Capacity Building for Fighting Cyber Wars

–Inderjeet Singh Barara,
Chief Cyber security Officer, Vara Technology, inderjit.barara@gmail.com

Cyberspace is growing at a speed unprecedented by any other commodity. Almost three billion people are now connected to the Internet through cyberspace; a figure growing rapidly and estimated to reach 5 billion people, using 50 billion IOT devices, by the year 2020. Today's critical information infrastructure networks are key targets for cyber attack because they have grown to the point where they run the command and control systems, manage the logistics, enable the staff planning and operations, and are the backbone of the intelligence capabilities. More importantly today, most command and control systems, as well as the weapon systems themselves, are connected to the Global Information Grid (GIG) or have embedded computer chips.

"Cyber is a key enabler of Information Warfare and unlocks Pandora's Box on the battle field"

Airplanes have become flying routers receiving and sending targeting information constantly. Air Defense and Artillery are guided by computers systems and they shoot smart munitions that adjust their flight based on Global Positioning System (GPS) updates to guide themselves to the target. The Intelligence Surveillance and Reconnaissance (ISR) systems gather so much information that the challenge is shifting through it to find the critical data. Today's infantry squad has communication gear, GPS, tracking devices, cameras, and night vision devices. It is both our strength and could be turned into our weakness if taken away. The loss of GPS satellites would take away many of our advantages on the battlefield.

Cyberspace is a new battlefield where no country is immune to the threats that its user entails. With rapid growth, there come possibilities in development and new ways to empower people through cyber war: however, this is accompanied by new vulnerabilities, risks and challenges. Cyber Capacity building of Cyber Army to safeguard the networks has become utmost important. It is also pertinent to understand the generations of warfare as discussed by (Lind, Nightengale, Schmitt, Joseph, & Wilson 1989)

a. **First Generation warfare**: The tactics of line and column i.e., the line with maximum fire power wins;
b. **Second Generation warfare**: Based on fire and movement i.e., massed firepower replaced mass manpower;
c. **Third generation warfare :** Based on maneuver rather than attrition i.e., non-linear conflict, outwitting the enemy; and
d. **Fourth Generation warfare:** Includes the whole of the enemies society, not just the military i.e., this leans towards a terrorism and guerrilla ideology where one does not know who or where the enemy is.

With this in mind, from a non-conventional point of view "Today's military commander must have an understanding of his cyber footprint that is every bit as sophisticated as his knowledge of the terrain, the forces at his disposal and the makeup of the enemy." (Carafano 2013).

As cyber attacks have increased and there is increased awareness of vulnerabilities, there is more demand for professionals who can stop such attacks. But educating, recruiting, training and hiring these cybersecurity professionals to be skilled for fighting cyber war takes time.

How Cyber Warriors Assist Military Forces

A military cyber army is a highly skilled information technology group of soldiers i.e., "cyber warriors" who have a vast understanding of cyber skills, are able to defend military and strategic government critical infrastructure, and can launch cyber-attacks. Cyber defence in the military includes a defensive role that ensures that the military and government computer networks are secured and neither are compromised via internal or external threats. The offensive role includes the proactive and reactive launch of offensive cyber-attacks using cyber weapons against adversaries, to destroy, exploit, corrupt, or collect information for intelligence.A cyber army's mission is to fulfill these roles for the military. The cyber army could givethe decisive edge on the battlefield with regards

to information collection, hardening of technology and communication computer systems within the military and government cyberspace to execute cyber defence and launch cyber offensive attacks against an adversary nation.

Cyber Warriors' Strategic Value to a Nation State.

A cyber army will be able to add value to a nation state by aiding in establishing strategic direction about the development of cyber policy and cyber strategy. It will have the capability to effectively safeguard national critical information infrastructures, and to executeand contribute to the national cyber threat analyses. Cyber armies will also be able to aid in securing the national cyber space to ensure cyber peace. Cyber armies will develop cyber weapons and capability to react quickly to cyber threats and execute proactive cyber policing of the incoming and outgoing data within military and government networks and develop cyber-attack prediction portfolios.

