WAR CRIMES AVOIDANCE & DETECTION: BATTLEFIELD MANAGEMENT SYSTEMS

By Nyagudi Musandu

Abstract

In today's world, almost any armed conflict involving national military forces or non-state actors, results in allegations of war crimes and calls for investigations and prosecutions. As continued penetration of the Internet in the society leads to ever more thorough scrutiny of military operations, the world's military forces are in a continuous struggle for situational awareness via their own network-centric Battlefield Management Systems(BMS). But in many publications on the subject matter, little attention is paid as pertains to improving the humanitarian conditions in the Battle-space. The focus for the moment seems to be geared towards the attainment of tactical military objectives, by conducting military operations against, seemingly virtual adversaries. Pragmatically speaking 'claiming that a war can be conducted without atrocities, is akin to claiming that a market can be free from fraud'.

Premise of the Paper

The focus of the researcher of this paper, was how humanitarian conditions can be improved in a battle-space by way of optimization of BMS, for attainment of a better human condition for both friend and foe, without compromising one's ability to obtain tactical military objectives.

Research Method and Background

A qualitative review of situations/publications on BMS, was carried out and was supplemented by additional reviews of other publications on related subject matter. The researcher utilized his experience in training personnel in tactical operations as a bench mark for relevance of selected publications. This experience spans not less than 20years of formal and informal exposure to tactical operations at various levels. The most recent 7years of experience include actual requests for advice and consultations by persons in difficult/challenging training circumstances – both from commander to operative level. The nature of examination of the commercially available BMS evaluated in this paper are dependent upon advertiser prioritized specifications.

The Analysis

The genesis of this analysis is the definition of our subject – the Battlefield Management System(BMS). It is a terminology that incorporates the hardware platforms, software environments,

network-protocols, sensors, data, informatics and system users. The concept is left loosely defined that it may qualify as many BMS as possible. An insurgent with a laptop, text transmission system, and tactical radio could qualify in the confines of this definition, as having a BMS of one form or the other - which can be enhanced by a wide range of database, geographical information systems and programming language compilers, that are readily available in the Internet for free-of-charge. It does not have to be a million dollar system provided by a well known IT contractor. But for a BMS to be efficient, it must have extraordinarily efficient and talented operators, at least at one or two of its nodes, if not all – these should be persons who can clearly comprehend and exploit, tactical information inflows. In many cases the most gifted persons is not always a military commander, and humility may go a long way in aiding smooth operation of a BMS.

The minimal skill sets for BMS operator to be qualified as competent are:

- possession of requisite Professional or Academic Information Systems Proficiency certification.
- A good grasp of the art of warfare, both historical and contemporary. This qualification is vital because a system user must fully comprehend what it takes for the adversary force to achieve what they have done to-date. An appropriate scenario would be that of someone with excellent Information Systems certification, obtaining a key trading position in a brokerage house, without understanding of concepts for avoiding risks such as leverage and trading margins.
- A proficient operator will understand the limitations of a BMS, to the extent that (s)he will be alert not to fall for surprises that come in through the 'cracks', 'crevices' and 'blind spots'.
- A proficient operator will search for information from the BMS and analyze it. If the requisite information is not available (s)he will demand that it be availed by the fielded forces or other personnel. Given the 'foggy' nature of any competitive battlefield, a good operator scans his/her fielded forces for various status reports, that may not be automatically generated.
- A good BMS operator can feel the pain, stress, injuries, distress and elation of his/her colleagues at other nodes. (S)he can fully empathize with other operators without compromising, the mental faculties that it takes to respond appropriately to the challenges that they are facing.
- A good operator must understand when, and how to call upon other resources, that may not be part and parcel of the core system. These could be other organization such as the Red Cross, or
- Within a few days(e.g. 2 weeks) of operational use of a BMS, a good system operator will have an

idea of new vital functions that could be incorporated. These may be specific to the ongoing operation or have general and widespread applications. Improvement could come by way of hardware platform retrofitting, software upgrades, fitting/upgrading of sensors, automation of routine operations, and last but not the least use of innovative concepts such as Artificial Intelligence, to achieve highly specialized functions.

Without these above mentioned skill sets, even the most advanced and reliable BMS can offer little assistance to a fielded military force. One of the greatest needs of professional military commanders, in today's battle-space is the desire to be informed of infringements against international law or likelihood of the same. But this may be problematic because of the nature of criminals or other persons in difficult situations, where they have to avoid even a semblance of self incrimination. Once this researcher was engaged in a lively discussion, he overheard someone he assumed to be a commander say, '...at times the reports you get from the field surprise you, and you wonder if those could really be your forces...' - Anonymous(2010). This statement was indicative of a felt need that could be achieved by way of a BMS, that incorporates enforcement/observance of International Humanitarian Law.

