Journal of Strategic Security

Volume 10 | Number 1 Article 6

From Tactical to Strategic Deception Detection: Application of Psychological Synthesis

Iain D. Reid
University of Malta, iain.reid@um.edu.mt

Lynsey F. Gozna
University of Leicester, lfg6@leicester.ac.uk

Julian C W Boon
University of Leicester, boo@le.ac.uk

pp. 81-101

Recommended Citation
Reid, Iain D.; Gozna, Lynsey F.; and Boon, Julian C W. "From Tactical to Strategic Deception Detection: Application of Psychological Synthesis." *Journal of Strategic Security* 10, no. 1 (2017) : 81-101.
DOI: http://doi.org/10.5038/1944-0472.10.1.1528
Available at: https://scholarcommons.usf.edu/jss/vol10/iss1/6

Introduction

Deception occurs across tactical and strategic environments presenting challenges within forensic and security domains. Tactical forms of deception are associated with individual acts and occur across multiple contexts, while strategic forms are part of larger operations targeting organizations and infrastructure.[1] Deception is proposed to comprise of simulation and dissimulation.[2] Simulation is considered to be showing false information to the target through mimicking, inventing, and decoying strategies.[3] Mimicking tactics seek to deceive the target through imitating reality, inventing tactics create something new, which is false, and decoying tactics deceive the target through diverting attention to another area.[4] Dissimulation means to deceive the target through hiding information by masking, repackaging, and dazzling tactics.[5] Masking aims to hide information by making it invisible to detection, repackaging hides reality through disguising and modifying appearance, and dazzling hides reality through presenting a range of options to blur reality in sense-making.[6]

In contrast to strategic and military deception, psychological approaches to deception have focused primarily on detecting deception in individuals rather than conducting deception operations against adversaries. Psychological theories of individual-level deception detection have focused either upon isolated cues to deception that are uncovered passively through examining behavior or more recent active interviewing approaches which aim to elicit cues to deception. Both passive and active approaches have targeted assessments of veracity towards individuals who may pose a threat across criminal and security related environments. These approaches may prove useful in detecting deception in individual cases; however, if individuals are part of a larger deception then additional challenges in uncovering deception will occur. Such challenges relate to deception conducted by a variety of actors covering both state and non-state groups, proxies and loosely aligned collectives. This article examines deception detection approaches across strategic environments, historical and current approaches to verbal, non-verbal, and online individual interactions. It advocates a focus towards how such approaches, combined with understanding the motives

[1] William Glenney, "Military deception in the information age: Scale matters," in Brooke Harrington (ed.), *Deception: From Ancient Empires to Internet Dating* (Stanford: Stanford University Press, 2009), 254-274.
[2] J. Bowyer Bell, "Toward a theory of deception," *International Journal of Intelligence and Counterintelligence* 16 (2003): 244,279; Whaley, Barton, "Toward a general theory of deception," *Journal of Strategic Studies* 5 (1982): 178-192.
[3] Whaley, "Toward a general theory of deception."
[4] Bell, "Toward a theory of deception"; Macdonald, Scot, *Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations* (London: Routledge, 2004); Whaley, "Toward a general theory of deception."
[5] Whaley, "Toward a general theory of deception."
[6] Bell, "Toward a theory of deception"; Macdonald, *Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations*; Whaley, "Toward a general theory of deception."

and context behind deception collectively may be deployed against strategic level deception. To illustrate how such approaches may combine, a scenario of a terrorist incident is presented with potential strategies to how deception in such a context may be detected.

Strategic Deception Detection

Strategic level deception is considered as deception that affects the critical infrastructure, including management structures of organizations and such deception may be wide-ranging or focused upon achieving specified goals.[7] To identify deception, there is a need for knowledge of the adversary alongside strong intelligence and analysis of their behavior and patterns.[8] Deception detection may be passive and active.[9] Passive deception detection consists of a continual examination of reality seeking false patterns and hidden threats alongside evidence of adversary deception planning.[10] Active deception detection consists of measures of identifying those who plan deception based upon their background history or perceived future intentions.[11] Counterpropaganda, including disinformation, is a neglected area of focus within operating environments. Current strategies are focused towards reactively identifying adversary propaganda and how situational awareness is shaped rather than proactively identifying counterpropaganda, which may mitigate threats.[12]

Deception may be detected through identifying elements of the deceiver's plans.[13] Identifying patterns involved in misdirection, identifying adversaries involved in an operating environment, the intentions they may have, what the payoff or gain may be, where the events take place, adversary strength, adversary style and the information channel involved in communicating the deception.[14] All of these areas may highlight vulnerabilities in an adversary's deception operation and in turn may exploit the target if undetected.

---

[7] Roy Godson and James Wirtz, "Strategic Denial and Deception," in Roy Godson and James Wirtz (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge* (London: Transaction Publishers, 2002), 1-14; Abram Shulsky, "Elements of strategic denial and deception," in Roy Godson and James Wirtz (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge* (London: Transaction Publishers, 2002), 15-33.
[8] Christian Cali and Marc Romanych, "Counterpropaganda: An important capability for joint forces," *IO Sphere* (Fall, 2005): 11-13.
[9] Bell, "Toward a theory of deception."
[10] Ibid.
[11] Ibid.
[12] Cali and Romanych, "Counterpropaganda: An important capability for joint forces"; Godson, and Wirtz, "Strategic denial and deception."
[13] Bell, J. Bowyer, *Cheating: Deception in War & Magic, Games & Sport, Sex & Religion, Business & Con Games, Politics & Espionage, Art & Science* (New York: St Martin's Press, 1982); Barton Whaley and Jeffrey Busby, "Detecting deception: Practice, practitioners, and theory," in Roy Godson and James Wirtz (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge* (London: Transaction Publishers, 2002), 181-221.
[14] Ibid.

https://scholarcommons.usf.edu/jss/vol10/iss1/6
DOI: http://doi.org/10.5038/1944-0472.10.1.1528

Intelligence Approaches to Deception Detection

Approaches towards assessing intelligence and detecting deception include Analysis of Competing Hypotheses (ACH), and techniques outlined by Barton Whaley and Jeff Busby.[15] Analysis of Competing Hypotheses (ACH) consists of a series of steps firstly involving the identification of possible hypotheses. Second evidence and assumptions are listed for and against each hypothesis. Third tentative conclusions are drawn about the likelihood of each hypothesis, including analysis of the sensitivity of the conclusion to significant evidence. Last, the identification of future observations that would confirm or eliminate the hypotheses is made.[16] Analysis of Competing Hypotheses (ACH) has been applied to historical incidents of deception including the D-Day landings and the Battle of Midway.[17] However, ACH may increase vulnerability to adversary deception through weighing hypotheses upon evidence that may be false, and further confirmation biases may occur if evidence fits with multiple hypotheses.[18] To counter confirmation biases and aid decision-making there should be an increased emphasis on seeking refutations for hypotheses rather than confirmations.[19] Although ACH may appear as a promising method of supporting decision-making processes involved in detecting deception, there is a need to incorporate behavioral cues to deception.