Legality of Cyber Warriors

The legitimacy for nation states to have a cyber-army in their military is justified due to the threat of the global explosion of cyberspace. A nation state has the right to protect itself and defend itself from another nation state if attacked via a cyber-attack. The biggest challenge is to determine when a cyber-attack will change into war and how to establish attribution: who the aggressor was. Detailed planning to launch a cyber-attack against a nation state is vital, thus, the collection of information is critical and the convergence to intelligence is vital. Cyber armies must be seen as legitimate within a nation states' strategic military arsenal in which control and defence of a nation's cyber infrastructure can be safeguarded against malicious intent. Research and development and offensive capabilities are also fundamental within a cyber army.

The Tallinn Manual on International Law applicable to Cyber Warfare (Schmitt 2013) was initialised by the NATO Cooperative Cyber Defence Centre? of Excellence via a group of legal experts. This manual has currently not been adopted internationally. The manual pertains exclusively to Cyber Warfare and includes the law of armed conflict, rules of engagement and the Geneva conventions that most nations adhere to in times of conflict and military intervention. There are 95 rules that range from sovereignty, jurisdiction and control to the use of force, self defence, attacks, espionage, blockades and zones, as well as objects that are indispensable to the survival of the civilian population.

The manual emphasizes cyber to cyber operations as well as both international and non-international armed cyber conflict; when to launch a cyber-attack on a nation's critical information infrastructure or to target an enemy's command and control system. This manual does not discuss a kinetic attack to cyber-attack i.e., precision bombing on a cyber centre (Schmitt 2013). There has, however, been a call for nations to adopt a common universal law and understanding on what the rules should be to conduct cyber operations against other nations. Although most nation states have not adopted a universal cyber law yet, they have implemented cyber policies and internal cyber laws within their nations.

Cyber Army Operations

A logical deduction on how cyber armies operate in general is that there needs to be a target or an objective, strategically identified, of which the attack or defensive target tree is drafted with contingencies. Techniques, Tactics and Procedures (TTPs) are then used to collect information by means of various software tools, or techniques i.e., phishing and spear phishing attacks, Advanced Persistent Threats (APTs) or rouge applications or patches are deployed. From there, cyber weapons are deployed stealthily so as to execute the desired effect i.e., a zero day exploits, malicious code etc. After the desired effect is reached, cyber weapons can be destroyed or reused, if not detected. When detected, re-planning anddevelopment ofan alternativeattack or a defensive targettree is to be appreciated, or else revert to a contingency. Thereafter, the cyber operation is complete.

The cyber army must be under strategic military command to comply with the fundamental composition and elements of a cyber army to ensure strategic direction. Cyber defence will be a huge investment for the nations due to the necessity to develop defensive technologies and offensive cyber weapons. The cyber operations centre component must have the following elements:

a. Defensive component which must be able to execute cyber defence within the military and government and that is linked to a cybersecurity policy and the national cyber defence infrastructure;
b. Offensive component is a valuable military resource used as a platform to launch cyber offensive operations; and
c. Encryption and crypto analysis are vital to secure the military and governments incoming and outgoing classified information.
d. Cyber intelligence component is vital for the collection and analysis of the cyber space to provide a view on the cyber threats and vulnerabilities against any nation state.

World's Five Most Prolific Cyber Armies

The number of hacking attacks on governments and institutions has grown rapidly over the last decade.

