# Towards the Electronic Guerrilla

**Helmoed Römer Heitman**
**Association of Old Crows, September 2013**

## Introduction

There is much talk in recent times of ‘asymmetric warfare’, and an entire extended family of war-fighting concepts and theories has grown around that. ‘Cyberwar’ is but part of this wave of new thinking on defence and national security issues.

Among these concepts are “4th Generation”, “Complex”, “Compound” and “Hybrid” war, as well as two that are perhaps the most interesting to this group:

**Netwar**: RAND analysts have put forward the concept of ‘netwar’ which they have defined as “low-intensity undertakings by social-networked actors”, with the Zapatistas of Mexico as one example, who moved from a hierarchical insurgency to a “networked structure”, and some of the of the transnational criminal groups as other examples, among them some of the Colombian narcotics groups and some of the Somali pirates. The real threat here lies in the risk of criminals, guerrillas and terrorists making common cause and then being used by one or another state to further its own ends. Their networked structure can be difficult to counter, but is also believed to be difficult to maintain.

While guerrillas and criminals have co-operated in the past, and governments making use of such groups is also hardly new, this concept is worth closer consideration: It pulls together a number of strands already visible in Latin America, Africa and Asia, and sets out what will be a very difficult challenge for security forces. Just to begin with, how does one build up a useful intelligence picture when the opponent comprises several groups with very different backgrounds and agendas?

**Unrestricted Warfare**: This concept, put forward by two Chinese Army colonels, has been presented as a concept of how a country such as China can defeat a technologically superior opponent, such as the United States. It argues for “*a grand warfare method*” that combines “*all of the dimensions and methods in the two major areas of military and non-military affairs so as to carry out warfare*”, and that is executed by “*a composite force in all aspects related to national interest*”. Among the types of warfare it envisages as forming part of the whole, are ‘lawfare’, economic warfare (trade war, financial war), network warfare, terrorism and even what it terms ‘ecological warfare’, which includes future climate modification. The authors also argue that terrorism is a traditional means of using limited resources to fight an unlimited war, and that the ‘new terror war’ will probably take the form of cyber war. Like ‘netwar’ this is something to ponder.

But we also need to understand that ‘asymmetric warfare’ as such is not a new concept. Ever since the first human realised that the only way to overcome a larger opponent was to sneak up hit him on the head from behind or while sleeping, we have had the concept of the weaker of two opponents seeking some ‘asymmetric’ advantage. Guerrilla warfare and terrorism are the two primary examples.

The other concepts mentioned above are also worth considering – even if they are not really any newer that guerrilla warfare as such, because we will encounter them in the future and are, indeed encountering at present:

**4th Generation Warfare**: This theory considered the rise of non-state actors as real military threats, argued that future war would centre on terrorism, psychological operations and trans-national action, would blur the lines between war and politics and would be long drawn-out. A nicely concise setting out of some of the challenges that armed forces will face over the next decades.

But new? It sounds suspiciously like the thoughts of General Beaufre in the 1960sGerrie, not to mention some of the wars fought by Rome in the outer regions of its empire.

**Compound War**: This has been defined by Thomas Huber as the "deliberate simultaneous use of a regular main force with dispersed irregular forces".

How does that differ from Soviet co-ordination of conventional and partisan forces in World War II? Or from North Vietnam's co-ordinated operations by regular army units and local Viet Cong guerrillas, or the SADF's co-ordination of operations by conventional and special forces with Unita forces? Or, for that matter the co-ordinated employment of regular legions to face the main opposing force and local auxiliaries to disrupting the opponent's rear areas, as the Romans would seem to have done on occasion? There has also been an argument that the war in Afghanistan in 1980s was 'compound', in that there were hostile conventional forces to the Soviet's rear (NATO) and providing sanctuary to the south (Pakistan), and supplying the Mujahidin with modern weapons (Stinger).

**Complex War**: this is a similar concept that considers the challenge of a war in which there are multiple actors operating in the same theatre at the same time, with different agendas.