Alternative analysis approaches including, ACH, have limitations in identifying significant events, and advocated methods of testing alternatives have not been regularly employed with frequent bias towards the most consistent alternative even if there are potential incongruities.[20] To enhance alternative analysis approaches there is a requirement for:

- increasing analytic imagination by testing many hypotheses;
- independently check source vetting for increased accuracy in deception detection;
- the assessment of missing data to determine validity and check for denial and;

[15] Heuer, Richards, *Psychology of Intelligence Analysis* (Center for the Study of Intelligence, 1999); Karl Spielmann, "Strengthening intelligence threat analysis," *International Journal of Intelligence and Counterintelligence* 25 (2012): 19-43; Frank Stech, and Christopher Elsässer, *Deception Detection by Analysis of Competing Hypotheses,* McLean, Virginia: The Mitre Corporation, 2003; Stech, Frank, and Christopher Elsässer, *Midway Revisited: Detecting Deception by Analysis of Competing Hypothesis,* Mclean, Virginia: The Mitre Corporation, 2004.
[16] Stech, and Elsässer, *Deception Detection by Analysis of Competing Hypotheses*.
[17] Ibid; Stech, and Elsässer, *Midway Revisited: Detecting Deception by Analysis of Competing Hypothesis*.
[18] Ibid.
[19] Richards Heuer, "Limits of intelligence analysis," *Orbis* 49 (2005): 75-94.
[20] Spielmann, "Strengthening intelligence threat analysis."

- make an unbiased assessment of the dominant views evidence and reasoning.[21]

However, further synthesis is required to build upon psychological approaches to deception detection as part of this process – particularly in building from an individual's deception to uncover strategic threats. Findings need further to be made clear to practitioners and lay audiences.[22]

One proposed theory of counter-deception examines techniques employable across multiple contexts.[23] Nine categories of cues (pattern, players, intention, payoff, place, time, strength, style, and channel) are argued to be elements that the deceiver may conceal or reveal during deception. The major principle of this approach is the 'plus-minus rule' where a series of the above characteristics may indicate deception by their presence or absence.[24] Real-world deception may not enable clear differentiation as to a characteristics presence or absence and the 'congruity-incongruity rule' is advanced to suggest where incongruity occurs deception maybe as well.[25] Multiple techniques may be applied to deception detection:

- 'Locard's exchange principle'–where a deceiver may leave evidence at the scene and takes some away;
- 'verification'–of the deception;
- 'the law of multiple sensors'–examination of multiple channels for deceit;
- 'passive and active detection'–the examination of current evidence and the search for further evidence;
- pre-detection–where understanding an adversary's deception modus operandi, goals and capabilities may uncover potential deception;
- 'penetration and counterespionage'–uncovering an adversary's plans through espionage and neutralizing adversary operatives to protect target infrastructure;
- 'the prepared mind and intuition'–where preparation for deception and the intuition to detect it enables counter-deception and;
- 'indirect thinking and the third option'–the ability to detect potential adversary options for deception is required for counter-deception.[26]

[21] Ibid.
[22] Karl Spielmann, "Using enhanced analytic techniques for threat analysis: A case study illustration," *International Journal of Intelligence and Counterintelligence* 27 (2014): 132-155.
[23] Whaley, and Busby, "Detecting deception: Practice, practitioners, and theory."
[24] Ibid.
[25] Ibid.
[26] Ibid.

One final element is the 'Ombudsman Method' where irrelevances, discrepancies, and misdirection are examined alongside indirect thinking and intuition.[27] This approach to deception detection appears promising; however, there is a need for the incorporation of psychological principles of deception detection and decision-making.

Bennett and Waltz's counter-deception approach examines 'intelligence functions' including deception cues, deception detection and exposure, adversary discovery and penetration alongside 'operational functions' incorporating mitigation and exploitation of adversary deception. These functions are argued to be interdependent and present deception as a continuum rather than individual elements.[28] Human reasoning and self-assessment of own beliefs and methods of intelligence gathering and intelligence-gathering channels will identify potential vulnerabilities potentially mitigating the effects of deception.[29] Multiple channels of information should be used to ensure a greater range of human intelligence (HUMINT) with which to assess credibility.[30] Threat and situation assessments are required to understand the influences and circumstances in which deception may occur and such approaches parallel recent psychological approaches to understanding high-stakes future intent.[31] Bennett and Waltz recommend incongruity testing and ACH as tools for detecting deception, and combined with psychological deception detection methods will enable a more accurate credibility assessment.[32]

Tactical Deception Detection

Verbal Deception Detection

Verbal deception detection approaches focus upon examining statements, typically derived from interviews or online content.[33] Traditional approaches have focused upon examining statements taken from interviews through techniques including Statement Validity Analysis (SVA) and Reality Monitoring (RM). Recent Differential Recall Enhancement (DRE) approaches seek to increase the behavioral differences between truth-tellers and deceivers, whilst

[27] Ibid.
[28] Bennett, Michael, and Edward Waltz, *Counterdeception Principles and Applications for National Security* (Artech House: London, 2007).
[29] Ibid.
[30] Ibid.
[31] Ibid; Gozna, Lynsey, and Rebecca Lawday, "An applied scientist-practitioner model for the assessment of high-stake deceptive future intent in forensic and security settings: Incorporating critical consideration of personality, motive, mindet and risk," poster presented at *DECEPTICON 2015: International Conference on Deceptive Behavior*, University of Cambridge, Cambridge, UK, August 24-26, 2015.
[32] Bennett and Waltz, *Counterdeception Principles and Applications for National Security*.
[33] Aldert Vrij, "Verbal lie detection tools: Statement validity analysis, reality monitoring and scientific content analysis," in Par Anders Granhag, Aldert Vrij and Bruno Verschuere (eds.), *Detecting deception: Current challenges and cognitive approaches* (Chichester: Wiley Blackwell, 2015), 4-35.

Forensic Statement Analysis and other linguistic analysis approaches have sought to examine linguistic differences between truth-tellers and deceivers.[34]

Statement Validity Analysis (SVA) involves a review of relevant information, a semi-structured interview, criteria-based content analysis (CBCA) and a Validity Checklist to assess findings, focusing on behaviors that truth-tellers are more likely to perform than deceivers do.[35] In studies of CBCA, some criteria are present more often and have more support in lie-truth discrimination. For example, 'unstructured production' and 'contextual embedding' appear in more than half of studies involving CBCA, whilst 'self-deprecation', 'related external associations' and 'pardoning the perpetrator' appear in only a handful.[36] Such differences in the CBCA literature may in part reflect the studies being variously conducted as field or laboratory research. There are limitations to SVA with scoring, reliability of criteria, establishment of ground truth, lack of a standardized training program, vulnerabilities to countermeasures and further effects generated by culture, context, and personality.[37]

RM proposes that recollections of real experiences are developed from perceptual processes whereas false experiences developed from our imagination will be cognitive in nature enabling discrimination between truthful and deceptive accounts.[38] Reality Monitoring (RM) has shown similar levels of deception