While some cyber armies are officially created and operated by governments, others operate independently, while others occupy a murky in-between. Following are five of the world's most prolific cyber armies:

a. The People's Liberation Army Unit 61398

AKA: 61398, "Byzantine Candor"
First approximate appearance: 2004
PLA Unit 61398 is the Military Unit Cover Designator (MUCD) of a People's Liberation Army advanced persistent threat unit that has been alleged to be a source of Chinese computer hacking attacks.Its operations are considered a state secret, and officials have denied all allegations, but Unit 61398 of the Chinese Army is widely believed to be actively involved in cyber crime and espionage.

b. United States Cyber Command

AKA: USCYBERCOM, ARFORCYBER
First appearance: 2009
Most known for being the first government agency to officially acknowledge that it intends to build offensive cyber capabilities. Although the US government has experienced cyber attacks as far back as 1998, it did not create a unified cyber army command until 2009, instead relying on information security from the NSA and the CIA. However, its cyber capabilities have been rapidly accelerated since then, creating a fighting force that's expected to reach 6,000 people by 2016. This force is aimed at not only defending US public and private networks, but being able to destroy and sabotage adversary's systems and cyber capabilities.

c. Russia's shadow hacker network

AKA: "Net NGOs"
First appearance: 2007, although allegations of online propaganda "brigades" go back to 2003.
Most known for Distributed Denial of Service attacks on Estonia in 2007 and Georgia in 2008, shutting down government websites and services. Russia has only very recently announced the creation of a cyber warfare unit in its armed forces. However, it has long been expected of coordinating a patchwork of criminal and volunteer hackers that can carry out its bidding, hacking into foreign government and company websites.

This includes the Russian Business Network, a notorious hub for cybercrime such as child pornography; spamming and identity theft as well as members of the pro-Putin youth group Nashi.

d. Military Intelligence Unit 8200

AKA: 'Unit 8200, "eight-two hundred"
First appearance: 1952
Most known for 2009 Stuxnet worm that sabotaged as many as 1,000 nuclear centrifuges in Iran, delaying its nuclear program.

Operating in tandem with Israel's highly advanced civilian tech sector, Unit 8200 of the Israeli Defence Forces is something of a combo of the NSA and USCYBERCOM.

It has existed since 1952, conducting electronic surveillance both inside and outside of the country. In recent years, however, coinciding with the boom in the Israeli high-tech industry, Unit 8200 has grown to several thousand soldiers, capable of both cyber defense and offense.

Many of its efforts are concentrated towards its rival Iran, including the Stuxnet worm and the Flame virus that allows operators to monitor a computer users every move.

e. Syrian Electronic Army

First appearance: 2011
Most known for posting a graphic propaganda video on the Twitter account of President Obama's campaign group

Perhaps the least sophisticated of the organization on this list, the SEA makes up for it with sheer persistence. The group, which supports Syrian President Bashar al-Assad, has carried out hundreds of denial of service and defacement attacks against foreign websites.Targets included the sites of Harvard, the New York Times, the recruiting site for the US Marines, Microsoft, and eBay (Wikipedia has a more complete list).Attacks mostly consist of hacking the front end of the website to display pro-Assad propaganda, but the group has also temporarily shut down sites and posted fake Tweets and YouTube videos. It is not clear how closely related the SEA is to the Syrian government though it's suspected that many are based outside of Syria and are proficient in English but their loyalty to Assad is unquestionable.

Considerations for Capacity Building a Cyber Army

Following considerations are to be taken into account when forming a cyber army:

a. Cyber threat to the nation and vulnerability analysis.
b. Cyber defensive and offensive policy, strategy and legislation.
c. Cyber readiness of the nation state.
d. Connectivity and cyber space of a nation.
e. Cyber skill levels and cyber researchers.
f. Cyber educational level in secondary and tertiary facilities.
g. Cyber weapon development.
h. Co-operation between the security cluster and judicial departments, buy in and top cover from government.
i. Recruitment of possible external and internal specialists, and the holistic profile of people to be recruited.

With the above in mind there is a need for strategic level thought process to ensure understanding of what is expected of a cyber army as well as its mandate, role and functions.

