AARMS Vol. 12, No. 1 (2013) 9–23. **10.32565/aarms.2013.1.2**

The Radio Controlled Improvised Explosive Device (RCIED) threat in Afghanistan

GuLyÁS Attila

The Radio Controlled Improvised Explosive Devices (RCIED) are one of the most sig- nificant IED-threats in the region of southern Afghanistan. Since I began my military service in ISAF I have recognized that the occurrence of RCIED threats have been increasing continuously since 2008. My survey will provide a short overlook of these types of threats, furthermore my aim is to show the common manner of RCIED's fre- quency-use and the insurgent's "favourite" devices and bandwidths (frequency-bands) to help avoid serious damage to the Hungarian military servicemen, vehicles and mili- tary compounds in the theatre. I am sure that the knowledge of commonly used RCIED- types will help to the Hungarian Special Operations Forces units (HUNSOTUs) to learn the insurgent's (Taliban) tactics, techniques and procedures and overpass many of their IED-systems.

Introduction

The radio Controlled Improvised Explosive Devices' (rCIED) threat in Afghanistan has changed little technically since late 2006. In 2008 Afghanistan experienced more than 4,000 Improvised Explosive Device (IED) attacks, it means more than double that of 2007.[1] Afghanistan is the coun- try where IED employments are systematically used. Facing this threat, the coalition members are trying to improve the protection of their soldiers and to act against the devices.[2] These human and financial investments are focusing on a technological answer and the deployment of new capabili- ties. However, despite these efforts IeDs remain efficient and NATO and Afghan National Security Forces (ANSF) losses have never been so high. Indeed, the IEDs are implemented in very simple ways and tested by technological processes, in a rustic style just the opposite of NATO technolog- ical answers.[3]

The majority of radio Controlled IEDs continue to use purpose-made Dual-Tone Multi-Fre- quency (DTMF) VHF systems (commonly referred to as "spider" devices). The south provinces (near Pakistan's border) such as Nimroz, Helmand, Kandahar, Zabul, Paktika, uruzgan, and Farah are the most dangerous territories, in regards to rCIED threats. E.g. rCIED incidents in Helmand Province account for 10-15%[4] of the IED threat. The Victim-Operated IEDs (Pressure Plates) ac- count for almost all of the remainder. It is judged that any change in the use of ECM which remove coverage on known rCIED frequencies would likely be exploited by Enemy Forces (EF). The presence of rCIEDs can not be discounted in areas where other types of IED (e.g. Victim-Operated Pressure Plate) are assessed to be the most prevalent threat. It is judged that the spread of personal mobile communications networks into new areas offers the greatest potential for the development of the rCIED threat in those areas.

This survey is based on my personal experience and the overall defence intelligence systems' reporting and information sharing. These provide source assessments, which draw on the range of available sources including intelligence reporting, military intelligence collection, imagery, diplo- matic reporting and other open source materials (Internet).

The technical and historical evidence are strongly based on reporting from the theatre and ex- ploitation of recovered equipment, in my experience. Technical and engineering principles concern- ing the manufacture of IEDs, some of which are based on other theatres of operations, are also used. The assessment of future IED trends and evolution of types is based on the statistical analysis, the interpretation of enemy forces' trends and modus operandi, previous technical evolution, known technical limitations of enemy forces, their dispositions and the processes for countering threats.

My rCIED assessment of the threat in Afghanistan is in accordance with the requirement to make the readers understand the formation of several defence policies and the commitment of the Armed Forces and includes the commonly used rCIED jammers' types and bandwidths.

What is the RCIED threat?

The effectiveness of Coalition Force (CF) electronic countermeasures (ECM) in Afghanistan is a prime factor in the continued relative reduction of the rCIED threat. Since late 2006, Enemy Forces (eF) have used essentially the same types of RCIeD firing switches. Different versions of the spider family of VHF receivers (DTMF) are used for telecommunications signalling over analogue telephone lines in the voice-frequency band between telephone handsets

[1] report on Progress Toward Security and Stability in Afghanistan (2010). p. 54.
[2] DOCTrINE General Military review, editions of 2009-2010
[3] DINGLEy (2009) p. 104.
[4] GrAHAM (2011) p. 137.

and other communications devices and the switching centre[5] have all been seen, but to date, their operating parameters have remained broadly consistent with earlier models. The spread of mobile com- munications networks such as GSM mobile phone and Code Division Multiple Access (CDMA) local loop services, which are already established in the larger population centres in Afghanistan, continues. Infrastructure is presently centred on population centres and the main route (Highway 1). [3] The wireless telecommunications market has been growing continuously since 2002 and will likely continue to do so for the foreseeable future. As of January 2009 the 4 licensed GSM providers in Afghanistan had 7.2 million subscribers. In addition, several companies have been allowed to operate networks using the uS 3G standard (CDMA 2000)[6]. GSM providers will con- tinue to roll out more capability and continue to expand network coverage across Afghanistan. The increasing availability of mobile personal communications makes it more likely that EF will make greater use of the systems in rCIEDs. Figure 01 shows the occurrence of rCIED among all of the C-IED threats[7] in South Afghanistan in 2009. Mobile phone networks already operate in the main population centres of Helmand province (in Kajaki, Gereshk, Lashkar Gah, Musa Qal'el and Sangin).