---

[34] Kevin Colwell, Cheryl Hiscock-Anisman, and Jacquelyn Fede, "Assessment criteria indicative of deception: An example of the new paradigm of differential recall enhancement," in Barry Cooper, Dorothee Griesel and Marguerite Ternes (eds.), *Applied Issues in Investigative Interviewing, Eyewitness Memory, and Credibility Assessment* (London: Springer, 2013), 259-291; Charles Morgan, Kevin Colwell and Gary Hazlett, "Efficacy of forensic statement analysis in distinguishing truthful from deceptive eyewitness accounts of highly stressful events," *Journal of Forensic Sciences* 56 (2011): 1227-1234; Charles Morgan, Yaron Rabinowitz, Deborah Hilts, Craig Weller and Vladimir Coric, "Efficacy of Modified Cognitive Interviewing, Compared to Human Judgments in Detecting Deception Related to Bio-threat Activities," *Journal of Strategic Security* 6 (2013): 100-119; Charles Morgan, Yaron Rabinowitz, Robert Leidy and Vladimir Coric, "Efficacy of combining interview techniques in detecting deception related to bio-threat issues," *Behavioral Sciences and the Law* 32 (2014): 269-285; Charles Morgan, Yaron Rabinowitz, Beau Palin and Kirk Kennedy, "Who should you trust? Discriminating genuine from deceptive eyewitness accounts," *The Open Criminology Journal* under review; Jeffrey Hancock, Lauren Curry, Saurabh Goorha and Michael Woodworth, "On lying and being lied to: A linguistic analysis of deception in computer-mediated communication," *Discourse Processes* 45 (2008): 1-23; Matthew Newman, James Pennebaker, Diane Berry and Jane Richards "Lying words: Predicting deception from linguistic style," *Personality and Social Psychology Bulletin* 29 (2003): 665-675.

[35] Vrij, "Verbal lie detection tools: Statement validity analysis, reality monitoring and scientific content analysis."

[36] Stephen Porter and Leanne ten Brinke, "The truth about lies: What works in detecting high-stakes deception?" *Legal and Criminological Psychology* 15 (2010): 57-75.

[37] Aldert Vrij, "Criteria-based content analysis: A qualitative review of the first 37 studies," *Psychology, Public Policy and Law* 11 (2005): 3-41; Aldert Vrij, Wendy Kneller, and Samantha Mann, "The effect of informing liars about criteria-based content analysis on their ability to deceive CBCA-raters," *Legal and Criminological Psychology* 5 (2000): 57-70.

[38] Gary Bond and Adrienne Lee, "Language of lies in prison: Linguistic classification of prisoners' truthful and deceptive natural language," *Applied Cognitive Psychology* 19 (2005): 213-329; Siegfried Sporer, "Reality monitoring and detection of deception," in Par Anders

https://scholarcommons.usf.edu/jss/vol10/iss1/6
DOI: http://doi.org/10.5038/1944-0472.10.1.1528

detection accuracy and similar limitations to SVA while differences between real and imagined events may fade over time and behavioral differences may actually be due to interviewing techniques rather than RM.[39]

Differential Recall Enhancement (DRE) approaches focus on increasing behavioral differences between liars and truth-tellers using cognitive mnemonics, questioning strategy and use of evidence, for example, Assessment Criteria Indicative of Deception (ACID), strategic use of evidence (SUE), and cognitive approaches.[40] Differential Recall Enhancement (DRE) is considered to assist honest people in their recall and provides more detailed and verbose statements whilst deceptive people work harder to maintain credibility and over-rely on short, carefully constructed narratives.[41] The mnemonic section of statements can lead to an increase in accuracy of the order of 10-27 percent in veracity assessment – suggesting that DRE techniques are useful for detecting deception in investigative interviewing.[42] DRE techniques may overcome the paucity of valid cues to deception, although their application outside of interview specific contexts will be limited. [43]

The ACID technique analyses the admittance of potential errors, length of responses and RM criteria associated with differences due to memory, impression management, and unique contextual and internal/external details as they appear during a police investigative interview.[44] The Reality Interview (RI) increases an interviewee's cognitive load to elicit cues to deception and to challenge impression management strategies.[45] There is evidence that the ACID approach can accurately classify 86.8 percent of statements (78.9 percent truthful and 94.7

Granhag and Leif Strömwall (eds.), *The Detection of Deception in Forensic Contexts* (Cambridge: Cambridge University Press, 2004), 64-102; Vrij, Aldert, *Detecting Lies and Deceit: Pitfalls and Opportunities*(Chichester: Wiley, 2008).

[39] Colwell, Hiscock-Anisman and Fede, "Assessment criteria indicative of deception: An example of the new paradigm of differential recall enhancement."; Marcia Johnson, Mary Ann Foley, Aurora Suengas and Carol Raye, "Phenomenal characteristics of memories for perceived and imagined autobiographical events," *Journal of Experimental Psychology: General* 117 (1988): 371-376; Vrij, *Detecting Lies and Deceit: Pitfalls and Opportunities*.

[40] Colwell, Hiscock-Anisman and Fede, "Assessment criteria indicative of deception: An example of the new paradigm of differential recall enhancement.";
Par Anders Granhag and Maria Hartwig, "The strategic use of evidence technique: A conceptual overview," in Par Anders Granhag, Aldert Vrij and Bruno Verschuere (eds.), *Detecting Deception Current Challenges and Cognitive Approaches* (Chichester: Wiley-Blackwell, 2015), 231-251; Aldert Vrij, "A cognitive approach to lie detection," in Par Anders Granhag, Aldert Vrij and Bruno Verschuere (eds.), *Detecting Deception Current Challenges and Cognitive Approaches* (Chichester: Wiley-Blackwell, 2015), 205-229.

[41] Colwell, Hiscock-Anisman and Fede, "Assessment criteria indicative of deception: An example of the new paradigm of differential recall enhancement."

[42] Ibid.

[43] Maria Hartwig and Charles Bond, "Why do lie-catchers fail? A lens model meta-analysis of human lie judgements," *Psychological Bulletin* 137 (2011): 643-659.

[44] Colwell, Hiscock-Anisman and Fede, "Assessment criteria indicative of deception: An example of the new paradigm of differential recall enhancement."

[45] Ibid.

percent deceptive) and has the potential to be applied across cultures.[46] However, the ACID technique is limited when individuals are questioned about their attitudes and intent, in uncovering concealed information, and when an individual believes or is mistaken in what they are saying.[47] Validation in applied contexts is therefore required although research into its application to online environments is emerging.[48]

Use of evidence to increase behavioral differences between truth-tellers and deceivers has led to the development of strategic and tactical interviewing approaches[49]. Strategic and tactical interviewing approaches attempt to counter suspects' strategies by enabling the process of free recall before a challenge phase where varying strengths of evidence are presented which may highlight inconsistencies within suspects' accounts and between accounts and evidence.[50] Tactical interviewing approaches are suggested to be more cognitively demanding than strategic, potentially enabling greater behavioral differences between truth-tellers and deceivers.[51] However, the contexts in which these approaches can be usefully applied tend toward interviews concerning serious allegations where planning and time can be used effectively by interviewers. The application of such techniques in the online environment is presently unknown but appears to have potential in dyadic interactions.

Cognitive approaches increase behavioral differences between liars and truth-tellers through asking cognitively demanding and unanticipated questions to circumvent deceivers' preparations.[52] Cognitively demanding questions focus on reverse order recall and maintenance of eye contact whilst unanticipated questions have focused on sketch drawing to enhance behavioral differences between truth-tellers and liars.[53] Although validation in applied settings is required such techniques may be useful in uncovering verbal deception in interaction whilst application to areas outside of conversational interaction and other communication channels is more difficult to assess.

