understand their responsibilities and legal obligations with respect to the enterprise they oversee. Enterprise security (against both internal and external threats) for the purpose of protecting the many takes precedence over a seemingly ever-expanding effort to mollify insurgent employees and external interest groups – the few. Malicious actors will take advantage of vulnerabilities arising from employee behaviours and employer insouciance.

Protecting the many, rather than ferreting out the few, may be criticised by some mangers, employees, and unions as potentially increasing the risk of insider threat. However, the alternative to not responding to the evolving insider threat is to suffer the consequences of vulnerabilities being exploited, resulting in materiel damage to an enterprise as demonstrated by Teixeira and Snowden.

Dr Eric Lang, in his *Seven (Science-Based) Commandments for Understanding and Countering Insider Threats*,[16] writes: "Without effective management, such insider threats can undermine mission execution, employee safety, productivity, morale, financial stability, network functioning, asset integrity, public welfare, and local and global trust." Amongst Dr Lang's seven commandments are some I see of particular relevance to this discussion (my observations in *italics*):

- **Human factors are paramount.** *Effective leaders appreciate the threats to their people and create relevant controls that identify risk events and assist their people to operate securely thus promoting the wellbeing of both employees and the enterprise.*

- **Employees are an organization's greatest strength, especially for identifying insider threats.** *Enterprises already invest heavily in recruitment, retention and support for their workforces. We can invest greater resource in protecting the workforce we've recruited, retained, and supported.*
- **Initial personnel screening is critical but not sufficient.** *The granting of employment should not be the end of the vetting and screening process. People change throughout their employment cycle; an ongoing assessment as part of an enabling security framework that safeguards both the employee and the enterprise is necessary.*
- **Leadership and organizational culture at every level are key.** *Leaders and managers need to appreciate the value and significance of the asset they are responsible for and are duty-bound to protect it. In taking action to protect the asset they are also protecting the wellbeing of the workforce in terms of a safe working environment, supportive culture and, in extreme situations, the ongoing existence of the asset and hence employment of the people dependent on their decision making. Culture is king and must be demonstrated by leaders and managers.*

Countering Insider Threat in a Fractious Workforce

How might leaders and managers counter insider threat in a contested environment where employee trust and loyalty are difficult to identify and win, social norms are eschewed in favour of self or tribe, victimhood is celebrated as part of social justice expectations and the pressures of day-to-day life can convert a trusted employee into a trusted insider overnight?

Based on our client engagements and research I offer the following observations to help counter insider threat.

- Insider threat is a perennial source of harm and is endemic in the workforce.
- Insider threat is consequential, irrespective of the nature of the insider threat, be it careless, negligent, malicious or coerced.[17]
- Robust legal pre-employment screening is essential. The pre-employment process is the best opportunity to mitigate insider threat because of the potential thoroughness of the process and the opportunity to determine a candidate's 'fit' with the culture and values of the enterprise. Getting 'fit' right is more important than employment skills as these can be taught.[18]
- Surveys highlight the vast majority of insider threat events are careless or negligent. Accordingly, targeted security education and employee support is a key mitigation to the largest part of the risk posed by insider threat.

- Culture is king. Because insider threat is about people, as distinct from a cyber threat or natural hazard threat, a people-centric approach (albeit supported by information technology) is required. Create an enterprise culture people want to be part of, a culture that they will want to trust and be loyal to.
- Leadership and clear messaging of expected behaviours are fundamental inputs to culture and human resource activity as the spine of all insider threat mitigation. Leaders and mangers need to be confident and equipped to act humanely and legally to perceived aberrant behaviours for the benefit of the many as well as for the benefit of the few. But they must act.
- Leaders need courage to make contentious or unpopular decisions, informed by a risk assessment, in the face of dynamic social norms and workforce expectations in order to mitigate insider threat.
- People are subject to drivers, some beyond their control. They may rapidly change to become an insider threat through no fault of their own and so there must be measures in place enabling timely detection of relevant indicators. Workplace colleagues are a key to timely detection, in concert with technical security means.

