CENTRE FOR LAND WARFARE STUDIES, NEW DELHI

NATIONAL SEMINAR ON CYBER WARFARE

CHANGING CONTOURS OF WAR FIGHTING

Cyber Warfare training for the Indian Armed Forces – A fresh look

By Marc Kahlberg,

CEO and Managing Director,

Vital Intelligence Group, Israel

The integration of Cyber Specialists and Legal Experts into Cyber Warfare Units is as natural as the new Cyber warfare tools that are emerging from what once was a secret domain. The conflicts that are already taking place in the cyber space are only an additional tool or weapon that allows for the enhancement of physical combat capabilities of future battles.

While many nations scramble to establish cyberwarfare centers a and are still undecided as to if cyber defense units should be integrated with cyber intelligence units, others, mostly the nations with bigger budgets and higher risk are already active and have cyber units embedded into filed units as well as command headquarters.

Cyber defense and Cyber offense are not the same and neither should they be categorized as such. When Cyber units are required to deliver effects and derive results against an enemy (let us use ISIS as an example), they should be able to protect themselves from an attack but at the same time and with no interference from the defensive interface be able to deliver offensive methods such as altering electronic communications for example.

Today's offensive cyber weapons and highly skilled cyber personal should be of key interest to not only nations constantly under threat but emerging nations as well. For many years countries like China,

Russia, the US and perhaps India, Israel and others may have been deploying various cyber self-defense tools or counter espionage tools and tactics as part of their overall cyber operations. The nations with the best tools and most advanced cyber minds are certainly in the forefront of today's cyber war.

In taking a fresh look at the cyberwar risks and threats that national leadership and certainly the protectors of India face, like Israel, the leadership should be looking at the advancing tools, the education and the teaching of a new cyber syllabus that should be compulsory and part of every facet of education like mathematics or English for example.

As in the physical world of espionage or terror and organized crime operations, deception has always been a key tool. Cyberspace provides an almost stealth platform for many an attack or hack, it has also become a global language feeding social media and chat platforms with vast amounts of information and disinformation. Where the speed of this expanding big data mass of digital information frenzy or perhaps an orgy of disinformation can have devastating effects on critical and strategic infrastructure, organizations, people, places and indeed cripple economies and make or break governments, let alone provide the underground organized criminal world with tools that hurt and affect even the most innocent of children in the form of human trafficking and pornography. Having said this we must all admit that we are indeed in the midst of a cyber war with only more devastation to come.

In training and practicing for future cyber wars or indeed any war, it is imperative and extremely critical to put well planned concepts together for combatting and counter attacking cyber aggression. The cyber battlefield is perhaps invisible to the naked eye in a sense but it is clear that cyber deployment into this battlefield must be initiated and integrated in order to succeed.

We must realize that the key to success is in theory and practice is precision, predictability and maximum effect with obvious deployment of defensive methods for networks and communications but all of which are impossible without the necessary selection and training of top class personal for this complex mission.

In establishing The Vital Intelligence Group, I understood that my skills in the physical security sphere were indeed of the highest level, my training and background within the Israel National Police provided me with experience and knowledge, not taught in textbooks but in the field and in dealing with the consequences and effects of being physically present at 16 deadly terrorist suicide bombing attacks culminating in my creating and developing the "Secure Zone Concept". This concept is known today globally as Safe City and recently the terminology Smart City has edged forward in our daily language. I also understood that I was lacking the Cyber aspect while trying to prevent and thwart terror and stop the organized and petty crime that hurt so many. As policy and protocol in any advisory capacity, I believe and always ensure that my clients understand that combining and fusing together both physical and cyber aspects of security with a mindset of having a good defense must culminate in having an even better offense.

Today, the Vital Intelligence Group delivers advanced tools focused on Cyber Intelligence, Cyber defensive methods and indeed integrated advanced training. The fusion-key of procedures lie in the concept and design of each plan of action. The methods, strategies, tactics and understanding of cyberwarfare lies squarely on preparation, planning, education and training in the undefined and borderless digital cyber battlefield we live in.

On the 4th May 2017, the Times of Israel reported that Israel was upgrading what is known as one of the worlds most coveted military intelligence units that are responsible for protection and as per the report counter attacks. In taking a fresh look at the way Cyber warfare training is conducted one should first look at who should be trained in the first place.