---

[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Coral Dando and Ray Bull, "Maximising opportunities to detect verbal deception: Training police officers to interview tactically," *Journal of Investigative Psychology and Offender Profiling* 8 (2011): 189-202; Maria Hartwig, Par Anders Granhag, Leif Strömwall and Ola Kronkvist, "Strategic use of evidence during police interviews: When training to detect deception works," *Law and Human Behavior* 30 (2006): 603-619.
[50] Dando and Bull, "Maximising opportunities to detect verbal deception: Training police officers to interview tactically,"; Granhag and Hartwig, "The strategic use of evidence technique: A conceptual overview."
[51] Dando and Bull, "Maximising opportunities to detect verbal deception: Training police officers to interview tactically."
[52] Vrij, "A cognitive approach to lie detection."
[53] Ibid.

https://scholarcommons.usf.edu/jss/vol10/iss1/6
DOI: http://doi.org/10.5038/1944-0472.10.1.1528

Forensic statement analysis examines narrative accounts of events though focusing on response length, unique word count, and type-token ration (the ratio of unique word count to response length).[54] Current application of these techniques has sought to identify differences between truth-tellers and deceivers related to biological threats at both group and low-base rate conditions, which more accurately reflect the reality of such threats.[55] Forensic statement analysis has further application to distinguishing genuine and deceptive eyewitness accounts, including the input of false information.[56] Examining the credibility of claims is crucial in strategic environments as passively accepting presented information may enable exploitation by the deceiver.

Linguistic techniques for analyzing behavioral differences between truth-tellers and deceivers have focused upon analyzing narrative to understand underlying thoughts, motives, and emotions across real world and mediated environments.[57] Further, analysis of language change in online communication has enabled the identification of cues to deceit, including potential cues to deception related to insider threat and linguistic markers for radical violence.[58] In linguistic patterns in synchronous computer-mediated communication (CMC), deceivers may use a greater number of words, sense-based words, and other-oriented pronouns and use less self-oriented words when lying than when telling the truth.[59] Increasing

---

[54] Morgan, Colwell and Hazlett, "Efficacy of forensic statement analysis in distinguishing truthful from deceptive eyewitness accounts of highly stressful events"; Morgan, Rabinowitz, Hilts, Weller and Coric, "Efficacy of Modified Cognitive Interviewing, Compared to Human Judgments in Detecting Deception Related to Bio-threat Activities"; Morgan, Rabinowitz, Leidy and Coric, "Efficacy of combining interview techniques in detecting deception related to bio-threat issues"; Morgan, Rabinowitz, Palin and Kennedy, "Who should you trust? Discriminating genuine from deceptive eyewitness accounts."

[55] Morgan, Rabinowitz, Leidy and Coric, "Efficacy of combining interview techniques in detecting deception related to bio-threat issues"; Morgan, Rabinowitz, Hilts, Weller and Coric, "Efficacy of Modified Cognitive Interviewing, Compared to Human Judgments in Detecting Deception Related to Bio-threat Activities."

[56] Morgan, Colwell and Hazlett, "Efficacy of forensic statement analysis in distinguishing truthful from deceptive eyewitness accounts of highly stressful events"; Morgan, Rabinowitz, Palin and Kennedy, "Who should you trust? Discriminating genuine from deceptive eyewitness accounts."

[57] Newman, Pennebaker, Berry and Richards "Lying words: Predicting deception from linguistic style"; Bond and Lee, "Language of lies in prison: Linguistic classification of prisoners' truthful and deceptive natural language."

[58] Hancock, Curry, Goorha and Woodworth, "On lying and being lied to: A linguistic analysis of deception in computer-mediated communication"; Catalina Toma and Jeffrey Hancock, "What lies beneath: The linguistic traces of deception in online dating profiles," *Journal of Communication* 62 (2012): 78-97; Lina Zhou, Judee Burgoon, Jay Nunamaker and Doug Twitchell, "Automating linguistics-based cues for detecting deception in text-based asynchronous computer-mediated communication," *Group Decision and Negotiation* 13 (2004): 81-106; Paul Taylor, Coral Dando, Thomas Ormerod, Linden Ball, Marissa Jenkins, Alexandra Sandham and Tarek Menacere, "Detecting insider threats through language change," *Law and Human Behavior* 37 (2013): 267-275; Katie Cohen, Fredrik Johansson, Lisa Kaati and Jonas Mork, "Detecting linguistic markers for radical violence in social media," *Terrorism and Political Violence* 26 (2014): 246-256.

[59] Hancock, Curry, Goorha and Woodworth, "On lying and being lied to: A linguistic analysis of deception in computer-mediated communication."

the number of words may be used by deceivers to appear more credible or as a strategy of distracting the receiver from inconsistencies in narrative, while other tactics may involve the deceiver distancing themselves from their behavior.

Non-Verbal Deception Detection

Non-verbal approaches have focused upon detecting deception through examining facial expressions, including micro-expressions and body language.[60] However non-verbal cues are potentially rare and do not guarantee the presence of deception. Furthermore, assigning such cues as being 'deceptive', as distinct from idiosyncratic behavior or forms of arousal may lead to error. Although discernible differences in facial expressions may be specific to high stake environments such as appealing for the return of missing loved ones, an awareness of the manifestation of genuine emotions is applicable to assessing veracity in interpersonal and online domains.[61]

Micro-expressions are considered universal and comprise seven composite facial expressions of particular emotional experience (happiness, surprise, sadness, fear, disgust, contempt, and anger) that are argued to appear for less than a quarter of a second and in a particular context may suggest that an individual is deceiving.[62] There is evidence for variations in the occurrence of facial expressions, in particular, some expressions appearing in the upper or lower face, some emotions appearing easier to fake than others, micro-expressions presenting for longer than anticipated, occurring more in high intensity emotional displays, appearing in truthful and deceptive accounts, and less frequently than anticipated.[63] It is argued that the context of an interaction and its effect on an individual results in micro-expressions exposing true emotions; however the impact of individual differences is largely unknown.

---

[60] Ekman, Paul. *Telling Lies: Clues to Deceit in the Marketplace, Politics and Marriage* (London: W.W Norton & Company, 2001); Bella DePaulo, James Lindsay, Brian Malone, Laura Muhlenbruck, Kelly Charlton and Harris Cooper, "Cues to deception," *Psychological Bulletin* 129 (2003): 74-118.

[61] Leanne ten Brinke, Sarah MacDonald, Stephen Porter and Brian O'Connor, "Crocodile tears: Facial, verbal and body language behaviors associated with genuine and fabricated remorse," *Law and Human Behavior* 36 (2012): 51-59; Leanne ten Brinke and Stephen Porter, "Cry me a river: Identifying the behavioural consequences of extremely high-stakes interpersonal deception," *Law and Human Behavior* 36 (2012): 469-477; Leanne ten Brinke, Stephen Porter and Alysha Baker, "Darwin the detective: Observable facial muscles reveal emotional high-stakes lies," *Evolution and Human Behavior* 33 (2012) 411-416.

[62] Ekman, *Telling Lies: Clues to Deceit in the Marketplace, Politics and Marriage*.

