Journal of Military and Strategic Studies, Spring 2005, Vol. 7, Issue 4.

SEARCHING FOR SECURITY BY PREDICTING RISK

Alvin Harvey Shapiro, Centre For Military And Strategic Studies

The Current Situation

The terrorist attack on the United States of America that happened September 11, 2001 was a great shock to our neighbours to the south. At first, dazed, the U.S. effectively rallied by gathering its storehouse of newly-upgraded weaponry; and, then applied these “smart” weapons to Afghanistan and Iraq.

Simultaneously, at home, actions were taken to defend American soil. One significant action was to create a special department labelled, “The Department of Homeland Security”.

Similarly to other mighty nations, existing before the United States emerged as a super power, the maintenance previous nations’ supremacy focused primarily upon their superior technology. Regarding the United States, an immediate effect of their rapid response military technology (called “Shock and Awe”) was to deploy smart-bombs, laser-guided which were – to effectively achieve a counter offensive and temporarily numb the identified aggressors – much as had occurred to the U. S. on September 11th.

However, similarly to the recuperative powers of America, the pummelled enemies regrouped and are today counterattacking. These nations’ preferred weapons of choice: are variously labelled as, “terrorism” or “insurgency”. In remote Iraq and Afghanistan, distant from the United States, terrorists and “insurgents” are embarrassing the armies of the United States (and its allies) by their successes. This form of insurgency, outside of America, is unable to be contained by even the newest technology. Such involve smart bombs, photographing drone aircraft or "gatling—gun," bristling Humvees. Technology alone, it may be concluded, appears to be unable to contain complex, planned and formulated disruptive human behaviour.

Within the United States itself it appears that this technology-based mentality has similarly taken over the thinking of that country's self defence system. Apparently, highly influenced by advances in medical computer technology and biogenetic research, digitized electronic techniques are being deployed as a "comprehensive" terrorist counter weapon through the many portals of entry into the United States.[1]

Retinal structure ID is being used at airports, light-sensitive finger printing is in use at border crossings, and digitized photographing operates at every custom border guard's imposing kiosk. The underlying assumption appears to be, that if applied effectively, the smart camera, the fingerprint sweat, the back of the entrant's eyeball, will match a risk Macro at Homeland Security's web bank. This, in turn, "should" instantly ID the troublemaker who may then be quickly apprehended. Hence, technology will have saved the country from an imported threat, as it was designed.

This description, placed before the reader, is essentially an exaggerated scenario of what is eventually supposed to take place. It mirrors current reality as it is being enacted. A high tech reliance upon sophisticated electronics is being put into operation without any real check upon its effectiveness. In security circles there is every appearance that electronics is supplementing any and all other consideration of alternative risk identifiers. The point here is, that decision makers, responsible for

[1] Quoted in U.S. Department of State, "Homeland Security Chief Launches New Border Entry Procedures," January 5, 2004, http://usinfo.state.gov/gilArchive/2004/Jan/05-19561.html, accessed on
January 15, 2005.

security, are placing billions of dollars into unproven technology. As such, in the rush to implement unproven technology it is this author's opinion, that the electronic technocrats may be placing the United States into a High Risk position. Fundamentally, terrorist risk may be increased, because <u>none</u> of this digitized technology has any predictive power on its own, at all.

Neither instant photographs, finger sweat patterns, retinal scanning nor DNA sampling can make any risk prediction to the country or its citizenry - <u>unless</u> the person being identified, has been pre-identified through some form of background check, as "having done something wrong" "in some way", "somewhere" before. Their past actions may involve having been associated with wrong groups, having been in the wrong area at the wrong time, or supporting a suspicious cause. Without a single exception, though, no known technological device currently in use, without a prior "record" existing somewhere, can forecast, can foretell, how someone, anyone, will potentially misbehave or wreak havoc once they have entered the country. That is, the high-tech. systems can only "predict" wrong behaviour, if some previously existing link of deviancy exists in a data bank somewhere. Thus, all of the current technologies now in use are ***reactive*** in nature. None are ***proactive.***