Evolutionary ancestors of the BMS are described in Wells *et al.*(1962), in p. 13 we get a feel of how spotting and reporting fed data to the high command – which was a defense filter center, where symbols were moved across tables to reflect the tactical situation. Communication was via radio or cable. At that time global positioning systems (GPS) such as those that were being miniaturized in the early 1990's(as illustrated in several pages of Armada(1990)) did not exist. Slow and inefficient was the system, and no real-time information was available for command and control application. Speed did not matter until supersonic jets and rockets featured prominently especially towards the end of the Second World War. Though at the time the limited range of these assets gave military commanders in the defense filter room some breathing space.

Wells p. 20 - 21, details importance of survival of friendly/local civilian populations, which could be enhanced by way of early warning – in relation to Ballistic Missile Early Warning Systems. If we are to believe that behind the iron curtain, were oppressed masses of humanity, who were seeking liberation – then more relevant is the question of their well being in the event of a retaliatory strike.

The focus of Wells(1962) is computer controlled Early Warning Systems for air defense application, which were coming into service in the late 50's and early 60's. A problem that was to emerge in the early sixties, and was to preoccupy the United States Air Force (USAF) well into the early 1970's during the Vietnam War, to the present day – was the question of how to use aerial combat assets in support of ground combat units. At the time portable computers may have been a non-existent asset and there were no fielded BMS systems that could tap int Aerial Combat Assets for tight control of Close Air Support operations.

The methods/modes of deployment of air power assets in support of ground forces during the Vietnam Conflict, left little or no consideration for civilian populations(the humanitarian aspect). In Yenne(1984) there are some insights into the application of air power in Vietnam with respect to civilian population. This oversight was indeed a costly one, as revolutionary warfare of the guerilla type thrives on support of local civilian population, more than anything else. Good relations with civilian populations is a primary asset in counter-revolutionary warfare, any conventional army today requires good relations with civilians in their areas of operations. These are summarized in *'Mao's Three Rules and Eight Remarks'* as detailed in Baylis (2007) and are critical insights into a revolutionary's mind, that can be tapped into by a counter-revolutionary.

Given the widely varying combat situations these rules and remarks can be incorporated as reporting parameters of a BMS, albeit in suitably modified format. The unique nature of human related observations, demands that commanders be prudent by evaluating feedback from multiple independent sources on the BMS and other open sources(where human rights abuses are report in great detailed).

Hon(2007) states situational awareness objectives that are incorporated into the doctrine of the Singapore Armed Forces, these entail real-time full coverage battle-space visualization; real-time analysis of tactical situations; well supported and prompt decision making; and efficacy of actions and reactions. Though these are in the context of combat operations, they apply very well to humanitarian situations within a battle-space. Sensors unlike manual data input devices offer enhanced capabilities for monitoring of fielded personnel. Helmet mounted cameras and other imaging devices, can be networked to the Command Center – these may send back photos in communication bursts(to avoid

tracking down of the wearer by electronic warfare units) and in some cases video streaming can be facilitated by automatic or manual controlled methods. The knowledge of what the soldier is doing, and where (s)he is located provides and incentive for tighter self-regulation by the war fighter, as repudiation and fabrication are no longer easy options. A BMS must be configured to deny its users or administrators the ability to destroy its records – at best such records must be copied on a real-time basis to other oversight bodies.

Though the primary drive behind the BMS is the attainment of tactical military superiority in the event of a conflict, but with its adaptive input devices, humanitarian objectives can be met to some extent via the same channels. But in most of the cases studies detailing the development of BMS, do not demonstrate the optimization of such systems for use in the humanitarian realm. The tactical networks are not relayed through or terminated at system nodes that are geared towards humanitarian missions in battle-spaces. In most of the papers on BMS available in the public domain, even the internal medical units of the fielded forces studied are not mentioned, this is surprising given the extraordinary preparations, that are required in order to properly attend to seriously injured war-fighters

Other probable applications include but are not limited to Tele-medicine instructions to fielded personnel when they cannot readily access the same medical services via the normal emergency evacuation channels.

A detailed description of the development cycle of a test BMS is given by Vertegaal(2001), a lot of emphasis goes into the systems engineering processes and field tests. Like many other BMS research papers, it does not mention the tough procedures such as those pertaining to the handling of prisoners of war. In today's world of aerial combat superiority, it is possible for relatively small ground units, supported by air power, to cause the surrender of large numbers of enemy combatants (well beyond the immediate resources and handling capabilities of a fielded unit) to surrender. An immediate implication would be the likelihood of mass murder by a victorious force not keen on handling prisoners of war or preventing civil strife, in their areas of operations.