[63] Stephen Porter and Leanne ten Brinke, "Reading between the lies: How do facial expressions reveal concealed and fabricated emotions?," *Psychological Science* 19 (2008): 508-514; Stephen Porter and Leanne ten Brinke, "The truth about lies: What works in detecting high-stakes deception?," *Legal and Criminological Psychology* 14 (2010): 119-134; Stephen Porter, Leanne ten Brinke and Brendan Wallace, "Secrets and lies: Involuntary leakage in deceptive facial expressions as a function of emotional intensity," *Journal of Nonverbal Behavior* 36 (2012): 23-37; ten Brinke, MacDonald, Porter and Brian O'Connor, "Crocodile tears: Facial, verbal and body language behaviours associated with genuine and fabricated remorse"; ten Brinke and Porter, "Cry me a river: Identifying the behavioural consequences of extremely high-stakes interpersonal deception."

https://scholarcommons.usf.edu/jss/vol10/iss1/6
DOI: http://doi.org/10.5038/1944-0472.10.1.1528

People may show discomfort when being interviewed and when engaging in deception in the form of manipulators, and illustrators, although these behaviors are not necessarily indicative of malign intent.[64] Increased cognitive load may lead to a reduction in illustrators which may make deceivers appear tense whilst truth-tellers are likely to increase their illustrators to complement their narrative.[65] The greatest challenge in interpreting such findings is to identify the extent to which they are applicable to non-student groups, for example, it is unclear whether non-students exhibit greater or fewer illustrator cues to deception.[66] There is evidence that offenders may increase manipulators during fabricated stories suggesting that deceivers' usage of these behaviors is context dependent or a strategy to distract from verbal content.[67] Hence, the baseline of truthful behavior in a particular context of interest has to be established before judgements regarding deception can be made. Non-verbal deception detection approaches have the potential to be used across real-world interactions and mediated interactions where there is visual content, and suspicious behavior based upon validated cues to deception may enable the identification of individual for further monitoring.

Online Deception Detection

Online deception detection approaches examine online verbal and linguistic content, features of the online environment that are used to make credibility judgements, identifying links between an individual's real world and online persona and heuristics individuals rely on in credibility judgements.[68] One approach related to analyzing features is the so-called 'Theory of Deception,' where individuals are argued to detect deception by noticing and interpreting anomalies in their environment through reference to the goals and aims ascribed to interactional partners.[69] In testing this approach, in conjunction with a real website, a 'hi-jacked' website was created to replicate the real website and half the

---

[64] Mark Frank, "Thoughts, feelings, and deception" in Brooke Harrington (ed.), *Deception: From Ancient Empires to Internet Dating* (Stanford: Stanford University Press, 2009), 55-73.
[65] DePaulo, Lindsay, Malone, Muhlenbruck, Charlton and Cooper, "Cues to deception"; Frank, "Thoughts, feelings, and deception"; ten Brinke and Porter, "Cry me a river: Identifying the behavioural consequences of extremely high-stakes interpersonal deception"; Joe Navarro, "A four-domain model for detecting deception," *FBI Law Enforcement Bulletin* (June, 2003): 19-24.
[66] Porter and ten Brinke, "The truth about lies: What works in detecting high-stakes deception?"
[67] Stephen Porter, Laura England, Marcus Juodis, Leanne ten Brinke and Kevin Wilson, "Is the face a window to the soul? Investigation of the accuracy of intuitive judgements of the trustworthiness of human faces," *Canadian Journal of Behavioural Science* 40 (2008): 171-177.
[68] See discussion of Verbal Deception Detection
[69] Stefano Grazioli, "Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet," *Group Decision and Negotiation* 13 (2004): 149-172; Paul Johnson, Stefono Grazioli, Karim Jamal and R. Glen Berryman, "Detecting deception: Adversarial problem solving in a low base-rate world," *Cognitive Science* 25 (2001): 355-392.

computer savvy sample was unknowingly directed to the 'hi-jacked' site.[70] In correctly identifying the deceptive site, individuals used fewer but more accurate cues related to information assurance rather than trust and such strategies may be used upon individuals' knowledge and use of a communication format alongside awareness of potential for deception online.[71]

Further development of 'Theory of Deception' argues that the recipient's individual disposition and perceptions are also vital for detecting cues to deception.[72] Disposition to trust and Web experience are influences on detecting phishing, however computer self-efficacy, security knowledge, perceived risk, and suspicion of humanity may not be strong predictors of detection.[73] In detecting phishing via email, there are two points of detection: The first point is before the email is opened, where email authentication cues are salient and second after the email is opened it becomes the only source of cues to deception.[74] Once opened there is an initial authentication of the email and perceived cues to deception before suspicion is activated by the relationship between the cues, context and individual factors.[75] Individual factors include sensitivity to the value of information, concern for privacy, obedience to authority and conscientiousness in judgement, whilst contextual factors were linked to knowledge of the institution. The third stage of deception detection involved individuals' confirmation of suspicion. The evaluation of the hypotheses was found to be related to two main categories: confirmation seeking of authenticity and individual investigation of authenticity.[76]

Prominence-Interpretation Theory (PIT) argues that individuals assess credibility of websites through noticing features, judging them and then assigning credibility.[77] Assignation of prominence is affected by user involvement, website content, the user task, user experience, and individual differences.[78] User assumptions, skills and knowledge, context and goals are argued to be linked to the interpretation of features.[79] Prominence-Interpretation Theory (PIT) focusses on the content and interpretation of the user in assessing credibility of websites,

---

[70] Grazioli, "Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet."
[71] Ibid.
[72] Ryan Wright, Suranjan Chakraborty, Asli Basoglu and Kent Marett, "Where did they go right? Understanding the deception in phishing communications," *Group Decision and Negotiation* 19 (2010): 391-416.
[73] Ibid.
[74] Ibid.
[75] Ibid.
[76] Ibid.
[77] Fogg, BJ, "Prominence-interpretation theory: Explaining how people assess credibility," *CHI '03*, Fort Lauderdale, Florida, April 5-10, 2003; Fogg, BJ, Cathy Soohoo, David Danielson, Leslie Marable, Julianne Stanford and Ellen Yauber, "How do users evaluate the credibility of web sites?: A study with over 2,500 participants," *DUX '03*, New York, New York, 2003.
[78] Ibid.
[79] Ibid.

https://scholarcommons.usf.edu/jss/vol10/iss1/6
DOI: http://doi.org/10.5038/1944-0472.10.1.1528

however, it seems possible that individual may assess credibility in this manner in other contexts including other forms of online content and has the potential for expansion to face-to-face situations.

Individuals are argued to use different prominent features to assess credibility of websites based upon the website context.[80] For example, e-commerce sites are judged according to their reputation and recognition, whilst news sites are judged according to perceived bias of information, non-profit organizations are judged according to their identity, and opinion/review sites are judged according to their information bias and accuracy with further judgements informed by individuals user experience.[81] Knowledge of how individuals construct credibility of websites based upon their features is important to understand, however, when dealing with deception in strategic environments false online content may have plausible features leading to inaccurate judgements of credibility.

When people are engaging in activities, including deception, depending on the nature of the behavior there can be 'warrants', for example, organizational credential's in an email account or a profile photo in an online social network, which enable links to be examined between an individual's real-world and online identities.[82] Individuals may deceive more frequently in online chat environments that enable greater anonymity, and less often in the use of email where warrants are visible. The stakes of such interactions and the intent of the deceiver are critical to ascertain in such situations, particularly those involving criminal activities and breaches of security. Although examining warrants may be a useful strategy for assessing credibility in low-stakes online interactions, in high-stakes interactions this may be more troublesome where motivation, resources and ability to manipulate identity may enable a convincing false warrant' to be displayed.