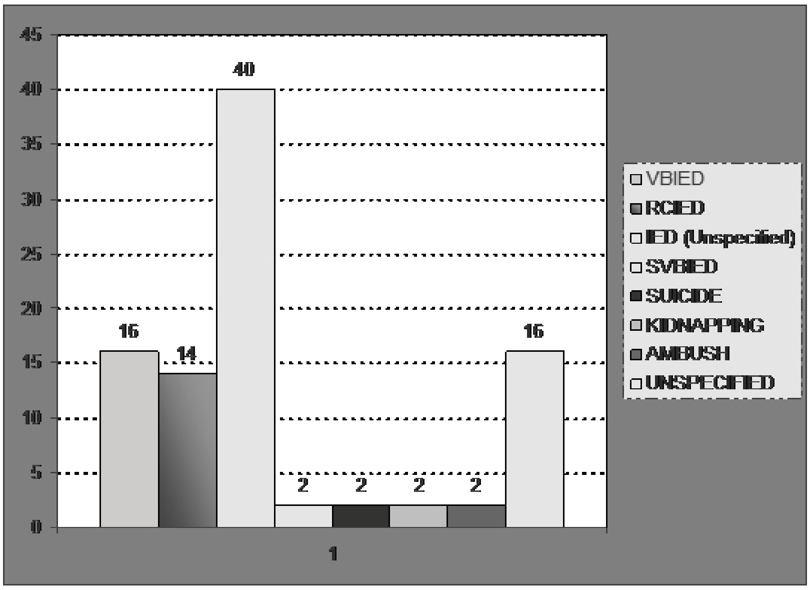

Figure 1.

Definitions

For a better understanding of what the acronym IED (rCIED) means it is necessary to specify the expressions regarding the improvised explosive devices' issues.

Improvised Explosive Device (IED): A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from non-military components. All IeD-related definitions will default to the Weapon Intelligence Team's IED Lexicon[8].

1. VEHICLE-BOrNE IED (VBIED): An IED delivered by any small ground-based vehicle (e.g. passenger vehicle, motorcycle, moped, bicycle, etc.) and/or serves as the concealment means for explosives with an initiating device.
   - Bicycle
   - Large Truck (Jingle/Tanker)
   - Small Truck (Pick up)
   - Car
   - Motorcycle
   - Other
   - SuV

[5] SCHENKEr L. (1960) pp. 235–255.
[6] GrOSS–SANGIN (2008)
[7] DOCTrINE Military review: Regional Command-Capital survey 2009, edition of 17/2009. pp. 37-40.

2. SuICIDE VBIED (SVBIED): A VBIED whose explosives are intentionally initiated by the vehicle's occupant.
   - Bicycle
   - Car
   - Cart
   - Motorcycle
   - SuV
   - Large Truck (Jingle/Tanker)
   - Small Truck (Pick up)
   - Other
3. rCIED: An IED initiated electronically in a wireless manner consisting of a transmitter and receiver (i.e. personal mobile radio (PMr), cell phone, cordless phone, pager, etc)
   - rC Cell phone
   - rC DTMF
   - rC DTMF (Mod unknown)
   - rC Vehicle Alarm
   - rC Other
   - unknown
4. COMMAND IED: Initiated with a wire and power source, may include a switch
   - Command Pull (Mechanical)
   - Command Wire (Electric)
   - Command Other
   - unknown

Threat priorities

Figure 2. shows the breakdown by type of known rCIED incidents since the start of 2009[9]. The spider family of devices accounts for approximately 75% of the rCIED threat, with various types of radio systems making up the balance. The commonly used frequencies are in the VHF band. It is because the electronic devices using this frequency-band are sold in every cheap market and it is not complicated to buy-assemble-install-operate the explosive devices mounted to rCIED.

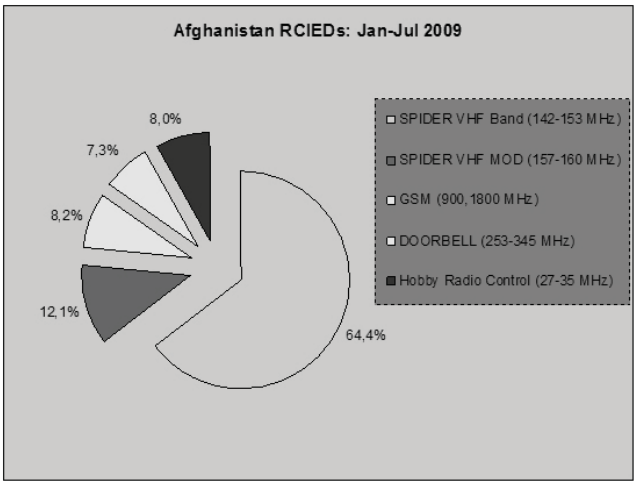

Figure 2.

The hobby radio control devices operate in high frequencies (HF). It is difficult to build a spread jammer spectrum-device against them. The commercial (Commerce Off The Shelf COTF) and few military jammers, mostly, do not jam under 30 MHz, so the rCIED operated in that fre- quency range could be extremely efficient and lethal.