Roles and Functions of a Cyber Army

The role of the cyber army for any nation will be the protection of cyber sovereignty of the nation state, specifically, for the protection of the military, government and civilian cyber information infrastructure. The functions of the cyber army could be:
Policy, strategy, doctrine and governance of cyber army.

a. Establishment of a centralised cyber command capability.
b. Ability to research and develop within the cyber environment.
c. Building offensive and defensive cyber capabilities.
d. Execute encryption and crypto analysis.
e. Sustainment of the cyber command capabilities, planning, coordination and execution of cyber operations (offensive and defensive).
f. Liaison between role-players from the cybersecurity cluster
g. Intelligence collection and analysis in the cyber domain.
h. Employment of cyber warriors.
i. Training and capacity building of cyber warriors.
j. Collaboration with external cyber specialists.

These functions will allow cyber army to have direction and purpose within a military organization.

Certifications for Cyber Warriors

There are three main types of certifications to be found across the technical computing industry:

a. Those that are vendor neutral and sponsored by a collective of organizations,
b. Those that are vendor neutral and put forth by a single organization, and
c. Those that are vendor specific and launched by the vendor itself.

In the general information security field the single certification that holds the most weight at present has to be the Certified Information Systems Security Professional (CISSP®) from the International Information Systems Security Certification Consortium (ISC)2®. The CISSP®, although considered to be a management certification has become the gold standard against which security professionals are weighed, and without which a job above entry level might be very difficult to find in the industry.

Also of note, in general information security certifications are a variety of offerings from the SysAdmin, Audit, Network, Security (SANS) Institute, with certifications provided by Global Information Assurance Certification (GIAC), the certification body associated with them, as well as the offerings from the Information Systems Audit and Control Association (ISACA).

In the penetration-testing field, certifications are somewhat fewer and farther between. A relative newcomer to the penetration testing certification cadre, and one that had gained a considerable amount of attention is the Offensive Security Certified Professional (OSCP), a certification created by the same group that develops the BackTrack pentesting Linux distribution. The OSCP test consists largely of being able to successfully attack and exploit a number of systems in order to retrieve specified information, a scenario much more closely matched to what we might find in a cyber warfare operation.

In the forensics field, we can again find several offerings from SANS/GIAC (there does seem to be a pattern forming here), in a few different subspecialties of forensics

Offensive skills

Offensive skills are somewhat more specific and focused in the direction of attack and, as such, do not overlap with quite as many non-security fields, although they still do to some extent. The set of skills found in hackers (ethical or otherwise) and penetration testers maps almost directly across, although with a slightly different focus and rules of engagement. The skills of fields such as network engineering, development, and others can also be of use here by changing the goals from keeping infrastructure, systems, and applications running to taking them down.

Defensive skills

Defensive skills are already rather prevalent in the computing industry in general, although generally not with the sole focus of withstanding a concentrated cyber-attack from a determined enemy with the resources of a nation state to back them. These standard skills are found in system administration, penetration testing, network engineering, and many other common areas. Although, they are skills found in most IT departments, we are less likely to find individuals that have the particular focus of defending against a large scale attack, outside of a few major providers or hosting services that have been through such trials already, such as Akamai, a company that provides, among other things, hosting services for many large companies, and is attacked quite regularly.

Conclusion

Cyber warfare is a reality and it is important that there is a cyber-army implemented in the militaries with a

mandate to execute defensive and offensive actions. A cyber army will ensure that the surfaces and gaps in the cyberspace are contained for nation states to be able to ensure cyber sovereignty.

Demand for trained cybersecurity professionals who work to protect organizations from cybercrime is high nationwide, but the shortage is particularly severe. Thus, the recommendation is that nation states need to invest in enabling a cyber army in a military so as to gain a favorable advantage on the battle field and to have a strong defensive national cyber space.