Uncovering hidden deception and malign intent across interpersonal and online environments can include the identification of 'digital footprints', 'digital exhaust,' or 'scent trails' that can be coupled with other forms of evidence such as surveillance footage.[83] Although rarely the focus of traditional deception approaches, examining patterns of behavior, including email communications, online statements and online searches of information about potential targets may

[80] Fogg, Soohoo, Danielson, Marable, Stanford and Yauber, "How do users evaluate the credibility of web sites?: A study with over 2,500 participants."
[81] Ibid.
[82] Warkentin, Darcy, Michael Woodworth, Jeffrey Hancock and Nicole Cormier "Warrants and deception in computer mediated communication," *CSCW*, Savannah, Georgia, February 6-10, 2010.
[83] Peter Forster, "Countering Individual Jihad: Perspectives on Nidal Hasan and Colleen LaRose," *CTX* 2 (2012): 1-11; Sandham, Alexandra, Thomas Ormerod, Coral Dando, Ray Bull, M Jackson and J Goulding, "Scent trails: Countering terrorism through informed surveillance," *Engineering Psychology and Cognitive Ergonomics – 9th International Conference*, Orlando, Florida, 2011.

enable the identification of concealed actions.[84] When drawing from tactical to strategic level deception detection, a proactive stance is required, where potential threats are monitored to ensure that information is collated and assessed for deceit. Furthermore, there is potential for collected evidence to be later used in investigative interviews with which to challenge suspects' narratives.

Further understanding of how credibility judgements are made regarding online content focuses upon construction of credibility, heuristics, and interaction, or how such strategies amalgamate.[85] The construct level examines how individuals construct credibility, which in turn influences how they judge credibility.[86] The heuristics level involves judgement strategies that are used across multiple contexts, whilst the interaction level focuses on judgements based upon source and content cues.[87] Heuristics identified from a U.S. sample include *reputation*, *endorsement*, *consistency*, *self-confirmation*, *expectancy violation*, and *persuasive intent*.[88] Although there is difficulty in sorting heuristics into explicit categories as processes may occur simultaneously in decision-making, and contexts may generate multiple heuristics, alongside one heuristic activating another.[89] The interaction level focuses upon individuals' interactions with a website and neglects the online interactions that occur between individuals that require credibility judgements that will be influenced by interpersonal dynamics. Furthermore, the framework proposed does not focus upon the accuracy of credibility judgements in identifying truth and deception.

Psychological Synthesis

To effectively understand and challenge the myriad forms of deception across varying contexts and communication mediums, alongside identifying emerging strategic deception there is a requirement for a synthesis of approaches. Such a synthesis will incorporate multiple deception detection techniques that will be tailored to reflect the context of the interaction, and it is acknowledged that not all techniques will be relevant for all interactions. Where possible in-depth analysis of the actors involved in deception should be conducted to understand the culture and motives from which strategic deception will emerge, and enable the identification of personalities that may present additional challenges to practitioners. Intelligence, surveillance and evidence will aid practitioners once sources and evidence have been verified for authenticity, they can enable the identification of truth or deception by individuals, or where such evidence proves

[84] Forster, "Countering individual Jihad: Perspectives on Nidal Hasan and Colleen LaRose"
[85] Brian Hilligoss and Soo Young Rieh, "Developing a unifying framework for credibility assessment: Construct, heuristics, and interaction in context," *Information Processing and Management* 44 (2008): 1467-1484.
[86] Ibid.
[87] Ibid.
[88] Miriam Metzger, Andrew Flanagin and Ryan Medders, "Social and heuristic approaches to credibility evaluation online," *Journal of Communication* 60 (2010): 413-439.
[89] Ibid.

inconclusive it will provide further justification for the surveillance of individuals of interest.[90] Once individuals have been identified as deceptive or flagged for further monitoring, social network analysis of these individuals should be conducted to identify further threats and deception targeted at strategic interests.

Intelligence, Surveillance and Evidence

Intelligence, surveillance, and evidence play a crucial role in uncovering deception by individuals and groups. Intelligence, surveillance, and evidence techniques may be used to identify potential threats, uncover links between individuals and groups, and contrast with individuals' accounts to ensure credibility. Intelligence and evidence can be used in investigative interviews to elicit greater behavioral differences between truth-tellers and deceivers. Whilst surveillance techniques can provide further monitoring of individuals who are suspected of deception if there is no current evidence. However, caveats of these techniques exist, as they are required to operate within the laws of the affected nation, and sources of information alongside the content need to be verified for credibility to ensure reliability of evidence.

There are varieties of forms of intelligence available to practitioners to assist them in their analyses, whether in criminal, security and other strategic environments.[91] HUMINT, image intelligence (IMINT), signals intelligence (SIGINT), open source intelligence (OSINT), and more recently social media intelligence (SOCMINT) all enable practitioners to develop comprehensive accounts of actions whether committed by an individual or a group.[92] However, to ensure the credibility of such intelligence requires verification of the source of information through an approach tailored by the techniques outlined above, and of the information, such source or communication channel provides. For example, linguistic analysis techniques may be used to assess the credibility HUMINT, OSINT and SOCMINT, whilst Subject Matter Experts (SMEs) may be used to assess the reliability of IMINT and SIGINT. Once intelligence and evidence is verified, it can then be used to assess the reliability of statements or used as evidence to elicit behavioral differences between truth-tellers and deceivers. Social network analysis however may be used to uncover links between actors and identify where strategic deception may be emerging.[93]

---

[90] Scott Schumate and Randy Borum, "Psychological support to defense counterintelligence operations," *Military Psychology* 18 (2006): 283-296.
[91] Sir David Omand, Jamie Bartlett and Carl Miller, "Introducing social media intelligence (SOCMINT)," *Intelligence and National Security* 27 (2012): 801-823.
[92] Ibid.
[93] Melonie Richet and Matthias Binz, "Open source collection methods for identifying radical extremists using social media," *International Journal of Intelligence and Counterintelligence* 28 (2015): 347-364.

Actors

To enhance understanding of deception an understanding of the individuals and organizations involved in deception is required. Practitioners in operational environments have readily accepted this premise, where enhanced understanding of culture and elements of personality has been required across counterintelligence.[94] Understanding how individuals present themselves in interactions has particular relevance to HUMINT interviews where gathered intelligence can have large-scale ramifications if it is accepted as credible when it is not.

The acceptance and likelihood of engaging in forms of deception may be based on exclusive or multiple personality traits alongside the motive and context of behavioral interactions.[95] There are disorders related to deception, pathological lying and instrumental gain that need to be considered by practitioners as potential explanations for suspects' motives and behavior and will present additional challenges in detecting deception that affects strategic interests. Psychopathy, Narcissism and Machiavellianism are three such personality constructs that will present additional challenges for practitioners.[96] Although not all individuals will have such personalities, practitioners nevertheless still require understanding of how such personalities manifest across individuals, groups and communication mediums.