> *Insider threat is an ancient phenomenon but is a virulent and damaging threat today. Leaders and managers must actively counter insider threat to securely operate the asset or capability they are responsible for. Technical solutions are available as a mitigation, and should be used, however the value of human-based mitigations – leadership, culture, communications, employee support – and the ability of leaders to understand the operating context are indispensable mitigations to meet insider threat, a human-based threat.*

DISCLAIMER

The information and views expressed in this presentation are solely those of the author and do not represent opinions and policies of the Department of Defense, U.S. Government, U.S. Special Operations Command, the Joint Special Operations University, or the institutions with which the author is affiliated.

REFERENCES

1. H. Arendt, *The Human Condition*, University of Chicago Press, 1958.
2. Cambridge Dictionary definition: the act of treating someone as though they are not part of a group and are different in some way, 2023
3. H. Pluckrose and J. Lindsay, *Cynical Theories*, Pitchstone Publishing, North Carolina, 2020, p16 .
4. Standards Australia, *Handbook 167:2006 Security risk management*, jointly published by Standards Australia, Sydney, and Standards New Zealand, Wellington.
5. H. Pluckrose and J. Lindsay, *Cynical Theories*, Pitchstone Publishing, North Carolina, 2020, p17.
6. Mores are the moral beliefs, customs, and ideals that define acceptable, expected behaviour within a society or social group. Mores (pronounced "more-rays") are preferred and socially sanctioned ways of behaving in any given society. These are stronger forms of norms, in which more fundamental habits of behaviour are involved.
7. American Psychological Association, *APA Dictionary of Psychology*, Trust defined as: reliance on or confidence in the dependability of someone or something. In interpersonal relationships, trust refers to the confidence that a person or group of people has in the reliability of another person or group; specifically, it is the degree to which each party feels that they can depend on the other party to do what they say they will do. The key factor is not the intrinsic honesty of the other people but their predictability. Trust is considered by most psychologists to be a primary component in mature relationships with others, whether intimate, social, or therapeutic.
8. D. Chandler and R. Munday, *Dictionary of Media and Communications*, Oxford University Press, 2020.
9. Argentina, Australia, Brazil, Canada, China, Colombia, France, Germany, India, Indonesia, Ireland, Italy, Japan, Kenya, Malaysia, Mexico, Nigeria, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Sweden, Thailand, The Netherlands, United Arab Emirates, United Kingdom, United States of America.
10. Paul J, Zak, *The Neuroscience of Trust: Management behaviours that foster employee engagement*, Harvard Business Review, January-February 2017 pages 84-90.
11. *K. Veenstra, Loyalty,* Social Identity and Insider Threat, for the Australian Criminal Intelligence Commission, November 2015
12. Edward Snowden was an American (now Russian) citizen who, whilst a contractor undertaking ICT-based tasking at the National Security Agency (NSA), stole millions of classified files which in 2013 he released either publicly or reportedly passed to Russia and China. Snowden accessed the classified files using the log on credentials of up to 25 NSA colleagues who gave their credentials to him. M. Hosenball and W. Strobel, Reuters 8 November 2013.
13. K. Veenstra, *Loyalty, Social Identity and Insider Threat*, for the Australian Criminal Intelligence Commission, November 2015, p5.
14. M. Myers, 15 *Air National Guardsmen disciplined in Discord server leak*, Military Times, 21 December 2023.
15. Utilitarianism promotes 'the greatest amount of good for the greatest number of people'.
16. Eric L. Lang, *Seven (Science-Based) Commandments for Understanding and Countering Insider Threats*, Counter-Insider Threat Research and Practice, Office of People Analytics, Personnel and Security Research Center (PERSEREC) 2022, page 1.
17. From the Institute for Critical Infrastructure Technology (2017), cited by Eric L. Lang, *Seven (Science-Based) Commandments for Understanding and Countering Insider Threats*, Counter-Insider Threat Research and Practice, Office of People Analytics, Personnel and Security Research Center (PERSEREC) 2022, page 2.
18. J. Kerr, *Legacy: What the All Blacks Can Teach Us About the Business of Life*, Constable, 2013.