

Deceiving the Deceived: Some Fundamentals for Deception and Detection

Associate Professor Robert Heath



Within the context in which deception happens there is the deceiver, the deceived, the environment surrounding them, and the channels or paths by which elements of deception are positioned for the sensory perception by the deceived. This is illustrated above where a combination of internal sources of credibility and validation such as beliefs, attitudes, and memories are elicited or shaped and external sources of credibility (from the perspective of the deceiver) and possible validity (from the perspective of the deceived) are used to shape judgement and actions by the deceived. This involves direct (DS) and indirect (IS) sources within the environment – and some false sources (FS).

Given the stream of mind and time illustrated above, deception has 3 stages: entry, ongoing, and exit. Most deception detection approaches focus on "ongoing" -- using such processes as internal audit and surveillance. *In most cases detection may fail should the deceptive activity have an existing non-detected history.* In short, "clearance" or validity may be assigned simply because the deceptive operation has not been detected. This is how Ponzi schemes succeed such as that conducted by Bernie Madoff.

Entry and exit stages may use different elements or sources to create and terminate a deception. *Entry and exit include introduced and removed sources.* Detect these appearances and disappearances and the trail and identity of the deceiver is much closer to hand. In most organisational situations, an indicator worth checking is expansion or contraction of "power" (signatory), "closed" (independent or sheltered operations) and "circulation" (confidential /secret/sensitive information management, cash flow entry; account management) activities take place. A basic element in this scrutiny becomes the opening or closing of circulation, power or access to files or accounts or raw data storage.

Six fundamental components of deception detection include the deceiver and the deceived, verbal and non-verbal indicators, credibility validation factors, and the use of environment to moderate and facilitate a deception. The environment moderation is briefly noted above and presented in the above illustration.

The Deceived. *While elements or sources that create a deception may be positioned by a deceiver, deception is a product of the cognitive processes within the deceived.* A combination of sensory perception and cognitive processing within the target or deceived develops and validates a deception. Beliefs, attitudes, and memories (BAM in the above diagram) can be used as a stimulus by the deceiver to emotionally and cognitively "validate" a deception within the target or deceived. As a common example, most media advertising uses beliefs and attitudes within the audience to create desire for the product being advertised.

Whether electronic, mechanical, or human-based, detection tools, systems and approaches can be used to enable as well as validate a deception. **To do so, the deceiver constructs tools and processes that deflect, nullify, or meet the non detection evaluation** of those detection tools or systems. *Really good deceivers look for system tolerances (that reduce false detection signals) and default "no anomaly" settings.* Organisations in particular need to consider the "cleared" data or environmental elements. *A detection hint here is to check at least a good sample of "perfect fits" for human-supplied forms and submissions as most humans submit forms, reports, applications, and reports with missing or inaccurate data – deceivers find this difficult to do.*

Well constructed deception often focuses on areas or environments or systems where the targets to be deceived think they are strong, protected, and watchful as these very beliefs can make people overconfident, less attentive, and less critical of presented data or sources. Moreover, the operating parameters and thresholds of screening and auditing-styled systems become generally known and are then more easily used to insert and validate the deception elements. Some current forensic computer programs that check data (and systems services such as emails) can also be blocked, deflected or absorbed simply by understanding the interrogation and/or sampling/refinement processes.

Human Non-Verbal and Verbal Cues and Clues. Starting from global basic clues/cues for detecting deception we a basic starter set of these can include:

- In face-to-face interactions across 118 countries most people claimed that liars look away to the left and downward (shutting out others). Research finds liars increase eye contact as if assessing the recipient's acceptance of the lie. Spontaneous lying, however, may do left and low shifts (or slow eye blinks).
- People across 118 countries believe that liars delay when responding with a lie (as the liar "manufactures the lie). Research finds that liars telling rehearsed lies respond too quickly. Spontaneous lying may show a response delay.
- Deceivers can emit a brief tight success smile with upper lip curl (superiority) on their belief a lie is accepted. A full upper lip lift can indicate disgust and thus a lie.
- A shoulder lift when responding when made at the beginning of the lie statement may indicate doubt over the a lie's success.
- Across cultures, when lies are spoken, natural hand gestures often cease. Temporary breakage may indicate a change in emphasis or actual statement.

- Deceivers can use word selections which they believe are true in order to appear more truthful and (in their “minds”) avoid actually lying. Example “Did you kill this person?” “I did not harm them.” Example: “Did you on any occasion take company money?” “I have never actually taken money that was not mine.”
- **In longer interactions and text (print or e-based), inconsistent or non-idiomatic** use can indicate deception. In fact broad plausible statements are often used to deflect or absorb probes for deceptive or missing information.