The impact of cultural differences on understanding deception is critical in the globalized world. Deception is an evolutionary trait found in varying forms in every culture in the world, although different cultures have different beliefs regarding deception; for example, amongst Arabic people deception is acceptable if an individual is seeking societal approval.[97] When people are communicating in different languages their ability to detect deception will be affected by language

---

[94] Richet and Binz, "Open source collection methods for identifying radical extremists using social media"; Schumate and Borum, "Psychological support to defense counterintelligence operations."

[95] Beverley McLeod and Randy Genereux, "Predicting the acceptability and likelihood of lying: The interaction of personality with type of lie," *Personality and Individual Differences* 45 (2008): 591-596.

[96] Taylor, Rachel, and Lynsey Gozna, *Deception: A Young Person's Life Skill?* (Hove: The Psychology Press, 2011); Cleckley, Hervey, *The Mask of Sanity,* (New York: Plume, 1982); Hare, Robert, *Psychopathy: Theory and Research,* (New York: John Wiley, 1970); Robert Raskin and Calvin Hall, "A narcissistic personality inventory," *Psychological Reports* 45 (1979): 590; Christie, Richard and Florence Geis, *Studies in Machiavellianism,* (New York: Academic Press, 1970).

[97] Charles Bond and Sandhya Rao, "Lies travel: Mendacity in a mobile world," in Par Anders Granhag and Leif Strömwall (eds.), *The Detection of Deception in Forensic Contexts* (Cambridge: Cambridge University Press, 2004), 127-141; Fayez Al-Simadi, "Detection of deceptive behaviour: A cross-cultural test," *Social Behavior and Personality* 28 (2000): 455-462.

https://scholarcommons.usf.edu/jss/vol10/iss1/6
DOI: http://doi.org/10.5038/1944-0472.10.1.1528

and it is hard to analyze whether this will benefit the deceiver or the target.[98] Cognitive load approaches to deception detection have also sought to detect deception in those from other nations and cultures.[99] ACID has been found to detect deception in Arabic, Spanish, and English from a range of cultures and has found similar impression management strategies in English and Chinese speakers.[100] Forensic statement analysis has further enabled discrimination between truthful and deceptive Arabic speakers whilst forced-choice questioning has also led to accurate identification of truthful and deceptive Russian and Vietnamese speakers.[101]

The CHAMELEON Approach to Interviewing (CAI) is a personality led investigative interview approach that takes into account a far wider breadth of information than traditional investigative interview approaches.[102] In dealing with individuals, it is acknowledged that every offender/suspect has the potential to be different from each other, to be different at different times, to behave differently with different people, to behave differently across different actions committed, to behave differently across different interviews, and to be different within each interview.[103] Individuals will have different backgrounds, life experiences, attitudes, beliefs, offences, and modus operandi (MO). Each individual has the potential to vary in his or her cognitive ability, his or her affect, and his or her cooperativeness at different times. There will also be endogenous and exogenous effects on an individual such that each will behave differently with different interactional partners due to personal dynamics including, age, gender and socio-economic status and previous experience with people and what are

---

[98] Bond and Sandhya Rao, "Lies travel: Mendacity in a mobile world"; Keens Cheng, Hiu Wan and Roderick Broadhurst, "The detection of deception: The effects of first and second language on lie detection ability," *Psychiatry, Psychology and Law* 12 (2005): 107-118.
[99] Colwell, Hiscock-Anisman and Fede, "Assessment criteria indicative of deception: An example of the new paradigm of differential recall enhancement."; Charles Morgan and Gary Hazlett, "Efficacy of forced-choice testing in detecting deception in Russian," *Journal of Intelligence Community Research and Development* (2009); Charles Morgan, Aaron Mishara, John Christian and Gary Hazlett, "Detecting deception through automated analysis of translated speech: Credibility assessments of Arabic-speaking interviewees," *Journal of Intelligence Community Research and Development* (2008): 1-22; Charles Morgan, Yaron Rabinowitz, George Kallivrousis and Gary Hazlett, "Efficacy of automated forced-choice testing dilemmas in detecting deception in Vietnamese," *Journal of Intelligence Community Research and Development* (2010): 1-11.
[100] Colwell, Hiscock-Anisman and Fede, "Assessment criteria indicative of deception: An example of the new paradigm of differential recall enhancement."
[101] Morgan, Mishara, Christian and Hazlett, "Detecting deception through automated analysis of translated speech: Credibility assessments of Arabic-speaking interviewees"; Morgan and Hazlett, "Efficacy of forced-choice testing in detecting deception in Russian"; Morgan, Rabinowitz, Kallivrousis and Hazlett, "Efficacy of automated forced-choice testing dilemmas in detecting deception in Vietnamese."
[102] Julian Boon and Lynsey Gozna, "Firing pea-shooters at elephants", *The Psychologist* 22 (2009): 762-764; Lynsey Gozna and Julian Boon, "Interpersonal deception detection," in Jennifer Brown and Elizabeth Campbell (eds.), *The Cambridge Handbook of Forensic Psychology* (Cambridge: Cambridge University Press, 2010), 484-491; Taylor and Gozna, *Deception: A Young Person's Life Skill?*
[103] Boon and Gozna, "Firing pea-shooters at elephants"; Gozna and Boon, "Interpersonal deception detection."

those people's objectives. Each individual will be different within and across interviews due to how penetrative questions are the subtlety of questions, and the degree of incriminations as the interview progresses.

Application to a Multi-Incident Terrorist Scenario:

Across modern operating environments, scenarios have been used to increase ability to respond to challenges posed by a variety of groups including, amongst others, terrorist organizations. Following recent terrorist incidents in Western nations including the failed Thalys train attack, the San Bernadino attack in the United States, the recent multi-location attacks in Paris and Brussels, and the resurgence of an active IRA, there is a need to develop complex scenarios. Scenarios are used to highlight how such incidences may be countered through understanding how multiple incidences of deception may enable a large-scale attack, alongside the objectives of individuals and groups involved in such activity. Scenario use for examining futures has been conducted across a wide range of areas, including in strategic planning, management, and business, the risk assessment and management of offenders, and in red-teaming terrorist scenarios.[104] Scenarios may be used as decision-making tools to overcome limitations and enable preparation for the unexpected and the construction of meaning from uncertainty and ambiguity through developing creative future responses.[105] Scenarios are socially constructed narratives, which integrate

[104] Edwin Bakker, "Forecasting terrorism: The need for a more systematic approach," *Journal of Strategic Security*, 5 (2012): 69-84; DCDC, *Global Strategic Trends – Out to 2040* (Swindon: DCDC, 2010a); DCDC, *Future Character of Conflict* (Swindon: DCDC, 2010b); DCDC, *Global Strategic Trends – Out to 2045* (Swindon: DCDC, 2014); Enid Mante-Meijer, Patrick van der Duin and Muriel Abeln, "Fun with scenarios," *Long Range Planning* 31 (1998): 628-637; Alex Wright, "The role of scenarios as prospective sensemaking devices," *Management Decision* 43 (2005): 86-101; Kevin Douglas, "Version 3 of the Historical-Clinical-Risk Management-20 (HCR-20 V3): Relevance to violence risk assessment and management in forensic conditional release contexts," *Behavioral Sciences and the Law* 2014 (32): 557-576; Stephen Hart and Caroline Logan, "Formulation of violence risk using evidence-based assessments: The structured professional judgement approach" in Peter Sturmey and Mary McMurran (eds.), *Forensic Case Formulation* (Chichester: Wiley Blackwell, 2011); David Romyn and Mark Kebbell, "Terrorists' planning of attacks: A simulated 'red-team' investigation into decision-making," *Psychology, Crime & Law* 2014 (20): 480-496

