



Penetrating Bomb Maker Networks and Winning the IED Conflict

Bridging gaps between leadership, operators, and technology to achieve a common objective.

By Grant Haber

Improvised Explosive Devices (IEDs), the terrorist's weapon of choice, continue to pose the greatest threat to global security, the global economy, and to the men and women serving in Afghanistan, Iraq, other areas of sustained conflict, and the local communities within those countries.

WHY? IEDs cost very little to make, the ingredients are sold in open markets, the recipes are found on the internet, and IEDs are an effective tool for killing coalition forces and civilians. What is commonly overlooked is that successful IED attacks kill more than coalition forces and civilians; they kill the confidence and trust of the local population which is a vital component for helping coalition and local police forces identify and penetrate *Bomb Maker* networks. Given the current economic times, we must also be cognoscente of the true costs of borrowing money to combat this asymmetrical threat.

Coalition and local police forces are doing a remarkable job combating insurgents and terrorists; given the tools they have. Government and military entities are focusing most of their efforts, and allocating a large portion of their resources, toward standoff explosives detection. The importance and value of standoff detection is understood, though while the perfect solution to detect and counter IED threats from a safe standoff distance is being developed, we must recognize that lives of service members, support contractors, and civilians will be saved if leadership allocates more resources toward effective penetration of the *Bomb Maker* networks.

If adequate resources can be allocated to identifying, capturing, or otherwise

neutralizing those who manufacture, store, or emplace explosives for the insurgence ("The Network"), the benefits are realized in combat intelligence that allows for successful operations to defeat them. Restoring the support of local populations stems from the improvement of

Everyone fighting terrorism has a responsibility to report, and provide feedback, that will allow leadership to make informed decisions.

their livelihood. But more importantly, their support comes from the leadership which seeks to effectively manage the sustained conflicts they are forced to live within. In the end, it is up to leadership to understand and act upon the knowledge that detecting and defeating The Network, are proactive measures that will result in a reduction of IED attacks, and bring us closer toward winning the IED Conflict. This is vital strategy to enabling allies and coalition forces to win the Global War On Terrorism.

The mission at hand, "Penetrating *Bomb Maker* Networks and Winning the IED Conflict" can be achieved if all involved take responsibility for the results within their available means. First, it is important for the user community to start spelling the facts out to their leadership. Given the diverse responsibilities of

government and military leadership, not to mention the political pressures they endure, leadership could unknowingly overlook the obvious and indirectly contribute to more casualties, or life-changing injuries. When in doubt about confronting leadership with the tools that are needed, wanted, and work, remember the following, "*Leadership has your best interest at heart, though as men and women on the front lines of insurgency and IED attacks, it is your responsibility to make it clear to your leadership what is working, what is not, and what is available to close the existing gaps.*"

It is equally important to keep in mind that leadership has allocated extensive monetary and human resources for explosives detection equipment and training. As far as they are concerned, they are doing their part to provide operators with the tools necessary for penetrating the *Bomb Maker* networks. Failure to communicate equipment shortcomings directly to your leadership may contribute to your receipt of additional inadequate equipment to combat the evolving IED threats.

As discussed, "Penetrating *Bomb Maker* Networks and Winning the IED Conflict" can be achieved if the preventative measures taken, and information gathered, is turned into actionable intelligence. One thing not to overlook, is the efficiency and reliability of the tools operators are using on the front lines. Leadership is often blind to the true effectiveness of tools issued to operators, because they are not the ones using them. To overcome this disconnect, the internet can provide a forum to improve the feedback that operators provide to all levels of leadership. By enabling operators to provide first-hand feedback,

leadership can implement strategies and make changes that address the obstacles encountered by front line operators.

Everyone fighting terrorism has a responsibility to report, and provide feedback, that will allow leadership to make informed decisions.

Before covering tactics, techniques, and procedures, there are several easy to verify facts you need to know, and to make very clear to decision makers. Divining Rods are as impractical as a coin toss, when it comes to determining if explosives, or an IED, is present. Sniffer technologies, also known as vapor sampling systems, where direct contact of the surface, item, or object being analyzed is not required, cannot detect all threat explosives, they commonly false negative (*fail to detect*) on trace amounts of low vapor pressure explosives such as RDX, HMX, and PETN, via non-contact vapor sampling, most become overwhelmed by bulk explosives in the field, and the operational challenges for sniffers in harsh environments are numerous. Raman-based systems are a useful chemical identification tool, though they cannot detect trace quantities of explosives.

Bottom line, one size does not fit all when it comes to explosives detection, and though it's convenient to create the perception of security by waving around a magical wand or device that analyzes vapors, false negatives will continue to provide an edge to terrorists, and a steady decline in the confidence of those who expect results under your watch or leadership.

As a bomb technician, you may be thinking, "What do explosives detection devices have to do with me?" Before you stop reading, I'm sharing this with you because you can start articulating the effects of an IED, to someone that likely makes decisions from behind a desk. Your voice to steer decision makers toward outfitting service members, police, first responders, checkpoint screeners, etc., with effective tools that will detect all threat explosives regardless of type or amount of explosives, operational environment, or user experience will save lives. It will also limit your call outs for nuisance alarms. Though it's clear a chain of command usually makes it dif-

ficult to debrief the decision makers, failure to start working through the barriers to your leadership will indirectly fuel a steady increase in IED attacks.