The Thirty Years War in Europe comes to mind here, but this is potentially a real issue for Africa, which is the last remaining practicable 'playground' for major powers. That could see several major powers, regional powers, local actors, multi-national corporations and criminal groups active in one theatre at one time. The present situation in the east of the DRC will seem simple by comparison. The recent fighting in the CAR was a not dissimilar situation at the strategic level, with Chad, China, France and Sudan – in alphabetical order! – all paying a strategic game of their own and/or in cooperation with one or more of the others, or believing that they were doing so.

**Hybrid War**: Colonel Frank G. Hoffman (USMC) has defined a hybrid threat as being: "Any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle space to obtain their political objectives", adding information and 'cyber-war' to the mix. US Army Colonel Bill Nemeth has defined 'hybrid war' as "the contemporary form of guerrilla warfare" that "employs both modern technology and modern mobilization methods", with the fighters transitioning from guerrilla to conventional operations as the situation suggests. He uses the examples of the Chechens in Grozny in the mid-1990s and the Hezbollah elements in South Lebanon in 2006, referring, for instance, to them grouping as "small fire teams and using guided missiles and other modern weapons". Several writers on the topic have made the point that such 'hybrid war' can include criminal activity, for instance poppy cultivation in Afghanistan to fund the operations of the Taliban.

This, too, sounds familiar, not unlike Russian and Yugoslav partisan operations in World War II, but it is important to note that Colonel Hoffman stresses that he is presenting ‘hybrid war’ as “a problem, not a concept”.

## Guerrillas and Electronics

Guerrilla forces worldwide make use of electronics for a wide range or purposes, including:

- Tactical communications;
- Operational communications;
- Strategic communications;
- Logistic communications – including electronic movement of funds;
- Remote bomb detonation;
- Reconnaissance (digital cameras, cellular telephones, i-pads, notebooks and laptops);
- Propaganda (interviews, social media, broadcasts and hacking into news networks.

Terrorist groups do the same; and so do some criminal enterprises, particularly the narcotics cartels, whose extensive international smuggling operations would be impossible to control in the absence of electronic communications means, and who have also used remotely-detonated bombs.

One anomaly to be considered here is the Hawala system of transferring funds that has been found to be commonly used by pirates and smugglers in northeastern Africa in particular: The system is based entirely on trust: You give $ x amount plus a handling fee to the Hawala man in your neighbourhood, with a contact number for the person who is to receive the funds in some other town or country; he contacts his opposite number in that town or country, and the person for whom the funds are intended can collect them from him the same day, less a small handling fee at that end. No sign of funds moving through the international banking system – and so no immediately practicable way of tracking those funds.

That said, intelligence services could focus on the telephone conversations – cellular, satellite or even skype – of Hawala dealers, but that will depend on good intelligence to being with and on massive collection and interpretation capacity.

## Communications

The first and most obvious area in which irregular forces have turned to electronics – as early as during WW II – is communications: The days of the ‘runner with cleft stick’ or messenger with a memorised message are long gone – or at least for now, with the likelihood of making a comeback in the face of improved COMINT intercept and tracking capabilities and, perhaps more particularly in the wake of Osama bin Laden being tracked and located – despite using ‘runners’ – to some extent precisely because those ‘runners’ used electronic communications.

Guerrillas, terrorists and criminal groups all make extensive use of electronic communication means to gather information, direct operations and arrange logistic support: Landline, cellular and satellite telephones; military radios, citizen band radios, e-mail, skype and messages left on web sites.

Considering some recent and current events: Look at photos of Seleka and M23 leaders and their immediate staffs, and note the numbers of cellular and satellite telephones and tactical radios. Also remember the third slide of this presentation, showing a tactical radio being used by guerrillas of the Ogaden Natinal Liberation Front.

Bear in mind, particularly, some of the more spectacular guerrilla operations of recent years in Africa – the 2006 and 2008 raids on Njamena, the latter involving at least 500 vehicles that moved along multiple routes on two major axes over distances of between 600 and 1 000 km, and formed up outside Ndjamena in the course of a single day, and the 2008 JEM raid on the Omdurman side of Khartoum. Operations like that cannot reasonably be conducted without radio communications.