The most common spider devices operate in the 142-153 MHz frequency range. In the free market of South Afghanistan anybody can purchase simple devices working in these ranges, the types of the devices are listed in the Tables of this survey. The Taliban mostly use the handy radios (ICOM, Kenwood) for this simple reason.

Figure 03 shows the breakdown, by type, of known rCIED incidents in Helmand Province since the start of 2009. The

[8] Standard Insurgent Action Terms - ISAF SOF FrAGO080705 pp.18-21.

[9] BArKEr (2010) p. 5.

spider family of devices accounts for approximately 84% of the rCIED threat, with various types of radio systems making up the balance. [4]

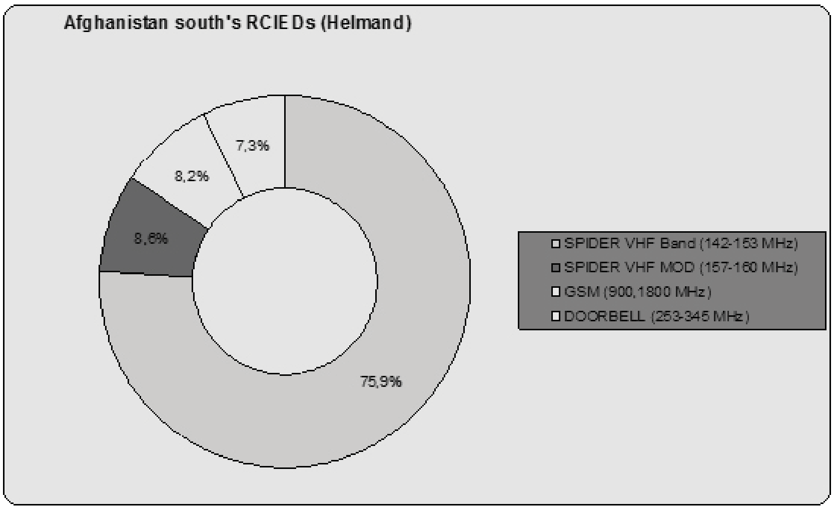

Figure 3.

In Helmand Province, rCIED incidents continue to account for 10-15% of the known IED threat. rCIED attacks are largely directed at CF but achieve the most success against ANSF when they are not protected by CF ECM. E.g. one of the successful rCIED attacks in June 2009 resulted in the death of an ANA officer. A CF (UK) KIA occurring in an RCIeD attack was in September

2007 and one WIA in March 2008[10]. It is assessed that the relatively low number of CF casualties from rCIEDs is directly attributable to the effectiveness of CF ECM. It is judged that any change in the use of CF ECM which removed coverage on known rCIED frequencies would likely be exploited by EF.

Threats in South Afghanistan

The RCIeD threat in Afghanistan varies significantly by province. The assessed RCIeD threat priorities, in decreasing order of priority, for areas in the south are:

a) Regional Command (South):

1. Bespoke DTMF-encoded VHF systems (includes purpose-built devices, e.g. Spider vari- ants and Sega, transceivers e.g. ICOM, Kenwood, Motorola - 136 to 174 MHz.
2. Bespoke key-fob switcher - 315 MHz.
3. COTS transceivers GMrS - 462 to 468 MHz.
4. GSM-based systems - 900 and 1800 MHz. (where infrastructure is available)
5. remote Switch – Purpose Built Transceiver (the Wireless Custom receiver (WiCr)) - 869 MHz.
6. COTS Transceivers - 409 MHz.
7. HPCP systems (normally Handset to Base Station) - majority 225 to 232 MHz.
8. Other rC systems seen to date are in very low numbers. Individual systems - such as door- bells, car alarm systems, rC toy and appliance controllers have been seen less than 4 times across Afghanistan since 2002. [5]

b) Capital Region:

1. Bespoke DTMF-encoded VHF systems - 136 to 174 MHz.
2. Bespoke key-fob switcher - 315 MHz.
3. GSM-based systems - 900 and 1800 MHz.
4. COTS Transceivers GMrS - 462 to 468 MHz.
5. remote Switch – Purpose Built Transceiver (WiCr) - 869 MHz
6. Telemetry systems - 418 MHz.
7. HPCP systems (normally Handset to Base Station) - majority 225 to 232 MHz.
8. Other rC systems seen to date are in very low numbers.

My detailed list of known threat frequencies is based on in-theatre reporting and technical exploitation. The value of technical exploitation in the identification of new threats cannot be overstated, but does rely on the timely recovery of intact

[10] BArKEr (2010) p. 7.

devices. It can be concluded that the most often used frequencies are in the frequency range of VHF/uHF and the mobile phone band. In the south part of the country the civilian merchants provide a great selection of electronic devices used in the civilian sector of industry and commerce. These electronic devices are operated in the free (not secured) frequency ranges and are easily purchased. This fact broadens the opportunities for the IODs' constructors to make easier and more low-profile RCIeD devices, and find the cheapest and the most efficient (laziest) way to buy and fit these devices together. Another problem to re- solve is that these cheap electronic devices using the VHF frequency range are very simple built-in constructions. For this reason the daily-weekly-monthly maintenance and the repairing cycles, im- portant to keep them in working order, are a simple-manner, understandable, and easily learnt. The proof position of coalition forces increases with the national jammers, operated by ISAF troops in the field. All of these provide higher security and all-round defence for national/international troops of ISAF against spider devices and other types of threats. These provide a higher level of power-output for jammers giving the troops higher levels of convoy velocity and beyond this op- erational capability.