Importance of incorporation of open sources into information inflows into BMS situational awareness modules is growing by the day – with the ever deeper penetration of the Internet. A number of BMS systems offer functions for accessing informative databases, to enrich the knowledge and situational awareness of their operators. Unless these systems have processes for automatically replenishing their contents from open sources such as the Internet, their utility may be limited. The world today has got millions of citizen journalists, human rights activists, who offer frequently updated information feeds on virtual platforms such as (micro)blogs.

While many of these persons are independent, unknown and unverifiable, continuous internet searches into any question as pertains to the situation on the ground at any geographical location on land, is likely to yield numerous results – these in turn enrich the situational awareness of a military force and when they are verified, they can be incorporated into the wider battle-space visualization picture. Since there may be no time for the war fighter to browse through search engines listings, Intelligent Agents such as web crawlers, which can be hosted in cloud computing environments can be prompted to search for and package information in formats that are readily usable in the field.

The intricate and rapidly evolving demands of most modern battle-spaces, may cause the need for the end user to have some knowledge as to how such a system may be configured, as and when the need arises. Information that can be readily obtained from the Internet searches can include but not be limited to :

- distressed civilian locations and conditions in urban or rural battle-spaces
- geographical profiling of criminal activities in the battle-spaces. (e.g. www.lracrisistracker.com which is used to document and geographically profile the criminal activities of the Lord's Resistance Army in East and Central Africa.).
- Psyops and public relations campaigns of an adversarial force can be analyzed for their operational insights
- Real-time or past layouts of battle-spaces may be detailed on the Internet
- Profiling information on the characters and behaviour of commanders or their fighters
- Tactical assets of adversaries could unintentionally be displayed on the Internet
- Emerging trends and key players of the battle-space could be detailed on the Internet

- Morale of fighters and their relations with local populations

Hartley(2003) clearly illustrates, why open sources are vital in conflicts. Often obscure and unknown persons and organizations, seek out journalists in order to publicize their causes, with a view to winning local or international support. Journalists in turn demand for news worthy material. It is a vicious cycle, that would benefit 'many-a-patient' Intelligence Analyst. From Hartley's autobiography, it is clear to see how those who followed his news outlets in the 80's and 90's would have obtained rare and valuable insights into the conflicts in Somalia, Ethiopia, Eritrea, Rwanda and some parts of the Middle East.

At command center level, where communication network bandwidth is not an issue, intricate internet searches can be done by online or desktop based intelligent agents. These can then be cleaned, summarized and sent to the war fighter in a readily usable format. Given the proliferation of hand held electronic warfare devices with functions such as emitter direction finders, it would be prudent that Internet Intelligent Agent configurations be done offline via text bursts and the feed back received in similar fashion, to reduce the electronic signature of the war fighter.

Armada(1990) on page 45 gives a good insight into the level of complex BMS systems available to NATO forces in countries such as France then, namely – Orchidée which was helicopter borne. At the time this system had got everything going for it – battle-space visualization, data-links of network-centric nature. Its only potential 'drawback' was the requirement of a helicopter airborne to facilitate its operations. That automatically assumes that you dominate the air space in uncontested fashion before the system could be deployed. But there is little if any indication of the humanitarian applications of the platform. But the publication offers some insights of the still disparate fire control systems, GPS, systems and other Command and Control tools, that are not marketed as independent systems today.

An interesting insight then appears on page 54, of the publication which highlighted the likelihood of the computer virus as a critical problem in today's ever more digitized military systems. It is not far fetched to assume that the prospect could arise for a war crime trial for persons who disrupt military systems by way of systems such as computer viruses or signal jamming, causing malfunction of such

systems that are critical in the delivery of humanitarian services, thereby resulting in quantifiable deaths in the civilian population within a battle-space.

If we study the Canadian approach to Operations as highlighted (Born, *et al*), in the 1990s, humanitarian concerns and peace keeping were the primary objectives. There was a drive to provide the civilian population with intentions of the Canadian military to facilitate the building of relationships that enable smooth operations in hostile territories. From the very onset the Internet was a capability that was in built into some of their command and control systems. But these newly emerging thoughts, concepts and systems were not formally deployed in difficult conflicts with serious humanitarian implications, that the Canadian Military was involved in such as those in Rwanda and Somalia in Africa.

