Electronic Warfare – From the victims perspective

SGT Gavin Wilson

Disclaimer

- All information in this presentation is derived from Open Source intelligence

SCOPE

- What do EW units actually do?
- Russian EW examples
- Other Nation’s EW
- Personal Communication Systems (PCS)
- Social Media
- Tactical
- Conclusion

What do EW Units actually do?

- Put simply, their mission is to:
  - Intercept, collect, locate (where possible), analyse and report on enemy Signals of Interest (SOI)
- This may allow a commander to discover or assess enemy
  - ORBAT
  - Priorities
  - Intent
- Or to destroy or degrade En. C2 at a later time

Russian EW Examples

- Russian EW forces used jamming, combined with precision artillery, to inflict 80%+ casualties on a Ukrainian Mech Inf Bn in under 15 minutes
- Likely Russian EW forces jam OSCOE (Organisation for Security and Co-operation in Europe) mobile phones and UAVs when they approach or pass Russian units or positions
- Likely Russian EW forces sent Ukranian soldiers messages – via SMS to their personal mobile phones
- Russia has demonstrated EA capabilities across the whole Electro Magnetic Spectrum. These have proved highly effective

Other nation Cyber/EW threats

- Iran – reported by Israel to have given terrorist organisation tools to hack UAS controls
- Iran – reported to have conducted cyber attacks against USA, Israel and various Gulf states
- Israel, long a leader in UAV's, is now mounting various EW payloads onto many of its UAV's
- China – has near identical capabilities as Russia
  - China has released EW aircraft including an F18 Growler equivalent
  - Media reports speculate recent US Navy collisions were the result of Chinese electronic attacks

Personal Communication Systems

- Technically, it is possible to detect and track your mobile phones and other devices.

- Within Australia, there are significant legislation making such activities highly constrained and controlled

So why the fuss about mobiles?

- Your mobile phone is a tracking device

- Turning off the phone GPS does not prevent your location being compromised. The size of the area increases a little – but your location can still be calculated to within a few hundred metres

Overseas

- Although most western nations have privacy laws protecting individuals, the remainder, mainly do not
- Foreign governments can often demand access to phone networks - where they don't already control them
- This means that your personal communication are HIGHLY vulnerable to foreign intelligence services when overseas and outside of western nations

Overseas examples

- Canadian Broadcasting Company reported on 03 Jan 2018 that Canadian soldiers in Baltic nations had experienced ‘unusual activity’ on their mobile phones

- The American Commander in Poland found someone trying to access his iphone. A trace identified the source as being from Moscow

Wi-fi

- Wi-fi networks provide your devices unique identifier (MAC address) which can subsequently be tracked – increasing your EMS profile
- When wi-fi is turned on your device sends probes/pings out looking for access points.
- Your device will remember all the access points it has connected to in the past. This allows third parties to tell where you have been.
- You can, and should, delete your wi-fi access history in settings/wi-fi
- New devices are using rolling MAC addresses to find access points, the devices actual MAC address is still used when connecting to an access point

Social media

- Social media is a huge source of intelligence for any self respecting government, intelligence agency or military
- There have been several high profile compromising incidents based on social media posts in the west
- On EX HAMEL 16, the Social Media Survey Team recorded over 900 OPSEC breaches
- Several breaches identified upcoming tactical actions
- Breaches were detected from all rank levels from soldier to senior officers

EW – In Tactical terms

- If it transmits, it can be located *
- If it can be located, it can be destroyed or degraded
- * HF is your friend!
- Single channel VHF / UHF can be detected and bearings calculated (DF'd) relatively quickly
- HF / VHF / UHF are vulnerable to electronic attack, commonly referred to as jamming
- Meshed nets like BMS are more difficult to DF and jam

Reducing your EMS profile

- Brevity
- When using single channel comms, change frequencies – often! (Weekly is NOT enough)
- Use encryption (EW hate that)
- Do not be tempted to drop encryption if comms degrade – that's what EW want you to do!
- Don't use standard c/s (victor etc. EW love that!)
- Terrain shielding
- Avoid routines – or at least try to hide them
- Use HF as much as possible

Reducing your EMS profile

- Use directional antennae
- Use Near Vertical Incidence Skywave (NVIS)
- Use burst data as much as possible. This is very difficult to detect and is equally difficult to DF
- Use of SPR is encouraged
- Whilst the above techniques are not always practical, they should be practiced whenever they ARE practical
- Use of combinations increases your protection

GPS

- GPS signals are relatively weak and not very difficult to jam
- Given that most of our new communications systems rely on GPS for timing synchronisation this may be a problem, as both Russia and China, (plus others), are known to have GPS jamming capabilities
- Russian GPS jamming has proven effective against US UAVs
- In Dec 2011, Iranian forces bought down a US UAV, likely involving interrupting GPS signals from its US controllers

GPS jamming counter measures

- Practice use of comms systems without timing on those systems where this is possible
- Shielding – tests have demonstrated that shielding GPS reliant devices from jamming can reduce or possibly eliminate GPS jamming
- Terrain, buildings, or even large vehicles may be sufficient to shield GPS devices, especially smaller ones
- Practice navigation WITHOUT GPS

Conclusion

- Uncontested access to EMS can no longer be guaranteed. The opposite is the case – it is quite possible access will be interrupted and unreliable
- You are vulnerable to enemy EW elements
- Whenever it is practical, you should reduce your EMS profile by methods such as;
  - Changing freqs – often
  - Use encryption and burst data
  - Use directional antennae and/or terrain shielding where practical
  - Use HF
  - Combinations of the above

Conclusion - cont

- Your personal communication systems, be they phones, modems, tablets or dongles, ARE vulnerable
- Turning off phone GPS means enemies cannot locate you down to metres – merely to a few hundred metres!
- The best way to protect yourself is to not take a device in the first place. If you do, ensure wireless and phone services are turned OFF