The passive infrared (PIR) firing switch

The PIR firing switch is not classified as an RC threat (the value of technical exploitation in the identification of new threats cannot be overstated, but does rely on the timely recovery of intact devices) but is directly associated with RC arming systems. The PIR firing switch has been known to have been used in an IED attack in Afghanistan just once (21 April, 2007). Intelligence agencies continue to monitor this threat, but judges that its further use is not imminent. It is assessed that the PIr threat should be allocated the same priority as the associated rC arming switch (currently the LINX 418 MHz telemetry module). The PIR firing switch is victim operated rather than radio controlled.

Jamming

All coalition troops have their own jamming system to avoid serious damage to their own forces using those in vehicles and manpack-series. As we have seen in the figures, the VHF/UHF band and the mobile phone band are the most dangerous frequency ranges used by the spider family.

Coalition troops in theatre use several types of vehicle-born jammer devices and tactical man- pack sets. These are mostly COTF devices and provide overall defence against EF's rCIEDs. One of the used types of vehicle-born tactical jammer units is the wide band systems - WBS[11] (Figure 04). The set is a compact, multi-channel, programmable active jammer, operating over the 25 to 2500 MHz frequency range. The operating range covers the surveyed radio spectrum between these two extremes allowing the selection of channels with no gaps or blind spots. It can be repro- grammed in the field using a laptop or PDA running a MS Windows operating system to change its jamming waveforms, target frequencies and operating parameters. Settings are stored in non-vol- atile memory and activated automatically whenever the equipment is switched on. Mission data and operating firmware can be rapidly cleared via a button sequence on the front panel or Remote Control unit (rCu) keypad. Division Multiplexing (TDM) technology is used enabling the unit to be programmed for a variety of operational requirements[12]. The user-friendly panel interface allows field-based operators to rapidly interchange between missions and cater for a variety of strategic and tactical scenarios. each unit has one fixed RF jamming channel operating over the 25 to 220 MHz frequency range (VHF/UHF frequency range), in addition to five user-definable 150 MHz jamming channels which can be steered to any part of the 25 to 2500 MHz frequency range as required. To eliminate the need for complex cabling configurations the unit contains two integrated power amplifiers (10-100W).

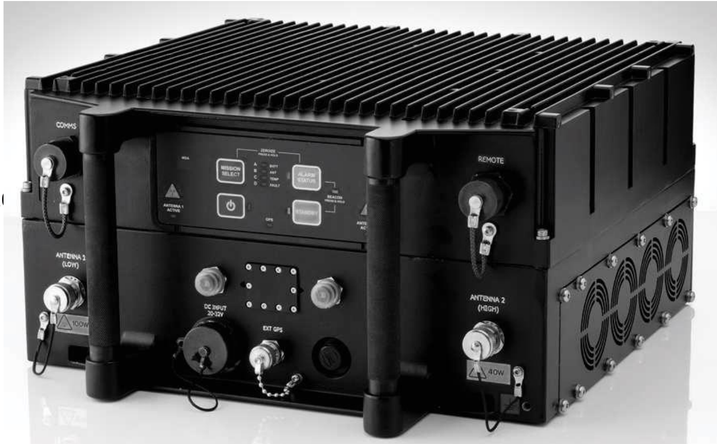

Figure 4.

[11] Asian Mil Review: Blocking the trigger – IED/ECM Technology Update, 03 May 2008, pp. 36-39.

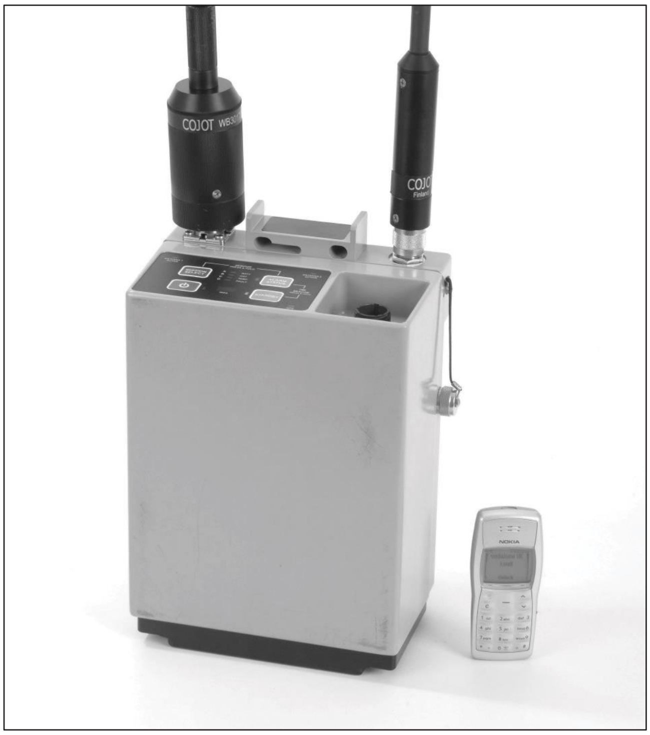

Figure 5.