1. Cyber Armies: The Unseen military in the grid. Available from: https://www.researchgate.net/publication/283697882_Cyber_Armies_The_Unseen_military_in_the_grid [accessed Jul 01 2018].
2. Lind, W. S., Nightengale, K., Schmitt, J. F., Joseph, W. S., & Wilson, G. I. (1989). The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette(October 1989), 22-26
3. Carafano, J. J. (2013). Fighting on the cyber battlefield: Weak states and nonstate actors pose threats. The Heritage Foundation. Retrieved 08 Jul 2018, [online] https://www.heritage.org/defense/commentary/fighting-the-cyber-battlefield-weak-states-and-nonstate-actors-pose-threats
4. (PDF) Cyber Armies: The Unseen military in the grid. Available from: https://www.researchgate.net/publication/283697882_Cyber_Armies_The_Unseen_military_in_the_grid [accessed Jul 08 2018].
5. https://curiousmatic.com/worlds-5-prolific-cyber-armies/
6. Libicki, M. C. (2014). Shortage of Cybersecurity Professionals Poses Risk to National Security. Retrieved January, 5, 2015, [online] http://www.rand.org/news/press/2014/06/18.html
7. Schmitt, M. N. (2013). Tallinn manual on the international law applicable to cyber warfare: Cambridge University Press.
8. Clarke, R. A., & Knake, R. (2010). Cyber War: The Next Threat to National Security and What to Do About It: HarperCollins.
9. Ventre, D. (2013). Information warfare. London, UK: John Wiley & Sons.
10. Welsh, B. (2014). Cyber Warriors: The next generation. Defence Systems: Knowledge Technologies and Net-enabled Warfare. Retrieved 01 Jul, 2, 2018, [online]
11. http://defensesystems.com/articles/2014/01/23/next-generation-cyber-warriors.aspx
12. Wilhelm, R. (2012). Cyber Warfare…The New Reality. Vital Speeches of the Day, May 2012 issue. Retrieved 01 Jul, 2, 2018, [online]http://www.boozallen.com/insights/2012/03/Cyber-Warfare-The-New-Reality.
13. Cyber Armies: The Unseen military in the grid. Available from: https://www.researchgate.net/publication/283697882_Cyber_Armies_The_Unseen_military_in_the_grid [accessed Jul 01 2018].

Colonel Inderjeet Singh is the Chief Cyber Security Officer and Head of the Cyber Security Center of Excellence at Vara Technology. In this role he is instrumental in building the Cyber Security Business Unit for the Group. He is working on the disruptive technologies in the Cyber Security Space for securing IT networks, Smart cities and Critical Information Infrastructure.

He served in the Indian Defence Forces, is Alumnus of IIT Kharagpur and Symbiosis Institute of Management. He is an experienced Information Systems professional with experience of more than 27+ year across wide spectrum of areas spanning Information Security ,Risk Management, Cyber Security, Cyber Forensics, Cyber Warfare, Cyber Terrorism, Expertise in SOC and CERT, Internet of Things (IoT) including IoT Security, Blockchain and Cryptonomics, Machine Learning and Artificial Intelligence and Smart Cities.

He has held prestigious appointments while in Indian Army and has been CIO of E-Commerce Company. He has also served in United Nation Mission in Democratic Republic of Congo.

He is visionary for Start-Up Incubation, Entrepreneurship Development, Strategic Consulting and New Technology Evaluation for commercial viability. He is a Subject Matter Expert on latest innovative Technological domains and effectively managed mission critical projects

He has consistently delivered mission-critical results in the field of in Information Security Management, Cyber Security, Cyber Warfare and Cyber Risk Management.

He is a Council Member of CET (I) and fellow of IETE, IE, Member CSI and Executive Council Member Society for Data Science, Founder of Cyber Watch India, Member ISACA, IEE, ISOC, IoT4SCTF, CCICI, IETF, USI and many other professional bodies.

He has been consistently been awarded while in Army and was awarded “Magnificent CIO of the Year “Award in year 2016.