NAME OF ACTIVITY: Fake Detectors Report

DATE: 25 September 2016

PLACE: C-IED COE, Hoyo de Manzanares, Madrid, Spain

ORGANISATION RESPONSIBLE FOR ACTIVITY: Defeat the Device Branch, Detection Section

C-IED COE ATTENDANTS: N/A

WARNING: FAKE DETECTORS

0. Target Audience.

Public Release

1. Executive Summary.

Multiple companies offer these types of "Magic Wand" devices for explosives detection, promising that they can detect both small and large quantities of explosives at near and very far ranges. These so-called explosive detectors are described as handy, easy to use, and deployable by anyone after a short training class. Manufacturers commonly advertise these devices as effective for detection of concealed explosives in various scenarios such as checkpoint controls and for search measures in preparation of VIP visits.

According to the manufacturer claims, these devices can detect all kinds of commercial and military explosives at a distance of hundreds of meters. They claim that the devices are capable of detecting these threats even when explosives are hidden behind metal or concrete barriers. They also claim that there are no atmospheric limitations, and that some devices do not possess or require a power supply.

The device design consists of a plastic or metal handle, where the "detection unit" is supposed to be located, with an attached telescoping antenna. This antenna can be moved freely within a certain angular range. For explosives detection, the antenna is purported to move by itself to indicate the direction of the searched substance, similar to the operation of a dowsing or divining rod. Devices with "similar operating principles" are listed in Section 2.2.

Despite the fact that there is no scientifically sound proof that any of these devices operate as advertised, as described further in the following text, they are still in use by several organizations and armed forces such as the Iraqi security forces. Prime Minister Haider al-Abadi has said that the police should stop using them. An officer using one of the devices told The Washington Post

simply: “We haven’t received an order yet. ... We know it doesn’t work, everybody knows it doesn’t work, and the man who made it is in prison now. But I don’t have any other choice.” [Published by Kathy Gilsinan, The Atlantic: http://www.theatlantic.com/international/archive/2016/07/iraq-fake-bomb-detectors/490088/]

The distribution of some of these devices was banned in UK in 2010, but the ban only applies to devices produced by UK companies. However, companies based in other European countries are still offering the detectors on their webpages.

2. *Description and Examples of Fake Detectors.*

2.1. Advertised Capabilities

The devices were marketed as being able to detect any and all explosives, drugs, smuggled ivory and a large number of other illicit substances.

2.2. Advertised Method of Operation

The method of operation described below describes the ADE-651 but can be applied to most of the detectors:

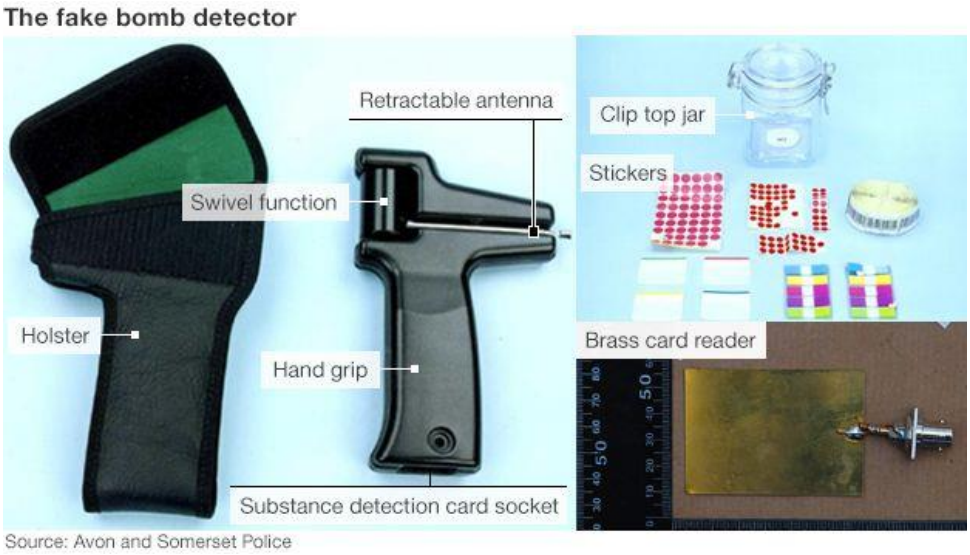

***Figure 1**. ADE -651 source: http://www.bbc.com/news/uk-29459896*

a) A sample of the substance the user wished to detect - such as explosives, drugs - was put in a crystal jar along with a sticker that was intended to absorb the "vapours" of the substance

b) The sticker was then placed on a credit-card sized card, which was read by a card reader and inserted into the device

c) The user would then hold the device, which contained no working electronics, and the swiveling antenna would indicate the location of the sought substance.