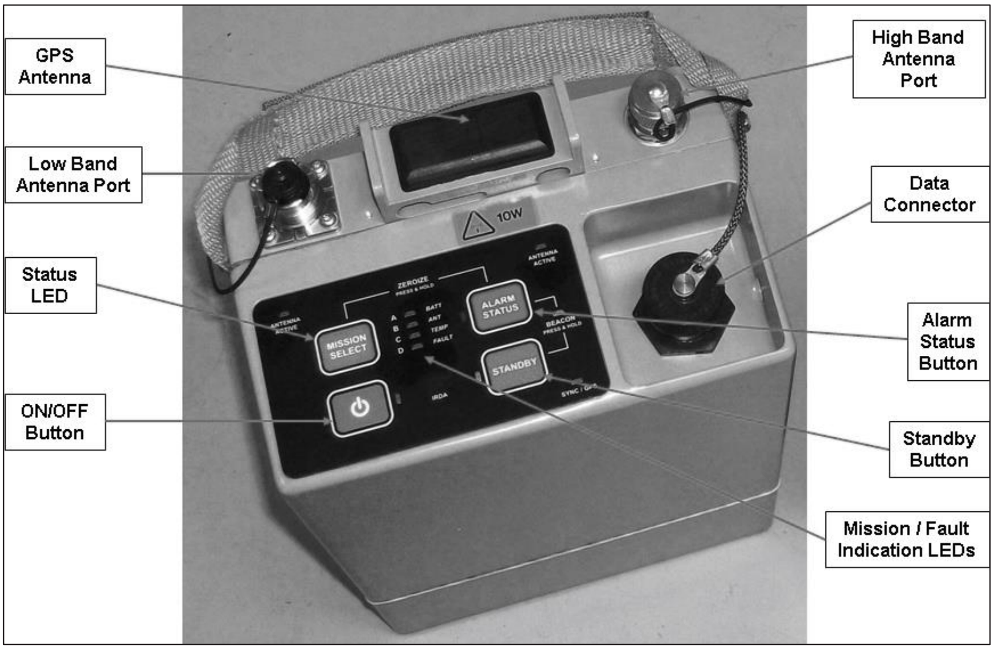

Figure 6.

The tactical manpack unit (Figure 5.) is an advanced man portable battery-powered program- mable ECM system focused primarily at counter-rCIED and Force Protection applications. It is fully field-programmable and allows new mission parameters and waveforms to be easily loaded into the unit from a laptop PC.

It is available in two variants:

- for operation in the 25-512MHz frequency range;
- for operation in the GSM900, GSM1800 and GSM1900 bands.

Both versions can generate transmit rF powers up to 10W. The set contains a versatile trans- mitter module, capable of generating up to 10W rF, coupled to a high-speed direct digital syn- thesizer (DDS) and digital signal processor (DSP) that are capable of generating a wide range of different jamming signals. The operating firmware and operational configuration of a jammer set can be field-reprogrammed and upgraded easily to respond to changing targets, priorities and techniques (Figure 6.). The set is designed primarily for man-portable applications and is typically carried in a special ECM backpack[13].

[12] Jane' Explosive Ordnance Disposal, 28 February 2011, pp. 42-43.

Summary and deductions

The favorable areas of attack are known; the targets, even if it is too difficult to get close to them, remain easily identifiable. The look for added value remains a constant, either aiming at tactical objectives by destroying the main threat, the C2 means or limited assets, or aiming at strategic objectives by striking facilities, VIPs or symbolic targets, and seeking psychological effect. These new assets, despite a costly development offer, for most of them, are only a partial answer to the problem. Moreover, they create important training needs, both learning how they work and integrating their tactical use. Taking this protection and its limits into account and in the scope of a relationship of the weak to the strong, the insurgents are keeping very simple operating modes without taking part in this technological logic. Despite some complex IEDs having already been used, it seems that homemade systems remain predominant. Thus, in reply to jammers being wide- spread, the insurgents use, more traditional assets in which mechanics overrides electronics. This trend explains the significant decrease of radio controlled systems and the renewal of pressure or wire systems even if they impose longer laying time. In the same way, facing a longer range and an improved capability of returning fire, he favors either the remote control of the launch unit at sev- eral hundred meters from the target or the combination of several ignition systems. These methods enable him to select the target without any collateral damage. [6]

The rCIED threat will continue to account for a sizeable proportion of IED incidents across Afghanistan. EF monitors CF use of ECM and retains the capability and intent to exploit weak- nesses and gaps in coverage and associated TTPs. It is judged that any change in the use of CF ECM which removed coverage on known rCIED frequencies would likely be exploited by EF. Table 01-07 show the occurrence of rCIED's device types and their frequencies and the threat they cause in the frequency spectrum of VHF. In addition, the presence of rCIEDs in the immediate area of other types of IED, e.g. Victim-Operated Pressure Plate, cannot be discounted. EF contin- ues to seek fresh and updated rC technologies and techniques in their efforts to overcome CF ECM and associated procedures. Although there have been no technical changes in the rCIED threat in the last months of 2009, it should not be assumed that this will remain the case.