Nor could, in most cases, the coordination of supply flights and later paradrop missions by the Sudan Air Force for the Lord’s Resistance Army and Allied Democratic Forces in the east of the DRC.

Consider also the guerrillas in Mali during their offensive in 2012, and operations by JEM – and the pro-government Janjaweed - in Darfur, those of the Oromo National Liberation Front in southern Ethiopia and Al Shabaab in Somalia. Or, for that matter, the now defeated Tamil Tigers in Sri Lanka – who also needed radio communications to collect supplies from ‘depot ships’ stationed a few hundred kilometres offshore – and the FARC in Colombia and the Zapatistas in Mexico.

In a different vein the Chechen terrorists who attacked the hospital in Budyonnovsk (1995), the Moscow theatre (2002) and the school at Beslan (2004), all had mobile telephone links to their home bases and all used ‘spotters’ with mobile telephones to keep them informed as to what the security forces were up to – from observation and from watching TV news. So did the terrorists who attacked Mumbai in 2008, and they additionally had tactical controllers in the town itself, who were in telephone contact with their commanders in Pakistan.

Some groups also make use of communications intelligence, at least as a ‘battle indicator’ or to track the movements of security forces, even if they cannot actually break into encrypted communications. That said, some of them probably can break into those communications: If a teenage hacker can break into US computer systems, what makes us believe that some well-funded guerrilla, terrorist or criminal group cannot crack the encryption of typical military communications?

Pirates, smugglers and narcotics syndicates are little different. Consider, just to take the two examples of narcotics smuggling by ‘go-fast’ boats and submarines, and the clandestine air freight operations used to fly ore out of the eastern DRC. All require telecommunications of some sort to coordinate and control.

## Communications: A Vulnerability

Those same essential communications links can also, however, prove a fatal vulnerability to guerrillas, terrorists and criminals:

- Unita leader Jonas Savimbi was tracked by a COMINT aircraft monitoring his satellite telephone, which enabled Angolan special forces to ambush his command party.

- Carlos, ‘the Jackal’ was traced to an apartment in Khartoum by his cellular telephone, with French and Sudanese special forces bursting in to arrest him and send him off to a life in a French prison.

Increasingly, intelligence services are also able to use telecommunications among members of the international terrorist groups to build an organisational picture of those groups and then to begin understanding them, tracking them, foiling them and sometimes spoofing them. Just as there is no ‘free lunch’ in business, there is no such thing as absolutely secure electronic communications: Sooner or later someone will break in, begin tracing the threads and build a picture.

## Guerrilla and Terrorist Propaganda

Guerrillas and terrorists – and some criminal groups – make extensive use of propaganda and the former two, indeed, often must do so to achieve their purpose.

Increasingly they use various electronic media for that purpose: The formal media, openly or by hacking into their systems or even transmissions; their own websites and by hacking into other websites; social media to spread their message; and, most insidiously, social media and e-mail to undermine the morale of the members of the security forces and their families

That, too, however, holds risk of being tracked over time and perhaps even being pinpointed at a given time and perhaps long enough to become vulnerable. Even if they avoid giving any live interviews, it can be possible to track journalists invited to interview them or move with them for a time by their mobile telephones and laptops. And while journalists may rightly be incensed that this undermines their function and potentially places them in danger, it is likely that few intelligence services will be put off by that.

And giving live interviews even holds direct risks: The Chechen leader General Dudayev was killed while giving an extensive satellite telephone interview by several anti-radar bombs that had been modified to home onto the particular type of telephone he was using: The journalist doing the interview was an intelligence officer in an EW aircraft accompanied by fighters that carried several such bombs – several because a hand-held satellite telephone is a rather more difficult thing to home on than an air defence radar.

Finally, of course, propaganda works both ways: Government agencies can broadcast their message on open networks, and can hack into the guerrillas’ networks from ground stations or from suitably equipped aircraft. The ‘airwaves’ are in this respect also just another battle ground, and he who seizes the initiative and keeps up the pressure will have the advantage.