2.3. Countries Who Purchased Fake Detectors (Government or Private Acquisitions)

Bulgaria, China, Cyprus, Georgia, Iraq, Lebanon, Mexico, Niger, Pakistan, Saudi Arabia, Vietnam, Thailand and others.

2.4. Fake Dectectors examples:

H3Tec: The main unit consists of a free swiveling pointer antenna housed in a plastic unit with a hand grip, a notebook computer, a separate apparent divining rod, a BNC cable to connect the divining rod to the main unit, and a USB cable to connect the notebook to the main unit. The unit main incorporates a 9v battery. The advertised capabilities include the detection of explosives, drugs, including Crystal Meth labs, hydro-carbons, and minerals e.g. gold, silver etc.

ADE-651, ADE650, ADE100, GADE651 (Advanced Detection Equipment): sold to Niger, Iraq, and other Middle Eastern countries. The Iraqis spent $85m on the devices at around $8,034 apiece.

GT200, GT5000 "remote substance detector": sold mainly in Mexico, Thailand, the Middle East and Africa. The device retailed at $8,034 but the highest price it attained was $803,000.

Figure 2: These devices, as sold, were only empty boxes that contained no electronic components.

The Alpha 6 (NMS International): sold to Egypt, Thailand and Mexico, usually at $3,213 per device. Its highest sale price was $24,906.

PSD-22 (Programmable Substance Detector): marketed as an early warning indicator and direction finder for explosive and contraband detection function in cold/dry/humid condition. Advertised capabilities: detection of Gunpowder, DNT, TNT, RDX, C4, Semtex, PeTN, Ammonium Nitrate, Nitro Glycerin, Dynamite, Nitro Esters(PETN, Ethylene, Glycol Di-Nitrate). Hexogen/Octogen, and all forms of Plastic Explosives.

DIODEBELL AL-6D: advertised to detect and localize explosives at long distances: detection of mines, weapons, RPG'S, stinger missiles, explosive devices, mortar shells, nuclear

projectiles, projectiles, antitank weapons, gunpowder, and many other explosives.

2.5. Suspicious Fake detectors examples:

SNIFFEX (German Procurement Services GmbH, GPS): The device consists of a metal handle with an attached telescoping antenna, capable of free movement, that acts as the pointer for the device. The handle contains two magnets and a 'secret' substance. When SNIFFEX® detects a nitrous oxide based explosive or a weapon that has been fired, the antenna is supposed to point or rotate in the direction of the explosive or weapon. This rotation is said to occur automatically as SNIFFEX® enters into an area containing an abnormally high concentration of "nitrous oxide radicals."

***Figure 3**: Figure Credit: Homeland Safety International*

According to the company, SNIFFEX® can detect explosives up to 300 meters away by reading the "interference between the magnetic field of the earth, the explosive, the device itself and the human body." One unit in the U.S. military bought eight of the devices—for about $6,000 each—even though the military's own tests said the SNIFFEX performed no better than random chance. [Published by Michel Grabel, ProPublica: https://www.propublica.org/article/sec-bomb-detector-bought-by-military-was-front-for-scam-717]

Currently, the SNIFFEX device is legally available for purchase from a registered company. Its appearance reminds us the aforementioned devices. Its advertised detection capability is more analogous to a divining activity rather than sound scientific principles.

On 15 December 2005, GPS GmbH provided a demonstration of the device's performance and detection ability to WIWEB (German Bundeswehr Research Institute for Materials, Explosives and Supplies) as well as representatives from the BKA. The German BKA assessed the detectors after a presentation as follows:

German BKA assessment. **[Translated from German]** "*The GPS firm was not in a position to explain the mode of operation of their "Sniffex" product in a sound, scientific manner. The explanation was merely a series of technical terms intended to impress the listener, without any context or sound scientific background information. This project opens the comparison to a divining rod. The localization of the explosive depends on the direction in which the operator deflects the antenna by tilting the wrist or with a finger.* ***End of German BKA assessment.***

The BKA strongly advises not to procure the described equipment. ***German BKA assessment.***

[Translated from German] "*Recommend the use of more established and scientifically recognized methods such as explosive detection dogs.*" ***End of German BKA assessment.***

HEDD®1 (Unival Group). This is the larger group that incorporates the **German Procurement Services GmbH,** responsible for the distribution and marketing of the SNIFFEX® detector. In February 2015, the manager of this Bonn-based company for safety technology was accused of commercial fraud. In 47 instances, he allegedly sold fake explosives detection devices for a total cost of 2.5 million Euros, although the company has communicated to this CoE that the case was closed without any court proceedings. The device has been sold to Saudi Arabia, Lebanon, Iraq and Pakistan, China, Vietnam and others. Nowadays, non-officially tested versions of SNIFFEX®PLUS (3rd generation) and HEDD®1 (4th generation) seem to be offered by the same distributor, although both devices could not be currently found through the company's website.