Even if the humanitarian capabilities were readily meshed into Canadian Command and Control systems, the low literacy rates of local populations would have proved to be a formidable challenge. There were no micro-bloggers in Somalia and Rwanda, then unlike today. Email was barely available to international media and other foreign organizations. This is indicated by sources such as Hartley (2003), as he was well placed in the information industry at the time. Canada (1997) does not give a BMS as a source of information for the inquiry at the time. The theft of a National Defence Operations Center hard disk drive is an indication that there were no proper access control systems at the site and that the information system involved at the time did not have sufficient redundancies.

Even with the manpower, certain factors influence quality of Command and Control services via a BMS platform if one is to use it as a viable source for evidence, these are:

- Once there is suspicion of criminal or notable conduct in the field, multiple independent sources should be interviewed/interrogated for details, giving rise to a better situational awareness around which physical evidence can be obtained and investigations conducted at a later date.
- System logs and stored data(including audio/video files) should be safe from fabrication or repudiation, by way of the design of the BMS.
- Pre-event and post-event credibility assessments of field system operators are part and parcel of ascertaining the integrity/credibility of their work done on the BMS.

- A wide range of sensors and other peripheral devices should be integrated into the system to enhance the situational awareness picture. But care should be taken to ensure that data-link bandwidth is not overwhelmed, another problem may be the electro-magnetic signature of more data streams from more sensors, that causes concealment difficulties.

In the specification and implementation a BMS – the opinion of Parliamentarians in a country matters. Parliaments are critical in the establishment of BMS because:

- procurement/expenditure oversight role of Parliaments influences the types and functions of BMS by way of budgetary allocation.
- Parliaments may compel private enterprise or the military by way of questions or interpellation to submit BMS captured/recorded data to a Parliamentary Committee for incident investigations
- Credibility and professional assessment of top military commanders who are end users of a BMS is a concern for those implementing Parliamentary oversight.
- Ascertaining Value for Money and Timely delivery in public procurement.

Born, H.(2003) p. 38 cites the role of journalists in battle-space situational awareness, to the extent that they are targeted by (non)state actors, particularly in matters related to irregular warfare, as observed by *'Reporters Without Borders'*. Though it is not usually the intention of many a journalist to offer support to combatants in conflicts – their work is often exploited for purpose of obtaining a tactical advantage in a conflict. On p. 45 of Born *et al*. , there are some insights into gender related issues in the battle-space such as gender based violence and rape. Women and the girl child bear the brunt of such abuse and it would be prudent for BMS developers, to consider embedded procedures for countering such challenges.

Slightly more information needs to be gathered as pertains to women and children in the battle-space as they are often victims of abuse and may require special protection and treatment. Born *et al.*, goes ahead to summarize the work of the Commission of Inquiry(1996) into the deployment(1993) of Canadian Forces in Somalia, in the view of Prof. Dr. Donna Winslow, a Technical Advisor to the Inquiry.

Initial notable signs of wronging doing included acts such as :

- illegal beating and extra-judicial killings
- attempts to repudiate or fabricate evidence held by the Canadian military

Though evidence such as photos and videos of the wrong doing came into public domain, they were not based on formal information gathering procedures and standards of the Canadian Military at the time. One could only have attempted to alter/destroy evidence, on the premise that a contradictory and verifiable copy of the targeted evidence had not been gathered by and secured in a formally designed BMS, which had transaction logging capabilities. Unaccountability of the type that was experienced at the Canadian Military compound in Belet Huen, Somalia then – could today be minimized by technologies such as remote IP(internet protocol) video surveillance. Different officers could also be assigned the task of filing reports via the Internet to the High Command structures. These officers should not be known to each other, such that a form of independent verification may be obtained.

The CDA Institute report *'A Nation at Risk'* was indicative of a trend that had continued in budgetary allocations right from the 1990s. In this research, defense spending is analyzed in the light of international influence and sovereignty. At that time, availability of systems and equipment were not the only challenges facing the Canadian Military, another notable shortage was that of expertise. Given that recruitment of technical experts was a problem, even if there was a fully functional BMS in place, the staff to man and improve it were unlikely to be in place. Furthermore the operational parameters that the system was to monitor and control were also in short supply.