[13] Tactical Manpack Unit descriptions, Jane' Explosive Ordnance Disposal, 28 February 2011, pp. 50-52.

Deductions

1. The spider device threats, using the VHF frequency range (140-160 MHz) are spreading. The basis of rCIEDs (electronic devices, electronic parts of devices) can be bought in the free market (COTF) so the assembling and the mounting of these devices are easy and well-known by insurgents. The all-round defence against these electronic devices could be the rigid control of merchandising, in regards to the devices operating in these frequency ranges.
2. In the programming phase of jammers the ISAF needs significant care of the frequencies using the spider (VHF) assets. The higher the power jammers' output, the higher the level of secure movements and operations. The average cover distance of national and international (ISAF) assets are 10-15 meters according to my personal experience. It would be beneficial if troops could broaden the cover-area to 20-30 meters or more, augmenting the all-round defence of convoys and dismounted troops. It could be possible with higher power output of vehicle and manpack jammers (versions detailed above). However the higher power results in higher measures and weight of assets, so it might only be realistic in the case of armoured personnel carriers (APCs).
3. It is necessary to provide great attention to the frequencies used by spider devices and to the all- round defence protecting our forces. If the 45 countries composing the ISAF provide a higher interest in operations planning against rCIEDs use the knowledge of spider frequencies and jammer capability, there might be efficient and reliable methods to better protect ISAF troops.
4. The electronic devices using the GSM range are electronically jammed by ISAF jammers. It could be distracting in the case of ISAF communication channels programming. Browsing through the operation system of the jammers, it is possible to install program gaps into these ranges. However, this is not the way the ISAF may move in the near future. My personal opinion of what the ISAF has to do is to use the frequencies not covered by coalition jammers. Turning off the jammers or not using their programming for these GSM frequencies (program- ming gaps into the jammers' band) cause serious harm (danger) to ISAF troops, because in this case the EF could also use their devices in an easy way.

I believe, and it seems very clear, that mobile communications networks will continue to ex- pand in Afghanistan. Experience shows that where this type of communications is available it is consistently used by EF in rCIEDs. As infrastructure spreads, it is judged that EF will make great- er use of the systems in rCIEDs. Taking into consideration the most commonly used frequencies and the types of devices using these frequencies, we can build an overall jamming defence based upon the direct instructions of the theatre intelligence sources and practical experiences of our own. From the following tables we can examine and understand the commonly used devices and their frequencies, preparing our troops by properly tuning their jammers to avoid the rCIED threat all over Afghanistan.

In concluding my survey, I will provide a few tables to summarize the commonly used devices by insurgents and the frequencies involved in their operations (Table 1-5.. Figure 7-8.).

Serial	Threat configuration		Operating freq. (TX)	Modulation coding/ schemes	Typical transmit	Typical link range	Comments
	receiver	transmitter					
Remote Switch – Keyless Entry System							
1	Keyless entry rX	-	306.2 to 313.33 MHz	-	-	≤ 100 m	Keyless entry system, most likely car alarm
Remote Switch – Car/Motorcycle alarm							
2	Car/ Motorcycle alarm rX	-	˜ 314 to 316 MHz	-	-	≤ 100 m	Steel Mate product
		-	˜ 315 MHz	-	-	≤ 100 m	Mitsuba & Little Flying Tiger products
Remote Switch – Wireless Doorbells							
3	Doorbell rX	Doorbell switch	˜ 253.14 – 345.5 MHz	-	-	≤ 100 m	All types
			253.14 263.5 MHz	-	-	≤ 100 m	Artslon TX product
			301.6 MHz	-	-	≤ 100 m	

Table 1. Threat frequency table (as of JUN 2010)

Serial	Threat configuration		Operating freq. (TX)	Modulation coding/ schemes	Typical transmit	Typical link range	Comments
	receiver	transmitter					
Remote Switch – Wireless Doorbells							
3	Doorbell rX	Doorbell switch	˜ 308 – 311 MHz 314.705 MHz	-	-	≤ 100 m	rL Type product (Chinese)
			316 to 318 MHz	-	-	≤ 100 m	CST TX product
			331 MHz	-	-	≤ 100 m	Consta NS-2000
Remote Switch – Purpose built devices							
4	PC game controller (SEGA)	ICOM IC-V68 KENWOOD or similar transceiver Bespoke receivers	136 to 174 MHz with many intermediaries Actual frequencies encountered in the range of 137.765 to 170.300 MHz.	FM	5W	km	Double superhet rX product DTMF decoder

Table 2. Threat frequency table (as of JUN 2010) – cont. 1.