## Cyber Operations

And then we come to the buzzword – ‘cyberwar’. That is, in fact, a reality: Both Estonia and Georgia have suffered deliberate attacks by Russian intelligence agencies and, so it is thought by some, also by Russian criminal groups working with those agencies (hardly unique to the Russians; remember the CIA cooperation with the Mafia?). Most major ‘western’ countries are also experiencing frequent, almost continuous in the case of the United States, attacks by Chinese military cyberwar units, albeit mainly conducting reconnaissance to establish future points of attack and conducting intelligence gathering, both against defence establishments and in the form of industrial espionage.

And the west is returning the favour: According to recently leaked documents, the various US intelligence services carried out 231 “offensive cyber operations” during 2011, three-quarters of them against “top priority targets” that included Iran, Russia, China, North Korea and also various bodies potentially involved in nuclear proliferation, as well as groups like Al Qaeda.

The US 2013 budget for “cyber operations” amounts to, according to those documents, which may not be comprehensive or even entirely accurate (remember the value of disinformation!) $ 1.02 billion, of which one-third is for defensive operations and the remainder, some $ 652 million, for offensive operations, such as GENIE, run by the Remote Operations Centre, and which plans to remotely place some 85 000 “covert implants” during 2013, in addition to the 68 975 that were already in place in 2011 and the 21 252 in place in 2008, a progression that nicely illustrates the expansion of this form of warfare and intelligence collection.

Interestingly, in 2011 the 1 870 staff of the ROC could only effectively monitor 8 448 of the “implants” in place, and additional staff are being recruited – as are contractors, one of whom was, of course, the major leak. The CIA equivalent of the ROC is its Information Operations Centre, about which less is known. In addition to the remote “implants”, the US also conduct “field operations” to physically place electronic devices or software in targeted computers or networks, but most work is in the form of remote “tailored access operations”. Some of the various operations are also initially passive, merely putting in place a “back door” for use in the future.

In this regard we might want to remember the rumour in 1991 that the French-supplied Iraqi air-defence command and control system was partly disabled by ‘bugs’ built into it by French intelligence services before delivery. Some years ago a Persian Gulf Army also found one of its communications nets mysteriously disabled by, as a technical investigation revealed, an apparently innocuous chip on one board in every radio that could be remotely triggered from an EW aircraft. Such aircraft had been in the area at the time, and an operator had suffered a little – definitely unintended – finger trouble. That country is believed to have changed radio and communications equipment suppliers since.

GENIE is to be complemented by TURBINE, which is intended to be able to manage up to “millions of implants”, and to conduct active attack operations if required. It is also intended to in the future have the capability to identify “selected voice conversations of interest”; not a new thing, but on a vastly larger scale. will also have the

Just one formal definition for interest: The US defines cyber-operations as being operations that are under taken “to manipulate, disrupt, deny, degrade or destroy information resident in computers or computer networks, or the computers and networks themselves”, and also to “harvest’ data and to “tunnel” into connected networks.

And to close section on a practical note, Estonia, which suffered the first Distributed Denial of Service Attack carried out on a large scale by another country, has responded creatively. In addition to various more formal steps, it also formed a cyber unit within the Estonian Defence League, a volunteer organisation. That was a deliberate decision by the Estonian military who understood, to quote the former defence minister, that many of the people best suited to this cyber environment were “not well suited” to the military environment. As he put it during a conference in Berlin, the members “range from teenagers with purple Mohicans, to 80-year old gentlemen in dressing gowns and carpet slippers; all they have in common is an interest in computers. They are supported by a cyber defence unit commanded by a regular officer, but mostly work from home, comfortably away from ‘spit and polish’ and the like.

Finally some words to consider from that same Estonian defence minister:

> “*We make immense efforts to become more interoperable. Have we ever considered that the more interoperable we become, the more vulnerable we make ourselves?*”

## Remotely Detonated Bombs

Returning for the moment to the more conventional, various guerrilla, terrorist and criminal groups have made extensive use of remotely detonated bombs.