The problem of lack of sufficient budgetary allocations for BMS in the early 1990's is not unique. At that time the most common field computers were the Artillery Fire Control, Command and Communications system such as the ATILA from Cimsa Sintra which was then a Division of Thomson-CSF(African Defence Journal, 1987). These were short range radio systems – talk of networking extravagant nation-wide networks for battle-space management were not within the grasp of many. In the early nineties the Internet was beginning to make in roads into places such as Africa. The IBM – XT was still the main PC, and software systems such as Dbase III and Word Perfect, were the staple. There was no talk of wide area networks and commanders could still get their way around, even if not computer literate. Ben-Dor(1989) is indicative of a seemingly international trend then. In an interview

the Officer-in-Charge of Ground Forces, Israel Defense Forces at the time a Maj.Gen. Uri Saguy confessed that they had studied 'issues related to the automated battlefield and electronic warfare' and had come up with concepts, but these were yet to be then implemented due to budgetary constraints.

A factor that must have pushed the world ahead was the first Gulf War of Iraq against USA and its allies, which was prompted by Iraq's invasion of Kuwait. At that time international satellite News TV stations were coming online, and many military forces worldwide must have been dazzled by the sophisticated weapons and command systems at the disposal of the NATO (North Atlantic Treaty Organization) forces that were fielded. But in any event these were not priorities of old style African military forces, who were well stuck on classic warfare concepts that had been embedded into their services by their East Bloc or NATO trainers.

Parry (1985) went through the basics of Command, Control, Communication and Intelligence solutions. This was a publication that was widely circulated to African Military Commanders, many of whom were trained in the finest military institutions in the East Bloc and NATO countries. The article was pretty well researched, it even touched on concepts such as computers and information overload, and automatic data processing. The article was well ahead of its time for many African readers.

The researcher of this paper was privileged to have had access to a well placed person in an African Government, and who was trying against all odds to digitize vital information handling, within his organization. He seemed to understand that concepts such as telex were on their way out, and was at one time in the early nineties privileged to have hosted a Western doctoral student at his office, as the student filed his research reports from some kind of laptop over an international call. This convinced the officer in question (Musandu(1990s)) that there was some revolution of technology that could not be ignored in any sphere of government. But for 80's and 90's it is difficult to find any citations of use of computerized Command and Control systems by African military forces.

By the early 2000's almost every organization that mattered in Africa had acquired a computer and email address, military forces included. From around 1996 internet browsing was taking hold, in Africa and it must have dawned on military forces that this could be utilized for some operational

value. At same time many foreign trained programmers and system administrators were beginning to return and work in African military forces. But most in logistics and related managerial work. Though in the 60s, 70s, 80s and 90s, computers might have been used by African military forces, these were ready prepared as systems embedded in air defense control systems, etc. Adaptive programming and versatility of current computing systems was not easily available or widespread.

A typical BMS advert today covers issues such as:
- instances of use in actual combat
- exposure to rigorous testing and validation procedures
- display systems / graphic user interfaces and other aspects of human computer interaction
- easy data inputs via buttons, voice, etc.
- reliability of underlying communication network
- efficacy of current military users in obtaining objectives in combat

An interesting addition to a BMS system the Battle Hawk(cited), was the provision of linking it with other different BMS in the event of international co-operation, but it does not detail if the nature of cooperation envisaged includes that of the humanitarian type. It would be futile to talk of BMS and the potential for the humanitarian good, without examining issues related to the integrity of their software environments and hardware platforms.

Krekel (2009) offers deep insights into present day network security issues. Though the paper does not explicitly examine the issue of BMS, its focus is about vulnerability of information systems used by the U.S. Military and their partners as has been exploited by third parties in the past. It correctly states that information dominance is a precursor for dominance in the battle-space. To this extent a military force that has implemented a BMS that cannot be interfered with in any way by its rivals, is a step ahead on the way to achieving military dominance in a tactical operation, when it has considered the armaments and personnel of its opponents.

With the concept of cyber warfare in mind, a knowledgeable enemy force can impede or delay

deployments of one's forces in the event of a conflict. In the case that a force has been deployed, the interference against its BMS platform via cyber warfare could render it inefficient/ineffective. To achieve interference against a BMS system elements of Information Warfare and Electronic Warfare may be effected simultaneously. In today's military arena, the potential damage by way of such attacks has been greatly enhanced because military forces around the world are engaged in the 'Informatization' of their operations at all levels.

Cyber warfare operations affords a military rival plausible deniability – this minimizes the likelihood of a counter-attack, which may not be possible in the first place, as a victim usually lacks the knowledge to respond or prioritizes network security enhancement. Krekel(2009) explores the concepts of humanitarian applications via the BMS platform. The implication of cyber warfare against the BMS platform could be one of impediment of humanitarian operations, which would in turn lead to unnecessary deaths and/or suffering of civilians in a conflict area. BMS could have silent logistical systems embedded in their implementation – the benefits of these would be to order and prioritize logistics without the actual intervention of fielded forces.

