JOURNAL OF FORENSIC SCIENCES

J Forensic Sci, November 2010, Vol. 55, No. 6
doi: 10.1111/j.1556-4029.2010.01474.x
Available online at: onlinelibrary.wiley.com

TECHNICAL NOTE

PSYCHIATRY & BEHAVIORAL SCIENCES

Ewout H. Meijer,[1] Ph.D.; Fren T. Y. Smulders,[1] Ph.D.; and Harald L. G. J. Merckelbach,[1] Ph.D.

Extracting Concealed Information from Groups*

ABSTRACT: Lie detection procedures are typically aimed at determining guilt or innocence of a single suspect. Serious security threats, however, often involve groups, such as terrorist networks or criminal organizations. In this report, we describe a variant of the skin conductance-based Concealed Information Test (CIT) that allows for the extraction of critical information from such groups. Twelve participants were given information about an upcoming (mock) terrorist attack, with specific instructions not to reveal this information to anyone. Next, each subject was subjected to a CIT, with questions pertaining to the details of the attack. Results showed that for every question, the average skin conductance response to the correct answer option differed significantly ($p < 0.05$) from those to all other options. These results show that the information about the upcoming attack could be extracted from the group of terror suspects as a whole.

KEYWORDS: forensic science, terrorism, lie detection, polygraph, concealed information test, CIT, Guilty Knowledge Test, network analysis

Lie detection procedures are typically aimed at determining guilt or innocence of a single suspect. Many of today's security threats, however, do not come from individuals, but from organized groups such as terrorist networks or criminal organizations. In this report, we describe a technique that can be used to extract critical information from such groups; and in this way, we help to increase the security of citizens.

This technique is based on the Concealed Information Test (CIT; also known as the Guilty Knowledge Test [1,2]). This test aims to detect the presence or absence of crime-related information in a suspect's memory. In a typical CIT, questions concern crime details known only to the police and the perpetrator, but not to an innocent suspect. With each question, several answer options are presented serially, while psychophysiological parameters, such as skin conductance, are recorded. Answer options include the correct, but also several plausible but incorrect ones (e.g., "Was the victim killed with a … (i) gun, (ii) knife, (iii) rope, (iv) bat, (v) screw driver"). For innocent suspects, all options are equally plausible and will elicit similar physiological responses. However, for a guilty suspect, the correct option is salient and elicits an enhanced response. Thus, consistent stronger physiological responding to the correct answer options indicates knowledge of intimate crime details, from which guilt can be inferred. This use of the CIT is supported by research on the human orienting reflex (3), has good validity (4), and is widely used as a forensic tool in Japan (5,6).

An alternative application of the CIT is the so-called Searching Peak of Tension Test (SPOT [6,7]). This variant can be employed when the correct alternative is not known to the investigative authorities, but rather is the topic of investigation. If that is the case, a series of answer options are presented to the suspect, and the option that evokes the largest response is considered to be the one that warrants further investigation. In this way, the CIT can be used to discover, for example, the location of the body of a murder victim when the perpetrator is known.

In organized crime and terrorism, there are often multiple suspects who are likely to possess the same critical information. The question arises whether this critical information can be extracted by presenting the same questions to multiple suspects. The correct alternative should evoke the largest response in the majority of them. Screening for answer options that, on average, evoke the largest response in a group could then provide a reliable method for determining concealed information unknown to the investigative authorities, for example about a terrorist plan.

Method

Twelve male undergraduate students of Maastricht University (mean age 22.4 years, SD = 2.9) were asked to participate in an experiment. They read and signed an informed consent and received financial compensation for their participation. The experiment was approved by the ethical committee of the Faculty of Psychology and Neuroscience, Maastricht University. Upon arrival in the laboratory, the participant was told that the experiment entailed role playing and that he had to pretend he was a member of a terrorist organization. Next, the participant was given an envelope that contained instruction to go to a bar located inside the university building for a briefing. In the bar, he found an envelope labeled "top secret." This envelope contained the details of an upcoming terrorist attack (target, location, and date), with specific instructions to make sure not to reveal these details to anyone. Next, the participant returned to the laboratory.