Most of those were initially detonated by infra-red beams broken by the target vehicle, or by simple devices such as remote garage door openers. Later came radio detonation and then the very practical and very secure (barring an inadvertent wrong number!) system of a cellular telephone wired to the bomb, triggering it when dialled. Those bombs have been placed in the widest possible range of places, from culverts to parked cars and bomb vests worn by suicide bombers considered to perhaps be a trifle reluctant, all the way to bombs inserted into body cavities and even surgically implanted.

One extreme plan involved placing bombs in 350 locations in different parts of the world, all to be detonated simultaneously by means of a signal sent out from a central laptop.

## Guided Weapons and UAVs

Guerrillas and terrorists have long made use of various shoulder-launched infra-red homing anti-aircraft missiles, perhaps the most famous being the use of Stingers by the Mujahidin in Afghanistan during the Soviet occupation of the country. Closer to home we might remember the two Air Rhodesia Viscount airliners shot down during the conflict there, or more recently, an Ilyushin-76 downed at Mogadishu and the attempt in Kenya to shoot down a departing El Al airliner and the DHL freighter hit over Baghdad but able to carry out a scary emergency landing without loss of life.

More recent has been the use of guided anti-tank weapons, most successfully in the Lebanon against Israeli forces in 2006. That same year also saw the first use by a ‘non state actor’ of an anti-ship missile, which hit the Israeli corvette Hanit off Lebanon that June, although the very limited damage suggests that the warhead did not detonate.

The ‘bottom line’ here is that we must expect guerrillas, terrorists and even criminal groups to make more use of guided weapons in the future.

And some of those may be unconventional, for instance a remotely piloted model aircraft with a camera and transmitter to ensure accurate delivery, and small explosive charge for the intended assassination or ordinary terror-inspiring attack. Such model aircraft can be bought in many a hobby shop and are not very difficult to fly; many hobby photographers – let alone professionals, have fitted such aircraft with still or video cameras. So all that is left is to find a suitable explosive device to add to the package; hardly much of a challenge to guerrillas or terrorists, or even major organised crime.

# The Challenge of Military Arrogance

There is no greater risk to the security of a country than a military suffering from an overdose of 'can do attitude' and an inclination to despise its adversaries as incompetent. The only risk that bears comparison, is a military that is not honest towards its political leaders about its shortcomings and weaknesses, leading the politicians to take strategic decisions based on an over-estimation of military capabilities. Both are recipes for disaster, and both have been very clearly demonstrated in this country over the more than forty years I have been involved with the Defence Force.

But let us return specifically to the arrogance challenge: Most experts in electronics affect a mild disdain for the steam-driven infanteer types like myself, and for the 'old buggers', also like myself, who cannot even pretend to understand what it is that they are talking about, let alone actually doing.

That is fine, let them enjoy it every bit as much as the disdain the rough infanteers profess to feel for the 'lang hare en dik brille' in the laboratories.

But it becomes a potentially fatal weakness if, like the professional soldier who despises the sloppy and supposedly cowardly guerrilla or terrorist – until experience teaches him better – the professional military electronics specialist or defence scientist similarly under-estimates his opponent. That opponent may not have a PhD in physics, but that no more stops him – or her – developing and building successful devices than the lack of a haircut, proper military bearing, pressed trousers and gleamingly shined shoes prevents the guerrilla shooting soldiers or blowing something up.

No matter how weird he might look, and no matter how weird we might think his cause or his beliefs or despise him if he is a drug smuggler, that guerrilla or terrorist or smuggler may well turn out to be just smart enough to kill us.

And there is no excuse for allowing smug arrogance to bring about that result. Any more than there is for politicians to send soldiers into a 'fair fight'. Either is to betray the people we ask to put their lives on the line for us.

And, as a final caveat, remember that guerrillas and terrorists sometimes have big friends to provide the know-how and wherewith all they may lack; just like criminals can often buy or rent what or who they need.