Credibility Validation Factors. Sources and items that give credibility to the presentation by the deceiver (or non-deceivers) are often used by the deceived as a means of validation. As an example, what appears to be a formal or official document (or email) that conforms to general expectations of the recipient often becomes perceived as being “valid”. The same processors are used for truth or lies, the real or the deceptive.

Superior deception strategies often focus on the content (reports, data) that will be delivered by a true (non-deceptive) direct or indirect source. Some source (person or information) regarded as being truthful and reporting what is believed to be truthful data/information “validates” deceptive information. Hence, positioning deceptive elements more than one step or operational element from the target to be deceived is usually quite successful. Part of the “weapons of mass destruction” evaluation is likely to have been exposed to this strategy and news media “leaks” and “sources” may also be successfully so used.

The Deceiver. *Everyone is deceptive about something at some time or place, so trying to identify or even profile all deceivers is impossible.* From espionage, security, fraud, and corruption perspectives, for example, obvious focal detection points include those who have access and/or position status for the above mentioned “circulation”, “power” and data management activities. Likewise, change in lifestyle behaviours is a common indicator whether these are positive (apparently more spending power) or negative (apparently spending less or “needing” more money). Having noted this, remember these are focal points for checking for inconsistency between behaviour (lifestyle change) and actual circumstance and not in themselves signals of actual guilt.

Some concluding duty of care and due diligence points include:

No single or set of cues necessarily indicates more than a need for further investigation.

Detecting a deception activity may not inform us of the motive or even the nature of the deception.

Brief CV of Associate Professor Robert Heath (Strategic Risk Management) PhD, BA(Hons) BA(Hons), BA, MAPS FBCI

Associate Professor Robert Heath is a psychologist who has consulted in management decision making, and strategic management and communication issues since 1982, in crisis management since 1986, in risk management since 1995, and in intelligence management (including counter deception, counter-terror, profiling action scenarios and people, and security) since 2001.

His doctorate researched how business decisions and decision maker confidence may be shaped and influenced by information.

At the University of Queensland, he developed the first undergraduate management course in Australia involving elements of crisis management and negotiation skills. In 1990, he provided expert evidence on crisis management issues for the New South Wales State Coronial Inquest into the Newcastle Earthquake of 1989. In 1993, La Trobe University (Melbourne, Australia) recruited Dr Heath to help develop and implement their MBA program.

Dr Heath was Managing Director of Crisis Corp (UK), 1994-2003. The majority of business clients were listed within the global 1000 companies. He also provided advice, consulting and training at local and national levels of government around the world... In May 27th 1999 Dr Heath gained the inaugural UK Business Continuity Personality of the Year, a national award that recognised his contribution to the business continuity industry, particularly in leading the industry into the 21st Century.

He is currently listed for his work in developing risk and crisis management theory and practice in the international editions of the Marquis *Who's Who in the World* (2003), *Who's Who in the Health Sciences* (2003), and *Who's Who in Science and Engineering* 2003, 2004, (6th & 7th Editions), 2007 and in various 2005 and 2006 editions. Currently, Dr Heath is Associate Professor in Risk and Strategy in the School of Management, the Division of Business, University of South Australia.

His book, *Crisis Management for Managers and Executives* (Financial Times/Pitman Books, 1998) provides a definitive introduction to crisis management for business, industrial and community organizations. The book is translated into Chinese, Russian, and Ukrainian and in 2004 in Greek (in line with preparations for the Olympic Games). Among many refereed and professional papers, Dr Heath has written a standard for the Business Continuity Institute on Crisis Communication and Public Relations and a chapter on the links between business continuity and crisis management for *The Definitive Handbook of Business Continuity Management* (John Wiley for Survive!, 1999). He is writing practitioner and theoretic text on all aspects of deception and counter-deception management, with specialist chapters on conducting investigations, interview management, deception (including fraud and corruption), security, and a mix of economic, political and military intelligence and deception practices.

Dr Heath is a Fellow of the Business Continuity Institute and a Member of the Australian Psychological Society. His experienced and expert advice and practice covers a diverse range of skills and capabilities -- from counter-terrorism,, profiling, and physical and psychological security practices, to risk evaluation, audits and management, to image, brand and media management, to problem and crisis management, to dealing with stress and post traumatic stress disorders, to negotiating in pressure-driven and in business settings, to intelligence and security management (including profiling, information evaluation, and deception/counter-deception management). He provides integrated services for all levels of government, corporations and businesses and offers predictive insights and advice on options and consequences for any situations.

Contacts:

Email: Robert.Heath@unisa.edu.au
Mobile: 0410632765
Phone: + [618] 8211 6667