Some Relevant History

Many billions of dollars and resources, under the shared dread of another attack, are currently being allocated into installing impressive electronic boxes in varied locations and endorsing entire unproven systems. The installation of many varied, newly minted security systems are, in the main being installed without serious examination of their actual capabilities. Indeed, there is a perception that some corporations are being opportunistic and may be reaping advantages from the public purse. Many products are being promoted as a reliable and valid way to predict future human actions, when in fact; no independent evidence, whatever, exists for that assertion.

Alternatively, a militarily proven method of predicting human actions has existed at least since 1904. And, astonishingly in these times of peril, it seems that this methodology is being very largely ignored within the security context. In 1904, a psychologist named Professor Spearman invented a way to objectively determine measure and predict a person's ability to learn. His invention became known as an I.Q. test – where I.Q. meant "Intelligence Quotient".[2]

Spearman's invention was so strongly predictive about learning on-the-job (and reducing risk) that in World War I (and later, WW II) the United States Army had all new recruits take their Army – Alpha or Beta tests, at the time of the recruits' enlistment. Subsequently, a large cohort of military studies have shown that general tests of ability will have up to an 80% accuracy rate of job success, be it for Nuclear Weapons Specialists, Vehicle Maintenance Personnel or (tellingly) Security Police.[3]

While over the years, I.Q. tests have been criticized and challenged from many different sources; this way of predicting human learning has withstood all the varied onslaughts attacking its credibility. In proven actual fact, an I.Q. test, properly

[2] C.S. Spearman, 'General Intelligence Objectively Determined and Measured', American Journal of Psychology, 1904, 15, 201-209.

[3] M.J. Ree & J.A. Earles, 'Differential Validity for a Differential Aptitude Test,' 1990, Brooks Air Force Base, Texas: Air Fare Systems Command.

administered, remains the gold standard of appropriate employment, training and personnel selection.[4]

As a side issue of measuring various life-related skills sets, testing for honesty and security has similarly been seriously attempted. Those attempts, however, have historically taken a somewhat different course. That somewhat different course, which was readily embraced in the past, and failed, may be an ominous signal of what may unfold in the electronically based risk prediction methodology. Unlike the paper-and-pencil I.Q. approach, testing for "honesty" at sensitive security sites began with the invention of the polygraph machine.

These machines, the avant-garde of technology of their time, were merchandised as foolproof "lie detectors". Simply by proxy, bad behaviour in the workplace, or rather risk behaviour prediction, fell into the hands of technicians who operated large impressive vacuum tube powered polygraphs. This "lie detector" approach relied upon electrical signals recording employee responses to questions. The polygraph was, at first, used extensively, in industry and forensics, however, by 1988, after extensive investigation, these electronic behemoths had been banished. That occurred through the Employee Polygraph Protection Act enacted by Congress.[5]

Polygraph security testing was outlawed, because, on the one hand, it consistently failed to screen out high-risk employees. On the other hand, it, unfortunately, tended to label many good and honest workers as liars and thieves. Polygraphs were also very costly and time-consuming. They were, furthermore, used

[4] R.J. Hemstein & C. Murray, 'The Bell Curve: Intelligence and Class Structure in American Life, New York: The Free Press, 1994.

[5] U.S. Congress, The Use of Integrity Tests for Pre-Employment Screening, Washington D.C.: US Government Printing Office, Office of Technology Assessment, 1990.

mainly on employees who were already under suspicion for stealing, or other unacceptable workplace behaviour.

As a result of the mere threat of having to undergo a polygraph test, an understandably very nervous, yet totally innocent employee, could negatively bias the machine. Then, once the printout graph was viewed, that hapless worker would be "proven" as guilty. Thus, because of the unreliability of the polygraph, with its high costs, and equally high misidentifications, a renewed interest to re-examine security issues through paper-and-pencil questionnaire approaches began to emerge.