Selection of the right people with the right backgrounds is critical. In creating and delivering these people who will manage and constantly upgrade the cyberwarfare platform program, there will always be a requirement for a distinct combination of attributes such as computer skills, high cognitive scores and scientific thinking. Motivation, moral value, team work and personality are all important traits for this specific skills sect. Intense social simulations in which candidates can be put to the test under a high-pressure leadership position is an important aspect of selecting the right candidate. Cyberwarfare Candidates must be creative, intelligent, and inventive with the ability to move from one area to another, and be able to take leadership in a group while being part of that group amongst other traits. Their moral values and willingness to make a contribution to their country and society should be of the highest esteem and of course the will to learn and be taught.

Cybersecurity is an area in which Israeli special units have indeed made their mark. In August of 2011, the newly created Israel National Cyber Bureau (INCB) was established. This bureau was set up to provide the prime minister with advice on managing a new and crucial threat, against which both defensive and offensive strategies would be needed. It was noted by the head of the INCB back in 2011 that cyber-attacks would be “a broad threat to human society”. These threats were seen as a challenge to the state but they also became an economic opportunity. The more invested in academia and industry, the greater the return the country would receive, from both economic and security perspectives. Prime Minister Netanyahu agreed, saying, Israel is a significant force in cyberspace, just as we developed the unprecedented Iron Dome system that successfully intercepts missiles, we are developing a kind of “digital Iron Dome” in order to defend the country against attacks on our computer systems. The INCB is designed – first and foremost – to organize defensive capabilities based on cooperation between three elements: Security capability, the business community and the academic world.

It was only last week when the Indian Prime Minister made an historic visit to Israel where he was with Prime Minister Netanyahu and on the agenda amongst other issues was possibly defense and Cyber. Both Prime Ministers obviously realize that cyber warfare is becoming more aggressive, intense and dangerous, and the tools and education available should be used now for developing a well-planned, effective, comprehensive and long-lasting response.

As Cyber weapons are constantly advancing and the hackers are always looking to locate a new vulnerability in their victims' defenses, where national borders are nonexistent. Just as Cyber terrorists don't respect borders or obey rules democratic governments should meet every attack with a counter attack. As in all law enforcement or military doctrine the conducting of intelligence and the ground work carried out is at times offensive, it must be the same in the cyberwarfare environment.

Israel and no doubt India are at the forefront of countering cyber -attacks. Both countries have an abundance of enemy elements who wish to cause harm. In Israel the size of the country does not allow for error and as in the doctrines of military and indeed some law enforcement strategy convey that both nations are understanding that only a proactive holistic approach towards cyber security and countering the cyber-attack is an option.

In summary cyber is changing the way conflicts and combat unfold on a daily basis, and many of the principles of kinetic warfare can be translated into fighting the ongoing-evolving cyber threat. We must prepare for the future generations and understand that cyber warfare starts as early as pre-military basic training. Just as a 16 or 17 year old learns to drive or a new conscript learns to assemble or dissemble a weapon or a 4th grader learns to search google, Cyber warfare education must surely be categorized as these basic educational elements of tomorrow.

As the Israeli military is assisting is raising the next generation of Cyber professionals, so probably is India. However with outside industry related assistance Israel's military is focused on a special programs for smart high school kids and in recent years, the Israel Defense Forces has given cyber warfare, both defensive and offensive, special attention. Teaching kids cyber skills is a national mission. Ongoing and new training programs always prepare children for careers in military intelligence, defense agencies, the high-tech industry and academia.

The training programs have led Israel to become a world leader in cybersecurity and cyber technology by placing its focus on the country's youth. There is a national center for cyber education, designed to increase the talent pool for military intelligence units and prepare children for eventual careers in in all sectors.

Israel has long branded itself the "Cyber Nation" and the threat of possibly facing a shortage of cyber experts to keep up with the country's defense needs and keep its cybersecurity industry booming the Country is starting young and fresh. Building up a wellspring of select talent, Israel is teaching children the basic building blocks of the web such as India can and should be doing.

We should consider that for years, cybersecurity and indeed physical security experts have warned that high-stakes cyber -attacks and hacks are inevitable – It is a matter of when, not if.