Even with the threat of criminal litigation, a military force especially that of a super power nation may not feel obliged to obey international humanitarian law in the event of a major international conflict. This may stem from the fact that its military personnel can be shielded from investigations and prosecution, after such a conflict. A line of thinking that may greatly increase the likelihood of war if a super power's military command perceives that there is potentially extraordinary gain in military criminality of any nature.

A review of Krekel(2009) gives insight into recruitment and regimentation of cyber warfare cadres in China. If there is a war that has been lost by the West it is the Global Cyber War. There is a notion that is assumed by the researcher of this paper as pertains to cyber warfare – it states that 'Cyber Warfare has its manifestations from the physical world into the virtual world and out again into the physical world'. At the current rate and extent it is safe to assume that cyber warfare attacks have cost Western military forces many of the advantages that they had accumulated over the years by way of expenditure in the realm of research and development. An obvious problem is the lack of personnel for the roles of

command, intelligence, offense and defense in Information Warfare. The rivals of NATO forces have made considerable effort to bolster their force numbers from the ranks of the skilled criminal underworld.

Given these enhanced force outlays and the intellectual capital and resources, as well as chronological capital available to them by way of man hours, the potential for exploitation of network vulnerabilities is greatly enhanced. In countries that are currently at contest with NATO, governments seek to recruit anyone with skill sets of any type in relation to Information Warfare. But NATO on the other hand has been slow to respond in boosting its intellectual capital pool for Information Warfare. It has not gone out of its way to utilize existing laws for military reserves mobilization to tap into and control the hacker underworld that is resident in their countries.

If the news that we read is anything to go by, incidents such as that of *'Wikileaks Cablegate'* are indicative that the reverse of what China is achieving by recruiting young hackers is happening in the ranks of NATO – probably for reasons of poor indoctrination(an area where the People's Republic of China is known to posses great strength). Radcliff(2001) as conveyed by Badey(2003) is indicative of another Western weakness in this realm – the embrace of elitism.

Though most texts assume that the most crippling type of cyber attack on a Nation, is that which brings down its infrastructure – modern computer communication networks by their own design are resilient. An assumption that can be made is that if a computer network that is administered by competent staff is attacked, the maximum extent of damage shall be of a temporary nature. But financial/banking systems if hit by a paralyzing and simultaneous cyber attack, even the most complex economy would grind to a halt within hours. Military logistical systems and routine functions would be affected to the extent of termination within days if not hours. International Humanitarian Law does not allow for the nature of attacks that can bring financial/banking systems of a country to halt – the implication of such an attack would be to deny civilians who are not combatants access to funding for their food and medicine.

Countries such as China recruit personnel who have got prior strengths and predisposition towards

cyber warfare, then it trains and indoctrinates them, but the West seems to have a predisposition of recruiting personnel from elitist channels, after which it strives to interest and retain them in the realm of cyber warfare. To this category of staff, cyber warfare is not a way of gaining dominance/superiority in the battle-space, but a way of earning a living. This elitist approach to recruitment is illustrated further in Radcliff(2001), when she mentions the National Security Agency of the U.S. Government to have established an outreach programme dubbed the 'Centers of Academic Excellence in Information Assurance and Education'(NSA(2012)).

It is common knowledge that there are hundreds of young teenager code writers in the U.S.A., who already have well established practical experience in hacking into corporate and government systems – but they never get an opportunity to get advanced university education in Information Technology or to work for the U.S.A. Government in its military projects via channels such as State National Guards or Armed Forces Reserves. As detailed in USA(2010) late establishment of the United States Armed Forces Cyber Command in 2009 well after the People's Republic of China had established its centralized units command and control in this domain, is clear proof the the United States of America was playing and may still be playing 'catch-up' in this field of operations. It is notable from Radcliff(2001), that there was the establishment of unco-ordinated cyber warfare activities units by the United States Armed Forces around the early 2000's.

CASE STUDY OF A BMS INTENSIVE CONFLICT – 'Operation Cast Lead' Israel (2009).

'Fog of War' – In article 110 of Israel(2009), there are some initial insights into the issue of targeting militarily abused civilian sites. This discussion is carried on to several other pages of the document in great detail. To analyze this report well, we need a broad appreciation of the Israel Defense Forces. It is common knowledge that it is a highly digitized military force. That is not mentioned in this report but the inferences can be drawn from their methods of analysis of geographical areas.