Serial	Threat configuration		Operating freq. (TX)	Modulation coding/ schemes	Typical transmit	Typical link range	Comments
	receiver	transmitter					
Remote Switch – Purpose built devices							

4	PC game controller (SEGA)	ICOM IC-V68 KENWOOD or similar transceiver Bespoke receivers	Special frequencies as follows: 137.765 MHz 138.880 MHz 139.055 – 139.705 MHz 141.275 – 145.750 MHz 145.865 MHz 146.000 MHz 146.525 MHz 147.050 – 147.055 MHz 148.100 – 148.630 MHz 149.150 – 150.305 MHz 150.905 – 154.470 MHz 154.700 – 158.185 MHz 158.295 – 170.300 MHz	FM	5W	km	Double superhet rX product DTMF decoder

Table 3. Threat frequency table (as of JUN 2010) – cont. 2.

Serial	Threat configuration		Operating freq. (TX)	Modulation coding/ schemes	Typical transmit	Typical link range	Comments
	receiver	transmitter					
Remote Switch – Switcher unit							
5	Key-fob switcher unit	Bespoke purpose built	313.7 to 315.036 MHz	-	12 mW into 50	≤ 500m	Super regenerative rX as Sony car door lock
Remote Switch – Telemetry Module							
6	Linx rXM-418 Lr-S	Bespoke purpose built	418 MHz	AM	-	-	Single Superheterodyne rX
COTS transceiver – professional							
7	ICOM IC-V68	ICOM IC-V68 or similar	136 to 174 MHz	NBFM ±5kHz DTMF	3-5W	km	Double superhet rX
8	ICOM IC-H16	ICOM IC-H16 or similar	136 to 174 MHz 151 to 172 MHz	FM with CTCSS+DTMS	3-5W	km	Double superhet rX
Hobby Radio Control – short range radio control							
9	-	-	27 to 35 MHz 49/50 MHz	-	-	≤ 100m	Feugyuan Toys product

Table 4. Threat frequency table (as of JUN 2010) – cont. 3.

Serial	Threat configuration		Operating freq. (TX)	Modulation coding/ schemes	Typical transmit	Typical link range	Comments
	receiver	transmitter					
Cordless telephones – High Power							
10	Mostly Senao SN-258 Nokia Nokia Albasha Brother Electron Samsung Chord music Famous Brand Product unbranded		115 to 227 MHz	NBFM	≤ 5W	≥ 10km LOS	Double superhet rX
			115 to 268 MHz majority in the frequency range of 225 to 236 MHz	NBFM	≤ 3W		
Wireless Network Phone							

11	Nokia 1100 Nokia 1112 Nokia 2300 Nokia 3310 Nokia 6100 Samsung SGH N-620 unbranded	900 MHz 1800 MHz	-	-	-	-

Table 5. Threat frequency table (as of JUN 2010) – cont. 4.

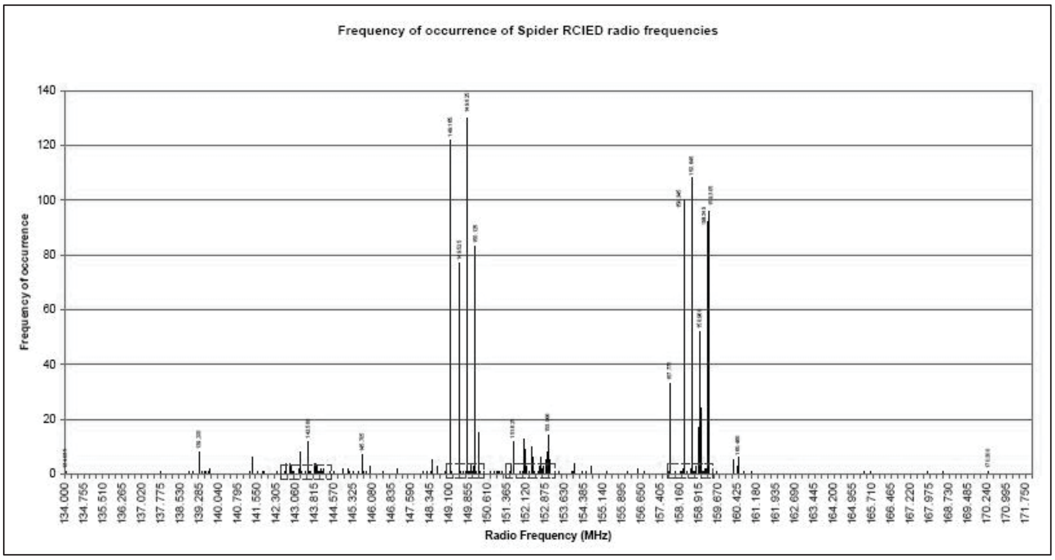

Figure 7. Threat frequency table (as of JUN 2010) – cont. 5.