Within a security context, this paper-and-pencil approach actually had its root beginnings in prison settings. Its purpose was to try and predict disruptive criminal actions of inmates by determining their risk potential at the time of arrival. Co-incidentally, questionnaire approaches were also developed to accurately identify severely mentally ill people for appropriate mental hospital admissions.[6] Outside of these institutions, however, momentum from industry grew as a desire to control theft, violence and sabotage. As a result, paper and pencil testing was soon being applied to new or suspicious employees in the workplace. As a result, when the late 1980's arrived; approximately 50 different "Integrity Tests" (tests of honesty) were being marketed, all purporting to measure various aspects of personnel / employee risk.[7]

The previous debacle with employment polygraph testing, however, resulted in a much more cautious approach by guardians of the public trust. The honesty tests were not immediately embraced. Sceptical about the tests' commercial claims alone, the

[6] For example see: C.D. Webster, K.S. Douglas, D. Eaves and S.D. Hart, HCR-20: Assessing Risk for Violence – Version 2. Burnably, B.C., Siemens Fraser University Press, 1997.

[7] William G. Harris presentation to the Management & Organizations Dept, College of Business, University of Iowa, 1997, The Development, Marketing and Use of Integrity Tests in the American Workplace.

United States government subjected the new non-electronic questionnaires to extremely vigorous scrutiny, by a wide and carefully chosen panel of experts. The major investigation was carried out by the U.S. Government Office of Technology Assessment in 1990. Their subsequent report, which was submitted to the United States Congress, essentially stated that while paper-and-pencil tests of risk assessment were then, a work in progress, they were at that time, better than, and different from, the inaccurate electronic polygraph device.

What is Ahead?

Still concerning ourselves with this paper-and-pencil approach, since the late 1990's a more tightly run ship has appeared on the horizon. This has come about in several ways: rigorous testing guidelines were developed to be followed; better employee sampling was required, and the application of more sophisticated statistical procedures was deemed essential.[8]

It is as a result of these application rules that routinely now, "risk assessment" is incorporated into well-researched personality tests and "integrity tests" for employees. The potentially pejorative words such as "honesty" and "integrity" used previously, for example, have largely been renamed as "conscientiousness" or "dependability".

How such tests account for intentional or unintentional "lying" has been well worked-out. "Lying" itself falls under a general heading of "Response Bias" in the risk assessment literature. It recognizes such factors as Social Desirability or "faking good"

[8] American Psychological Association, 1991, Questionnaires Used in the Prediction of Trustworthiness in Pre-Employment Selection Decisions: An APA Task Force Report. APA Task Force on the Prediction of Dishonesty and Theft in Employment Settings. Washington, D.C.

and includes the consistency of how the same question presented from different angles is answered.

When even a sophisticated person answers apparently straight forward questions, evidently of little consequence, so as to appear overly virtuous, their subset of these answers is statistically compared to others who are “known” to be truthful in developing the norms for comparison. Under such circumstances, if a statistical difference results, then the validity or truthfulness of all the rest of this person’s answers is cast in doubt.

Yet further, psychological questioning may be presented either in picture or “inkblot” form. Such are called “projective techniques” and have been refined over many years. Here too, statistical comparisons are made to pre-selected truthful responders. Should a test “faker” produce a statistically unusual response, their reliability as an honest responder will similarly raise suspicion.[9]

It should then follow, that once an individual is “tagged” as having answered in an unusual way, that other investigative techniques are then employed. These will likely consist of in-depth personal (forensic) interviewing and gathering of collateral information from external sources, including family and friends, about this person’s history and past behaviour.