[105] Muhammad Amer, Tugrul Daim and Antonie Jetter, "A review of scenario planning," *Futures* 46 (2013): 23-40; Frank Buytendijk, Toby Hatch and Pietro Micheli, "Scenario-based strategy maps,", *Business Horizons* 53 (2010): 335-347; Hugues De Jouvenel, "A brief methodological guide to scenario building," *Technological Forecasting and Social Change* 65 (2000): 37-48; Gary R. Bowman, Bradley MacKay, Swapnesh Masrani and Peter MacKiernan, "Storytelling and the scenario process: Understanding success and failure," *Technological Forecasting and Social Change* 80 (2013): 735-748; Philippe Durance and Michel Godet, "Scenario building: Uses and abuses," *Technological Forecasting and Social Change* 77 (2010): 1488-1492; Jiří Fotr, Miroslav Špaček, Ivan Souček and Emil Vacík, "Scenarios, their concept, elaboration and application," *Baltic Journal of Management* 10 (2015): 73-97; Michel Godet and Fabrice Roubelat, "Creating the future: The use and misuse of scenarios," *Long Range Planning* 29 (1996): 164-171; Sohail Inayatullah, "Six pillars: Futures thinking for transforming," *Foresight* 10 (2008): 4-21; Celeste Varum and Carla Melo, "Directions in scenario planning literature – A review of the past decades," *Futures* 42 (2010): 355-369; Wright, "The role of scenarios as prospective sensemaking devices."

https://scholarcommons.usf.edu/jss/vol10/iss1/6
DOI: http://doi.org/10.5038/1944-0472.10.1.1528

predetermined events with critical uncertainties to encourage future thinking and are not predictions or forecasts of the future.[106]

Methodology

The explorative approach to scenario development is a qualitative approach examining the structural uncertainty of futures to gain awareness and critical insight.[107] This approach has clearly defined goals, and the current research focuses on a deception issues-based scenario to illustrate how multiple acts of deception may be detected through multiple techniques for detecting deceit through monitoring intelligence, surveillance and evidence alongside an understanding of individuals' personality, motive and mindset. [108] Qualitative or narrative scenarios are considered appropriate for analysis of complex situations where there are high levels of uncertainty as they enable greater flexibility in adapting to threats and the scenario to be used to illustrate this approach falls within this remit.[109] Presented below is a scenario outlining a potential terrorist incident across multiple sites and how such incidents may be detected through tailored deception detection approaches.

The Scenario

A terrorist incident involving multiple actors in a capital city, for example, London, occurs across multiple locations. The group involved is required to conceal their true aims and motives and operate at a covert level during the planning of their operations, including their target selection and preparation of explosive devices and weapons and ammunition. Following the careful selection of their targets, the group aims to create maximum confusion and distract authorities from being able to respond effectively to the threats posed by them, providing them a greater opportunity to achieve their aims. The initial target selected for a mass casualty suicide-improvised explosive device (suicide-IED) attack was a public shopping center with a large crowd of people, which would create a large amount of media exposure for the group's aims. A second key suicide-IED attack location was a busy shopping street in the center of London. A third location for an attack by suicide-IEDs using automatic weapons was a cinema complex, whilst a fourth location was a popular restaurant. While these attacks are aimed to occur over a short space of time to reduce the emergency services effectiveness in responding to this threat, small explosive devices were also planted at multiple locations around London. These devices were designed to create attention and panic amongst members of the public and draw

[106] Wright, Alex "The role of scenarios as prospective sensemaking devices"
[107] Lena Börjeson, Mattias Höjer, Karl-Henrik Dreborg, Tomas Ekval and Göran Finnveden, "Scenario types and techniques: Towards a user's guide," *Futures* 38 (2006): 723-739; Philip Van Notten, Jan Rotmans, Marjolein van Asselt and Dale Rothman, "An updated scenario typology," *Futures* 35 (2003): 423-443.
[108] Van Notten, Rotmans, Asselt and Rothman, "An updated scenario typology".
[109] Ibid.

emergency service responses away from the actual intended targets. These devices were also planted across a range of locations, which did not actually reflect the aims, or ideology of the group made it harder to ascertain the groups' aims.

Methods of Detection

Intelligence derived from HUMINT, IMINT and SIGINT may be used to identify suspects during the planning stages of the attack. Such identification may occur during target surveillance where individuals may be seen across multiple locations and their non-verbal behavior assessed for potential cues indicative of deceit or concealed intent. Such analysis may be combined with SIGINT where communication between suspected terrorists may be intercepted and analyzed according to linguistic approaches to deception detection and online credibility assessment perspectives. Further, surveillance may identify suspects who are buying materials being used to manufacture explosive devices.

If suspects are intercepted based upon evidence generated from intelligence and surveillance approaches, then further HUMINT may be developed from the use of interviewing techniques. Verbal and non-verbal deception detection techniques can be employed to assess credibility in suspects and compare and contrast their statements with evidence generated from IMINT and SIGINT. In interactions with the suspects, it is important to understand how their beliefs will inform their actions and interview strategies will need to be tailored accordingly. If non-verbal behaviors indicative of deceit are encountered during suspect interviews, suspect's non-verbal behaviors will provide useful guides for practitioner to question further.

In the event that the suspected terrorists are not intercepted, then the terrorist attack may occur and a different approach to deception detection will be required. Surveillance from IMINT sources including CCTV cameras will provide evidence of where each explosion occurs. To minimize casualties, authorities require an effective emergency response where they can distinguish between genuine and distraction explosions. The use of SMEs in identifying the differences between the genuine and distraction explosions will enable the emergency services to allocate their resources effectively potentially reducing the number of casualties. While techniques related to pre-detection and alternative analyses, may enable a more robust response to the threats posed by anticipating the likelihood of an adversary course of action. If the course of an action is more likely to be anticipated, then it may be prevented or detected before the threat occurs.

Conclusion

The current article highlighted a range of techniques that may be used towards detecting deception and applying such techniques whilst keeping an open mind

https://scholarcommons.usf.edu/jss/vol10/iss1/6
DOI: http://doi.org/10.5038/1944-0472.10.1.1528

towards the possibilities of a larger deception may prove useful in detecting strategic deception. To illustrate how a tailored approach to deception detection may be deployed against multiple threats a scenario involving a terrorist attack was outlined alongside potential strategies of how to detect deception at different points across the scenario. While such an approach enables the ability to envisage new approaches to deception detection for practitioners, the approach to deception detection combining behavioral cues to deceit alongside a consideration of personality and motive will require validation both in experimental and real-world conditions. The list of techniques discussed is not exhaustive and it is anticipated that many techniques will be refined over time to produce greater accuracy in deception detection. One key point to note is that deceptive behavior is not generic and attempts at deception will reflect the surrounding aims, culture, and personalities of those individuals involved in large-scale deception and this will differ accordingly between and within organizations involved in committing deception for strategic gain.