***Figure 4**: HEDD1 supposed handheld explosive detection for real-time and covert IED detection*

The operation of HEDD1 is described by the manufacturers as follows (http://www.army-suppliers.info/suppliers/unival-group/pdfs/hedd1_2012.pdf):

"The device works using a patented Magneto-Electrostatic detection (MED) method. The device creates a Modulated Magnetic Field (MMF) around HEDD®1, interacting with the vertical component of the earth magnetic field which creates the conditions for detection of chemical compounds, containing -NO2 / -NO3 and O^-. The magnetic field that is modulated from HEDD®1 is tuned for this bond-/ vibrational energy, and no other substances will be detected from the device. The conductivity/bi-polarity of the human body is needed to operate the device. The detection of explosives is achieved with the cross bearing method/triangulation."

2.6. Legal Actions

Quadro Tracker: Marketed as a novelty golf ball finder, the "Gopher" contained little more than radio aerials from the US, bought for less than $20 each. With the simple addition of a new label, the Gopher turned into a narcotics and explosives detector. It was sold in the US by a US citizen.

Figure 5: *This picture shows the Gopher. A gift for naive golf players. (legal)*

Mole (SCANDEC A / S): After the FBI declared the Quadro Tracker a fraud in **1996**, a British man involved with the device brought the idea back to the UK, where the scam resurfaced as the "Mole." Attempts were made to market the Mole to British government agencies, and in 2001 it was tested by Home Office scientist Tim Sheldon. It was declared "**completely misleading**" and "**potentially dangerous to use**" [Caroline Hawley, BBC: http://www.bbc.com/news/uk-29459896].

ADE-651: These devices were marketed by a Somerset UK-based businessman. He was jailed for 10 years in 2013.

GT200: In 2010, a Home Office defence expert tested the GT200 detector at the request of the Office of Fair Trading and found it had "no credibility as an explosive detector" because it had **no functioning parts**. A man in Kent, UK, was jailed for 7 years in 2013.

Alpha 6: The detectors, marketed through their company Keygrove, were just plastic boxes with an antenna strapped on to them and bits of torn-up paper on the inside. The company owner was jailed for three-and-a-half years at London's Kingston Crown Court. His wife was given a two-year suspended prison sentence and ordered to carry out 300 hours of unpaid work in the community for her role in the scam. Once again, these detectors had **no functioning parts**. In 2010 the UK government established and imposed export controls - and then only to prevent its sale to Iraq and Afghanistan.

3. Conclusions

1. These devices have no functional components. They do not detect any device, material, or component at all.
2. The marketing and packaging cost more than the devices themselves.
3. Lives were put at risk by trusting the claims of the manufacturers.

C-IED COE Assessment: Due to the absence of scientifically proven methods of operation, unclear results after several tests of the device conducted by different agencies and organizations, and related reports, the NATO C-IED Centre of Excellence Defeat the Device Branch dissociates itself from the company's declarations of detection capability, reliability, accuracy.

Although the two suspicious devices mentioned in **section 2.5** are legal to distribute and purchase, none of the manufacturers and responsible companies were able to scientifically prove their marketing claims related to detection performance.

It can't be ruled out that other similar fake devices are available or will be constructed, developed, or marketed in the future. The sure way to identify these fake detectors is to inspect the interior of the device. **END of C-IED COE Assessment.**

4. Recommendations

1. **Do not buy them.**
2. **Do not use them.**
3. **Remove and destroy them from military and/or law enforcement inventories.**
4. **Disseminate this information among all other possible users.**

5. Publications and references

Due to the long presence of these detectors on the market, there are a large number of related publications and media releases available in open sources. The following is a sample of these references.

1. https://www.theguardian.com/world/2016/jul/04/iraq-orders-withdrawal-uk-fake-bomb-detectors-baghdad-haidar-al-abadi-james-mccormick
2. http://www.bbc.com/news/uk-29459896
3. https://www.theguardian.com/uk-news/2016/jun/15/earnings-from-fake-bomb-detectors-to-be-confiscated-judge-orders
4. http://www.nytimes.com/2009/11/04/world/middleeast/04sensors.html
5. http://www.mirror.co.uk/news/uk-news/conman-james-mccormick-sold-golf-1850330
6. http://em.fis.unam.mx/public/mochan/blog/20110612gt200.pdf
7. https://en.wikipedia.org/wiki/ADE_651