Swipe sampling, also referred to as swabbing, though perceived to some within various government and military leadership positions as archaic, and too burdensome for most screening applica-



Detecting the Bomb Makers before this vest is assembled and strapped to a suicide bomber is vital to saving lives.

tions, is the only effective means for collecting trace explosive residue. According to independent testing, and a survey of commercially available explosives detection technologies and equipment funded by the U.S. Department of Justice, and documented in a report published by Sandia National Laboratory, "When working with low and medium pressure explosives at room temperature, more explosives materials is contained in a fingerprint than would be present in a liter of air saturated with vapor (by a factor of 1,000 to 1,000,000)." "Thus, for low and medium pressure explosives, explosives detection is usually based on particulate detection."

As the user community has learned through extensive trial and error, collecting explosive particulates through swipe, or swab sampling will only provide a benefit if the explosives detector that will be analyzing the sample has merit. Collection of explosives particulates via swipe

sampling will provide no benefit to operators if the detector analyzing the sample cannot function in its operational environment, or it will not detect the type of explosives present.

Things to consider before recommending any explosives trace detector that can analyze particulates include:

- Can the device detect every threat explosive on your requirement's list?
- Does the detector require a lengthy warm-up time, making it impractical for your mission, or is it ready to analyze samples with the flip of a switch?
- Does the detector require recalibration as ambient conditions change, or is no calibration required?
- How much initial operator training is required, and if they don't use the detector on a regular basis, will they likely require retraining?
- Is the detector prone to false positives, *aka* nuisance alarms? And if so, from what?
- Does the detector perform equally well in hot, cold, humid, dry environments?
- Will the detector become overwhelmed, or clogged, after analyzing a bulk explosive, or after a positive detection of trace explosives residue?
- How quickly can subsequent tests be conducted after a positive detection?

These are only some of the questions that should be asked and answered to the satisfaction of the user community, prior to implementing wide-scale deployments for any explosives detector.

As members of the user community, you have to understand the challenges your leadership is facing. They have allocated a great deal of resources to equip their people with what they believed to be the best explosives detection equipment. Many of these decision makers have based their decisions on test data from labs, and/or familiarity with widely known explosives detection equipment that has been in service for many years. As the casualties, injuries, and IED attacks rise, the political inquiries and pressures increase, and in turn, more of the same equipment is deployed.

Though it is understood that bypassing a chain of command to debrief leadership is generally against protocol, know there are leaders and decision makers ready, willing, and capable of doing what is necessary to win if they have a clearer understanding of why operators have little to no confidence in the detection equipment issued to them. If leadership was better informed why standard issue equipment was being shelved, or remains hung up in depots waiting on service, or is ineffective at operating in the environments operators are deployed, or is unable to detect certain threat explosives operators continue to encounter, etc., you may quickly come to realize they are willing to issue operators more suitable equipment.

The new IABTI member tested, member recommended program is an ideal resource for vetting explosives detection equipment and sharing the strengths and weaknesses of the same throughout the user community and with government and military leadership.

Bottom Line: When military service members, police forces, first responders, etc., are equipped with tools that will reliably detect threat explosives off any surface or object, and without false positives, confidence is quickly gained by the operators and penetration into the *Bomb Maker* networks becomes attainable. When it comes to explosives detection, one must never lose sight of the tradeoffs associated with speed, and the method of sampling, versus reliable detection. A faster, or more convenient, analysis methodology that misses X, Y, and Z explosives can and will continue to be exploited by terrorists. Random sampling with reliable detection is a more responsible approach than 100% sampling, when it is understood that certain threat explosives cannot be detected.

For the operators that have lost confidence in the ability to utilize field explosives detection equipment to aggressively and effectively penetrate *Bomb Maker* networks, my advice is the following: "Reach out to other IABTI members and

share your successes and failures, then clearly articulate the facts directly to your leadership." As the financial costs, casualties, and life-changing injuries continue to rise, your leadership will continue to face increased scrutiny. A direct call, or email, to your leadership is timely. Facts cannot be lost in translation, and either may just be the opportunity you and your leadership have long awaited to help each other achieve a common objective.

In closing, remember this... what you know, learn, and share does matter, despite what you may believe. In addition, winning wars and saving lives are collective efforts between leadership, operators, and the technology they utilize.

Grant Haber has been an avid security advocate for over 15 years. In March 1995 he founded American Innovations, Inc., which originally aimed to alleviate security needs of homeowners, and soon thereafter shifted toward proactive homeland security and defense related initiatives. For 12 years he served as President and CEO, and now serves as the company's Vice President.

The World's Finest EOD Wireless System

MARK
 700EDU

- > Continuous handsfree communications with full duplex operation <
- > Low transmitter power <> Compatability with many makes of bombsuits <
- > Simultaneous VHF & UHF operation for maximum range and penetration <
- > Acting Radio Module for Med-Eng line of bombsuits <
- > Systems meet applicable Government standards: NASA proven <

*NATO stock number available upon request



CINEQUIPWHITE
A Comweb Group Member



FOR MORE INFORMATION
WRITE OR PHONE
CINEQUIPWHITE INC
1040 ISLINGTON AVE
TORONTO, ON, CANADA
M8Z6A4
TEL: 416-467-7700
FAX: 416-207-2757
WWW.CINEQUIPWHITE.COM