Upon return to the laboratory, the participant was told that he was suspected of being a member of a terrorist organization,

[1]Faculty of Psychology and Neuroscience, Maastricht University, The Netherlands.

*Presented at the 18th Conference of the European Association for Psychology and Law, July 2–5, 2008, in Maastricht, The Netherlands, and the 21st Annual Meeting of the Association for Psychological Science, May 22–25, 2009, in San Franscisco, CA.

Received 6 May 2009; and in revised form 10 Aug. 2009; accepted 5 Sept. 2009.

possessing important information about an upcoming attack, and was therefore asked to undergo a lie detection test. After attachment of the sensors, the participant was again reminded to keep any information secret. To increase motivation, participants were promised a €5 reward for beating the test. The test consisted of one practice question and three test questions. The practice question referred to the day of the week and served to familiarize the participant with the procedure. The test questions pertained to the target, the location, and the date of the upcoming attack. All questions were presented on a computer monitor. With each question, six answer options were presented serially, each for 2 sec, with an interstimulus interval of 25 sec (e.g., "On what date will the attack take place?" February 2, October 8, April 20, November 22, March 27, August 15). The first answer option presented was never the correct one and served to absorb novelty orienting responses. The remaining five answer options were presented in random order. Participants responded to the presentation of each answer option with a verbal "no." The order of the questions was determined by a balanced latin square (8). All testing took place in a sound-proof laboratory, and participants were monitored from a control room by means of a video surveillance camera and a microphone.

Skin conductance was measured in microsiemens (μS) using a 24 bit DC 0.5 Volt system (Contact Precision Instruments, London, U.K.) with a sampling rate of 60 Hz. Two Beckmann silver/silver chloride (Ag-AgCl) electrodes (8 mm in diameter) were placed on the medial phalanges of the first and second fingers of the participants' nondominant hand. Electrodes were filled with isotonic electrode paste (0.9% NaCl). Skin conductance responses (SCRs) were computer scored as the maximum positive deflection between 1 sec and 5 sec following stimulus onset. To eliminate individual differences in responsivity, within-question standardized scores were computed by subtracting the mean of all five responses (excluding the buffer option) from the response to each answer option and dividing that by the standard deviation of all five responses (9). Three separate univariate repeated-measures ANOVAs were carried out on these z-scores, one for each question. The original degrees of freedom are reported with the Greenhouse-Geisser adjusted *p*-value and Greenhouse-Geisser Epsilon value (ε).

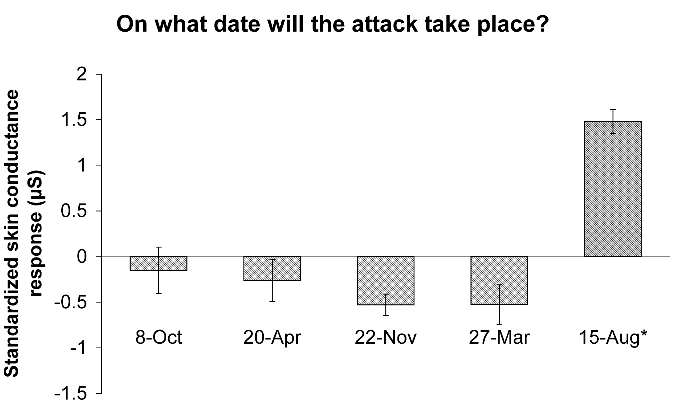

FIG. 1—*Mean standardized skin conductance response to answer options for the question about the date of the upcoming attack. *Denotes the correct option. Error bars represent standard errors of the mean.*

Results and Discussion

All three repeated-measures ANOVAs performed on the SCRs elicited by the different options revealed a main effect (date: [$F_{4,44} = 14.5$, $p < 0.001$, $\varepsilon = 0.66$], city: [$F_{4,44} = 14.5$, $p < 0.001$, $\varepsilon = 0.73$], target: [$F_{4,44} = 5.46$, $p = 0.004$, $\varepsilon = 0.75$], for an example see Fig. 1). *Post hoc* comparisons showed that for every question, responses to the correct answer option differed significantly ($p < 0.05$) from those to all other options, while, with one exception, responses to incorrect answer options did not differ from each other (see Table 1).