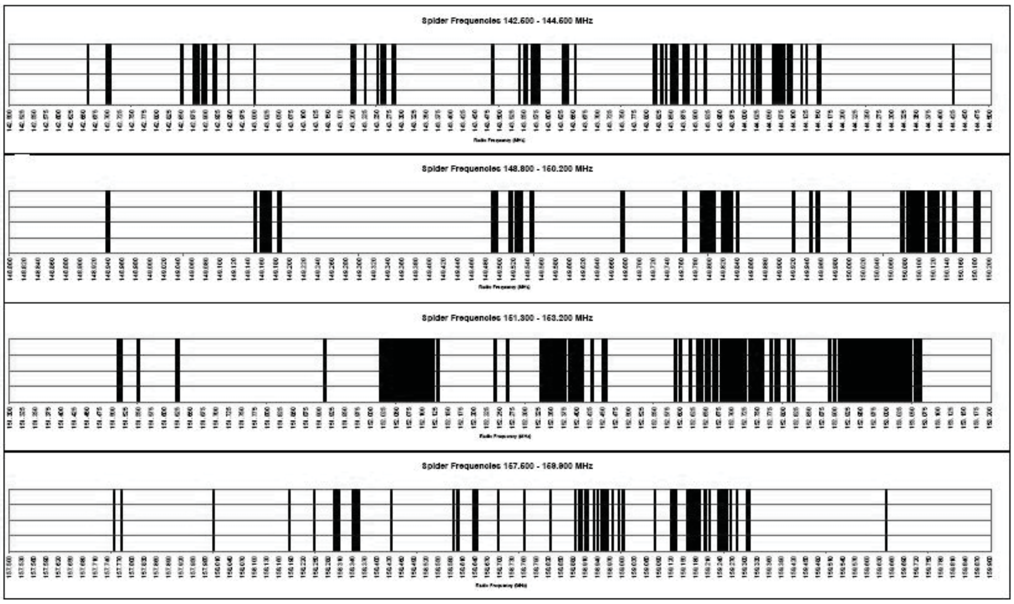

Figure 8. Threat frequency spectrum table (as of JUN 2010)

Abbreviations

ACTD	Advanced Concept Technology Demonstration
AOI	Area of Interest
AOr	Area of responsibility
BFT	Blue Force tracker
C2	Command and Control
C2IS	Command and Control information Service
C4I	Command, Control, Communications, Computers, and Intelligence
CCID	Coalition Combat Identification CDMA

Code Division Multiple Access CDS	Cross Domain Solution
CID	Combat Identification CONEMP Concept of
Employment DTMF	Dual Tone Multi Frequency FAC Forward Air
Controller	
FBCB2	Force XXI Battle Command Brigade and Below
FFT	Friendly Force Tracker HPCP High Power Cordless
Phone IFTS	ISAF Force Tracking System IP Interoperability Profile
ISAF	International Security Assistance Force
IT	Information Technology
JTAC	Joint Terminal Attack Controller
NFFI	NATO Friendly Force Interface
PLI	Point of Interest
PIr	Passive Infrared
RBCI	Radio-Based Combat Identification
rOE	rules of Engagement
SA	Situational Awareness
SADL	Situational Awareness Data Link
SHAPE	Supreme Headquarters Allied Powers, Europe
SÍP	Service Interoperability Profile
TOC	Tactical Operations Center
TTP	Tactics, Techniques, and Procedures

References

BArKEr, Alec (2010): Improvised Explosive Devices In Southern Afghanistan and Western Pakistan. In: *Counterterrorism Strategy Initiative Policy Paper.* April 2010, New America Foundation. COWArT, J. D. (2010): *Haditha Diary*. Xulon Press.

DINGLEy, James (2009): *Combating terrorism in Northern Ireland.* routledge, London and New york.

DOCTrINE General Military review, editions of 2009-2010

GrAHAM, Adrian (2011): *Communications, Radar and Electronic warfare.* Wiley.

GrOSS, David A. – SANGIN, Amir Zai (2008): Afghanistan's Communications revolution; The Tele- coms revolution. In: *The Washington Post*. Edition of 8 September 2008. *Report on Progress Toward Security and Stability in Afghanistan (2010)*

SCHENKEr, L. (1960): Pushbutton Calling with a Two-Group Voice-Frequency Code. In: *The Bell system technical journal,* 39 (1). https://doi.org/10.1002/j.1538-7305.1960.tb03929.x

The commitment of French Land Forces in Afghanistan. In: DOCTrINE General Military review 17/2009.

US Congress House, Committee of appropriations, Department of Defence: Appropriations for 2006: Army recruiting and retention programs, US GPO 2006.

WuNDErLE, William D. (2010): *U.S. Army Weapons Systems 2010-2011*. Skyhorse, New york.

http://books.google.hu/books?id=XztBugr9apcC&pg=PA227&dq=rcied+afghanistan&hl=-hu&ei=t9LhTdWtL4n5sgaTq4DuBQ&sa=X&oi=book_result&ct=result&resnum=5&ved=-0CEQQ6AEwBA#v=onepage&q=rcied%20afghanistan&f=false

http://books.google.hu/books?id=tvaGMerkXLsC&pg=PA217&dq=rc+ied+afghanistan&hl=hu&ei=it-PhTde2D8TLswbWvpmLBg&sa=X&oi=book_result&ct=result&resnum=10&ved=0CFcQ6AEwC-Q#v=onepage&q&f=false

http://books.google.hu/books?id=orgtAQAAIAAJ&q=rcied&dq=rcied&hl=hu&ei=2c_hTZvLMc7FtA-aHsZCEBg&sa=X&oi=book_result&ct=result&resnum=8&ved=0CEwQ6AEwBw

http://ew30.blogspot.com/2010/03/counter-remote-control-improvised.html