[9] It needs to be stated that every test has room for a margin of error. In other words, with extensive training, a person can actually “beat” many tests. The likelihood of that occurring in projective tests is, however, less, than in questionnaire formats. In projective testing, rarely would someone know what a correct answer should be because rehearsals of the “best” projective answers is very difficult. Projective tests tend to operate at an emotional level, and at that level, conscious censorship can rarely guide “correct responses”. Fundamentally, very few people know what answer to give to different inkblots. It has been well documented that such inkblot and picture-based testing can be both reliable and valid in detecting statistically rare responses.

Although risk assessment at the present time has not yet reached the predictor levels which are as robust as those of I.Q. tests, they are improving. It is gradually becoming apparent in industry and in security areas that risk-assessment tests are now credible, and, to a practical degree, helpful. For example, it is now known through techniques of Meta-Analysis (the combined analysis of many tests) that risk assessment test procedures, truly predict risk.[10] That very important point, though based upon valid scientific procedures, is currently being almost totally ignored by those within the sway of the very powerful technical lobby.

Although it is actually the case that potentially disruptive behaviour by individuals can be predicted to some degree by asking the necessary predictive questions, in the realm of security such questionnaires, to the author's knowledge, are not even being generally attempted. It is a fact that even without background checks, such procedures may be useful, if only for screening purposes. Nonetheless, the post 9/11 U.S. government and industry seems to be repeating the same mistake of history. There is every appearance of a desperate dash to deploy unproven electronic gadgetry again. Will such actions concerning the prediction of human behaviour be a contemporary repeat of previously discredited polygraphy in a newly packaged form?

Even though a very great amount of evidence exists that carefully designed I.Q. tests and related integrity testing predict actions in the field by use of its own military, that potentially life-saving history in the security testing sphere has, until quite recently been ignored.

[10] F.L. Schmidt & J.E. Hunter, Practical and Theoretical Implications of 85 years of Research Findings, 1998, Psychological Bulletin, 124, 262-274.

In January of 2005, under the auspices of the Executive Office of the President of the United States, The National Science and Technology Council produced a report. That report is entitled, "Combating Terrorism: Research Priorities in the Social, Behavioural and Economic Sciences."

The purpose of this report is to formulate research priorities for the 'SBE' sciences to address issues related to terrorism and terrorist attacks.[11]

The group representing this initiative is a somewhat late, but necessary step in the development of Homeland Defence in the United States. Its potential is designed to combat terrorism, and is the principal means for the President to coordinate science and technology policies across the (U.S.) Federal Government. It is a good first-start in coordinating risk assessment behaviours and internal vulnerabilities.

A strong likelihood exists, that from this group, various questionnaires predicting risk will emerge via the internet, or face-to-face in various contexts. These may include their use at border entries or other high security sites. There is some probability that this approach may unearth terrorist "sleeper cells" whose members may be local and have no discernable criminal background at all. These risk factors which are identified may also have no relationship to nations of origin whatsoever. The risk factors identified may be non-national, non-racial, non-color, non-religious and totally person-centered. In order to enhance security all the risk assessment may call for in action, is simply greater surveillance, once a pre-specified level of risk is reached. This may be carried through "benignly" and with discretion. It will be important for the preservation of

[11] Executive Office of the President of the United States. Report of the NSTC Subcommittee on Social, Behavioural and Economic Sciences, Combating Terrorism: Research Priorities in the Social, Behavioural and Economic Sciences. American Psychological Association, NSTC Report.html, April 2005.

democracy that no potential “blacklisting” be initiated. This can be avoided if foresight is utilized and safeguards are set into place in advance to protect human rights.

The Canadian Security apparatus may do well to compliment the efforts of our United States’ neighbours. So far Canada has been extraordinarily lucky not to be targeted by terrorism, as of late. But how long is our “luck of the draw” going to last? We are clearly at risk with our troops in Afghanistan. The concept of generating risk assessment protocols appears to be a logical first step in this proposal to develop a North American screening shield. Directly arising from this I suggest that some of our Canadian social scientists begin to seriously consider what we can now contribute in that regard, given our collective expertise.