Inevitably by deduction a good BMS must have the capability of giving geographical information distinctions between civilian and military areas. It becomes a priority of a prudent military commander to allocate recce/surveillance assets to monitor the civilian sites, that are likely to be abused by an opposing force, as it attempts to attain undue military advantage. Data streams from such

recce/surveillance missions are channeled into the BMS for analysis and action(if and/or when the need arises).

With monitoring of open sources via Intelligent Agent based systems, it may be possible for a military commander, to weigh the circumstances if there are civilians in distress, who are confined to a militarily abused civilian facility. But these open sources obtained via data streams would have to be subjected to further evaluation and monitoring by way of formal military recce/surveillance techniques before a decision can be reached. Provision of a geo-fencing type alarm function on a BMS can go a long way in raising alarms as a combatant enters an area that have be demarcated electronically on the system. Geo-fencing based warnings could be based on settings input by fighters who have recently ventured into an area. These settings could alert BMS users on likelihood of encountering civilians, booby traps, unexploded ordinance, snipers, or other enemy combatants.

On the military principle of proportionality when responding to aggression, human judgment and not the BMS is the primary determinant of proportionality and procedures. Even if a BMS was to provide serious artificial intelligence capabilities – its propositions would be assumed to be merely suggestions and not actionable commands. The reason for this perspective is very simple – almost all real battle-spaces in the world today are not sufficiently covered by sensors that may produce data streams that are of sufficient quality and quantity, which can be relied upon for decision making even of a non-autonomous nature – in matters pertaining to proportionality of responses.

Even if the hurdle of determining proportionality was to be overcome, the problem of developing appropriate software intelligent agents, that could probe sensors and analyze incoming data streams, would be present – each combat situation is usually unique and is not easy to fully anticipate. In effect it would amount to handing over combat decisions and military liability to computer programmers, who may not be soldiers as required by International Humanitarian Law.

A BMS system that is fully capable of perceiving all parameters in the battle-space, thereby analyzing/monitoring commander and operator inputs with feedback from the same, would be an interesting progression of Artificial Intelligence into the battle-space. This kind of system may have a

wide range of calibrations for gauging what may be excessive or acceptable, given a wide range of scenarios. Though a human being would have the final say on command, this type of Case Based Reasoning System, would assist a commander in making any necessary adjustments to his/her operations.

In the documentation of Israel (2009) it is very clear from the wide range of clearly labeled tactical aerial photographs(including those frozen from videos) and the analysis of real-time decisions that were made at the time, that the IDF had clearly labeled almost all buildings in the battle-space. Also discernible was what may be the probability, that IDF field commanders and pilots, are able to retrieve this information on a real-time, on-demand basis to aid their tactical decision making processes.

Sufficiently detailed labeling of the urban environment that is a battle-space, offers critical assistance to commanders, as they select which type of hardware and weapons that they can field. Use of artillery shells in an urban environment may be tricky because incendiary shells are likely to burn some type of structures and fragmentation blast type shell could cause casualties to civilians seeking shelter inside buildings.

The earlier stated function of geo-fencing the battle-space on a BMS could serve another purpose. It allows a field commander to identify an area and the nature of the population make-up in that specific area. Once this data is forwarded electronically by the BMS to the Central High Command, a method of communicating with civilians and opposing combatants in the area can be selected and effected. The nature of these communications can be logged into the BMS, to enable the field commander to retrieve them during future reference. If a system has got such versatility, then warnings to civilians and psyops, plus their related operations can be evaluated for efficacy upon interaction with the local population.

Interaction with local population shall normally be on a verbal basis, via radio, loud speakers, automatically generated phone calls and SMS messages, or even air dropped leaflets. A good BMS could offer facilitation for formulating opinion surveys and logging in the results, The 'hearts and minds' of civilians in an area should be of utmost concern to any prudent military planner. In fact

failure by locals to answer the questions verbally would be a matter of great concern.

CONCLUSIONS

A few lessons that we draw from this piece of research is that:

- Humanitarian aspects are often overlooked in BMS design and implementation
- Artificial Intelligence Agents enhance protection of civilians in a battle-space
- BMS programmers and system designers must be competent in International Humanitarian Law
- Artificial Intelligence offers the possibility of producing a BMS that can offer advice/suggestions to commanders in very complex combat situations via technologies such as Case Based Reasoning systems
- For autonomous weapons their programmers should be soldiers because their coders may be held accountable for some of their actions.
- The West is lagging behind in building up the military man power that is required in surviving in this age of Cyber Warfare.
- Data once input automatically into a BMS should be safe from repudiation or fabrication if it is to assist in regulating military conduct and military investigations.
- Krekel (2009) indicates that information technology supply chains have been compromised by the practice of recruiting cyber warfare staff from private enterprise.