These results show that with the CIT, one can extract critical information about an upcoming terrorist attack from a group of terror suspects. In this way, this network variant of the CIT (N-CIT) may help to prevent terrorist attacks, but it may also be useful in revealing the location of drug laboratories, weapons or persons, or identify details of money laundry operations. This way, it may help to increase security and may serve as an alternative to controversial interrogation techniques.

Even though the current experiment was performed under ideal conditions (e.g., all participants possessing the information), our results likely generalize to the field. CIT research typically shows very large effect sizes. Mock crime studies that best mimic real life situations have found a Cohen's *d* of 3.12 (4), and an estimation of Cohen's *d* for the current study is 2.45 (for the estimation procedure see [10]). Such high effect sizes create leeway for use under suboptimal circumstances, like a smaller group of suspects, or a group of suspects in whom not everyone possesses the critical information. In any case, the N-CIT can be used as a challenge test. If no differences are found, this should be interpreted with caution. If one option does differ, however, further investigation into that option is warranted.

Investigative authorities already put considerable effort into mapping criminal networks (11). Additionally, the N-CIT requires that plausible answer options are limited in number. In some cases, the number of available options may be naturally limited; in others, the available options need to be reduced by police work. If this can be achieved, the N-CIT may prove a valuable tool for information gathering from groups of suspects.

TABLE 1—p-*values for the* post hoc *comparisons for the three questions.*

Question	Date					Location					Target			
	20 Apr	22 Nov	27 Mar	15 Aug*		Den Haag	Eindhoven	Utrecht	Rotterdam*		C&A	HEMA	H&M	V&D*
8 Oct	0.80	0.22	0.32	0.001	Den Bosch	0.18	0.75	0.05	<0.001	Bijenkorf	0.24	1	0.90	0.02
20 Apr		0.33	0.52	<0.001	Den Haag		0.44	0.52	0.001	C&A		0.22	0.14	<0.001
22 Nov			0.99	<0.001	Eindhoven			0.13	<0.001	HEMA			0.88	0.01
27 Mar				<0.001	Utrecht				0.001	H&M				0.002

*Denotes the correct answer.
The different locations represent large cities in the Netherlands. The targets all refer to department stores that can be found in these cities.

References

1. Lykken DT. The GSR in the detection of guilt. J Appl Psychol 1959;43:385–8.
2. Lykken DT. A tremor in the blood. New York, NY: Plenum Press, 1998.
3. Verschuere B, Crombez G, De Clercq A, Koster EH. Autonomic and behavioral responding to concealed information: differentiating orienting and defensive responses. Psychophysiology 2004;41:461–6.
4. Ben-Shakhar G, Elaad E. The validity of psychophysiological detection of information with the Guilty Knowledge Test: a meta-analytic review. J Appl Psychol 2003;88:131–51.
5. Hira S, Furumitsu I. Polygraphic examinations in Japan: application of the guilty knowledge test in forensic investigations. Int J Police Sci Manag 2002;4:16–27.
6. Nakayama M. Practical use of the concealed information test for criminal investigation in Japan. In: Kleiner M, editor. Handbook of polygraph testing. San Diego, CA: Academic Press, 2002;49–86.
7. Raskin DC. Polygraph techniques for the detection of deception. In: Raskin DC, editor. Psychological methods in criminal investigation and evidence. New York, NY: Springer, 1989;247–96.
8. Williams EJ. Experimental designs balanced for the estimation of residual effects of treatments. Aust J Sci Res 1949;2:149–68.
9. Ben-Shakhar G. Standardization within individuals: a simple method to neutralize individual differences in skin conductance. Psychophysiology 1985;22:292–9.
10. Meijer EH, Smulders FTY, Johnston JE, Merckelbach HLGJ. Combining skin conductance and forced choice in the detection of deception. Psychophysiology 2007;44:814–22.
11. Borgatti SP, Mehra A, Brass DJ, Labianca G. Network analysis in the social sciences. Science 2009;323:892–5.

Additional information and reprint requests:
Ewout H. Meijer, Ph.D.
Faculty of Psychology and Neuroscience
Department of Clinical Psychological Science
Maastricht University
P.O. Box 616
6200 MD Maastricht
The Netherlands
E-mail: eh.meijer@maastrichtuniversity.nl