***Emotional Recognition Technology (ERT) and Psycho-Physiological Devices: Implications for Combating the Insider Threat in the Cyber Domain***

*By Ethan S. Burger[[1]](#footnote-1)*

Many organizations are examining how better to combat the ‘insider’ threat. *See* <https://www.ncsc.gov/issues/ithreat/index.html>. Cyber operates as a force-multiplier. It dramatically increases the potential for harm caused by insider attackers. <https://www.ncsc.gov/issues/cyber/index.html>; *see also* <https://ccdcoe.org/sites/default/files/multimedia/pdf/Insider_Threat_Study_CCDCOE.pdf>

Members of the national security community (including academia, businesses, government, and research institutions) are seeking to develop better practices to mitigate against the insider threat. *See* <http://www.cert.org/insider-threat/research/database.cfm>? <https://www.ncsc.gov/issues/docs/Common_Sense_Guide_to_Mitigating_Insider_Threats.pdf> and <http://www.cert.org/insider-threat/publications/index.cfm>.

In general, it would seem that there are no technological quick fixes to improving cyber-security. Nonetheless, there may be new tools around the corner, which if properly integrated into comprehensive cyber-defense systems, *could* allow organizations to improve their ability to withstand cyber-attacks and sabotage. Many persons with responsible for their organizations’ security will want to see if they can reduce their risk of cyber-attack.

For example, Emotional Recognition Technology (ERT) and Psycho-Physiological tools could conceivably pay vital roles in allowing organizations to improve their cyber-defenses. *See e.g.* <http://developer.affectiva.com/> and <http://isyou.info/jisis/vol6/no1/jisis-2016-vol6-no1-02.pdf>.

On the other hand, it might be reasonable to expect that the use of these technologies reduces organizations’ cybersecurity for many reasons, as was the case with polygraph machines. Polygraph machines largely measure anxiety. The use of polygraph examinations for security purposes results in numerous false negatives and false positives the results if which can be very real and undesirable.

Consequently, persons who are trained to ‘beat’ polygraph machines (as well as persons lacking a strong sense of conscience, e.g. psychopaths), are likely not to be found to be deceptive. This outcome leaves organizations exposed to persons inaccurately deemed to be reliable. False positives can lead to the purge of well-trained personnel. Also, a culling might lead to undesirable secondary effects. This situation is difficult to remedy quickly and in a cost-effective manner.

The colleagues of the individual who was ‘forced out’ of their job due to a ‘bad’ polygraph experience as likely to be troubled by the situation. They may decide to seek new employment since they fear being wrongfully found to be potential security risks based on the polygraph ‘test’ results. This situation also will rob organizations of vital expertise. Also, in some cases, organizations may be held liable for wrongful termination.

It would seem to reason that the underlying scientific basis for these machines use in certain situations (employment screening and event investigation) is not based on sound science. If the justification for using polygraph examinations as part of a personnel security system is flawed, it would seem that the use of more ‘accurate’ tools to monitor human behavior and responses to stimuli would be inappropriate. *See* <http://www.apa.org/research/action/polygraph.aspx>, <http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=10420>, and <https://www.fas.org/sgp/crs/intel/RL31988.pdf>.

What are you thoughts on the new technologies?

++++++++++++++++++++++

Only comment worth noting:



**Don't Look for Guilt - Instill Guilt**

* Published on August 14, 2016
* LikedUnlikeDon't Look for Guilt - Instill Guilt

[**10**](https://www.linkedin.com/pulse/dont-look-guilt-instill-raymond-parks?trk=hp-feed-article-title-like)

* Comment

[**1**](https://www.linkedin.com/pulse/dont-look-guilt-instill-raymond-parks?trk=hp-feed-article-title-like#comments)

* ShareShare Don&amp;#39;t Look for Guilt - Instill Guilt

**1**

**[](https://www.linkedin.com/in/raymond-parks-a755666)**

[**Raymond Parks**](https://www.linkedin.com/in/raymond-parks-a755666)**FollowRaymond Parks**

Cyber/Physical/Human Systems Security Consultant

This is a response to a posting by Ethan Burger on the Cyber Weapon Global Discussion Group titled "Emotional Recognition Technology and Psycho-Physiological Devices".

These technologies try to use machine vision and learning to tackle the huge scale of watching insiders constantly to detect misbehaviour.  The technologies look for signs of guilt.  The problem with this is that the observed are all humans and not consistent about showing signs of guilt.  Some show guilt when there is none, some show guilt for unrelated behaviour, and some don't show guilt when misbehaving.  Ethan even compares the technologies to polygraphs - which have high rates of false positives and false negatives.  When you change the scale of operation from roughly annual polys to hourly face scans or typing changes - you're looking at an overwhelming number of "security events" to investigate.  At best you'll end up like the cell phone police at Sandia Labs - it's a work process with a checklist, not an investigation.  At worst, you'll turn the software off, try to get a refund, and discover you've spent millions on something you can't use.

Behavioural Economics, e.g. Predictably Irrational by Dan Arielly, points out that the purely psychological reminders of good behaviour are probably more effective at far less cost.  A program of simply reminding people of their responsibility and that they are being monitored costs less (if, in fact, the organization is monitoring activity) and will prevent all but the most sociopathic from misbehaving.  The book mentions a study in which merely reading the "Ten Commandments" resulted in less "criminal" behaviour when tempted during a simple task.

The reminders need to be varied - everybody clicks through the standard warning page when logging in.  Keep the page for legal reasons - but supplement it with alert emails, reports of phishing scams caught, reports of porn watching caught, informative articles on cyber security incidents (properly anonymized), and so on.  Publicize the work your cyber-security staff are doing without giving away TTPs.  On Patch Tuesday (whenever it falls in your organization - it better be within the month) announce the security changes and how they will prevent attacks (and misbehaviour).  Slip in a little reminder to the employees to patch at home, particularly if you let them do any work from their home systems.  The same goes with mobile devices - I have yet to see an organization that patches business-owned devices in a public way and no-one seems to help users patch their own devices even in a BYOD situation.

We all know that employees will begin to tune out emails and internal web notices that are not interesting and take away their time.  So you need to get your communications/media folks into the process.  Make the news interesting and don't spam are the keys to this type of activity.  Don't let your reminders become routine - send them out at different times until you know you're getting the hits that reflect real interest.  Then, and only then, can you give your audience something to look forward to receiving at a certain time (probably no more than weekly).  You can get some good advice from Randy Cassingham, who's had a continuous, successful email list going since 1996, at [Emailified.](http://emailified.com/)

For the cost of few hours of your security team's time a week, some more hours of your communications/media folks' time, and some electrons, you can keep your insiders wondering if they will get caught.  Perception is the name of the game, here - when I was with IDART, we modeled insider adversaries as very risk conscious.  For all adversaries, if the risk of not succeeding is not acceptable, they won't perform the attack.  Most insiders include the risk of getting caught in that equation - it's part of their definition of success.  You can deter all but the most driven or sociopathic insiders - and those you should be catching through your current detection methods.

1. Ethan S. Burger is a Washington-based international lawyer and academic who specializes in cybersecurity, transnational financial crime, corporate governance and Russian matters. [↑](#footnote-ref-1)