BIBLIOGRAPHY

AFRICAN DEFENCE JOURNAL (1987). Military Information Monthly, No. 87 – November, 1987. *Societe Africaine de Publicate et d'Editions Fusionnees*, Paris, France.

Anonymous (2010). - Assumed to be a Commander.

ARMADA INTERNATIONAL (1990 June/July). *ARMADA INTERNATIONAL DEFENSE MAGAZINE.* Publisher: Karl Schwegler, Zurich, Switzerland.

BATTLE HAWK. Battle Hawk C4I Software and Systems
http://www.rovis.info/cdci/pdf/A4%20Battlehawk.pdf
http://www.cheltondcweb.com

Baylis, J. (*et al*) (2007). 'Strategy in the Contemporary World - 2nd Edition'. Oxford University Press, Oxford, U.K.

Ben-Dor, Charles (1989 Summer). 'Ground Forces HQ – Combined Forces At Every Level'. IDF Journal , Number 17, Summer 1989. Israeli Ministry of Defense.

Born, Hans (*et al*) (2003). '*HANDBOOK FOR PARLIAMENTARIANS No. 5 – 2003: PARLIAMENTARY OVERSIGHT OF THE SECURITY SECTOR – Principles, mechanisms and practices*'. Geneva Centre for the Control of Armed Forces & Inter-Parliamentary Union, Geneva, Switzerland.

Cameron, Mr. Fred (2005). '*Remote Sensing, Geographic Information Systems, and Operational Research in Urban Operations*'. Canadian Army Journal. Vol. 8.1 (Winter 2005). pp 31 – 38.

Canada, Government (1997 July). '*Report of Somalia Commission of Inquiry*'. Minister of Public Works and Government Services, Canada.

CDA Institute (Conference of Defence Associations Institute) (2002). '*A Nation at Risk*'. http://www.cda-cdai.ca/cdai/uploads/cdai/2008/12/nationatrisk_2002.pdf

Hartley, Aidan (2003). 'The Zanzibar Chest – A Story of Life, Love and Death in Foreign Lands.' *Atlantic Monthly Press*, New York, USA.

Hon, Pang Hee (2007 June). "C4ISTAR: Enabling Warfighters – Battlefield Management Systems: Perspectives from Singapore. *RUSI DEFENCE SYSTEMS* June 2007. RUSI(Royal United Services Institute – www.rusi.org). pp. 102 – 104

Israel, State of (2009 July). '*The Operation in Gaza (27 December 2008 – 18 January, 2009) – Factual and Legal Aspects*'. Ministry of Foreign Affairs, State of Israel. http://www.mfa.gov.il/NR/rdonlyres/E89E699D-A435-491B-B2D0-017675DAFEF7/0/GazaOperation.pdf

LRA (Lord's Resistance Army) Crisis Tracker Website – www.lracrisistracker.com

Krekel, Bryan (*et al*) (2009). '*Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation – prepared for the U.S. - China Economic and Security Review Commission*'. Northrop Grumman, VA, U.S.A. http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

Musandu, Shadrack. (early 1990s).

NSA (2012 April). http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

Parry, Don (1985 May). 'C3I – The key to success?'. *AFRICAN DEFENCE JOURNAL (1985).*

Military Information Monthly, May, 1985. Societe Africaine de Publicate et d'Editions Fusionnees, Paris, France. pp.64, 65

Radcliff, Deborah (2004). 'Info War Games'. Paper as carried in: Badey, Thomas, J. (2003). '*Violence and Terrorism 03/04 – Sixth Edition.'* McGraw-Hill/Dushkin, Guilford, Connecticut, U.S.A. pp. 191 -194

USA(2010). *United States Cyber Command* http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf

Vertegaal(MSc.), Mrs. Merel (2001 June). 'Development of a Battlefield Management System: how to user the user. *TNO Research*, the Hague, the Netherlands. http://www.dodccrp.org/events/6th_ICCRTS/Tracks/Papers/Track2/003_tr2.pdf

Wells, R. (*et al*) (1962). '*EARLY WARNING – Electronic Guardians of Our Country*'. Prentice Hall, Inc., Englewood Cliffs, N.J., U.S.A.

Yenne, B. (1984). '*THE HISTORY OF THE US AIR FORCE*'. Bison Books Corp, Greenwich, CT, U.S.A.

Article Date: 29th April, 2012

About the Author

Nyagudi Musandu is an Independent Security Analyst and Forensic Criminologist based in Nairobi, Kenya – East Africa.
