CLAWS

Seminar Report

Report on

National Seminar on

CYBER WARFARE

7 September 2016

CENTRE FOR LAND WARFARE STUDIES

Seminar Report on

CYBER WARFARE

Seminar Coordinator: Colonel Subhasis Das

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi-110010
Phone: 011-25691308; Fax: 011-25692347
email: landwarfare@gmail.com; website: www.claws.in

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an autonomous think tank dealing with contemporary issues of national security and conceptual aspects of land warfare, including conventional and sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

Printed in India by
Bloomsbury Publishing India Pvt. Ltd.
DDA Complex LSC, Building No. 4, 2nd Floor
Pocket 6 & 7, Sector – C
Vasant Kunj, New Delhi 110070
www.bloomsbury.com

CONTENTS

EXECUTIVE SUMMARY

- With the emergence of Cyber Weapons, which can also be termed as Zero Energy Weapons, a fundamental concept of warfare has been upset, which stated that Kinetic Energy is the most significant element in warfare.
- Applicability of The Laws of Armed Conflict and International Humanitarian Law to Cyber Warfare has not been deliberated. The anticipated release of the *Tallin Manual 2.0* is expected to address some of these aspects.
- At the national level, there are numerous diverse agencies responsible for action and co-ordination of cyber related activities. There is an urgent need for co-ordination of actions. The appointment of the National Cyber Coordinator under the Prime Minister's Office (PMO) is a significant and positive development.
- The existing framework of laws and policies are not comprehensive and do not address new technologies like social media and cloud computing.
- Both Pakistan and China have been targeting India in the cyber domain. Pakistan agents have used social engineering for espionage related tasks. China is indulging in cyber activities which have a long gestation period and targeted at the strategic level. The role of Chinese communication and Information Technology (IT) multinationals is implicit in the Chinese quest to achieve military and economic advantage.
- In the quest to achieve synergy in national cyber response including offensive capability, the lead agency role should be entrusted with the Armed Forces.
- The evolution and acceptance of the Bitcoin currency and outsourcing of IT services to non-organic agencies has contributed significantly to cyber attacks and crimes. There is an increasing trend of disruptive attacks as against targeted attacks.

- The Stuxnet malware attack continues to be the defining moment which brought in the phase of Intelligent Malware which can adapt, is stealthy, and can modify itself. The role of Chinese PLA unit 61398 and the NSA (National Security Agency of the United States of America) in launching of sophisticated cyber espionage activities is emerging in the open domain.
- The real world sectors like banking, national data repositories, e-commerce, and transportation are the most vulnerable.
- The increase in scope, type, and frequency of cyber incidents will soon render traditional data analysis tools and methods redundant. There is a need to incorporate Big Data techniques towards achieving a credible response strategy.
- The non-reversible and growing trends towards digitization, globalization, and mobility will also see the emergence of unknown threats. Hence, the new normal for cyber security would be prevention rather than remediation.
- There is a critical need for greater collaboration between the industry and the intelligence agencies/military in evolution of a national cyber response strategy.

DETAILED REPORT

Cyber related risks are a global threat of bloodless war. India can work towards giving the world a shield from the threat of Cyber Warfare.

– Narendra Modi

Introduction

1. Cyberspace is a complex domain quite unlike other war fighting domains like land, air, sea and space. The term *Cyber Warfare* is intricately enmeshed with other terms like *Cyber Security, Cyber Terrorism, Cyber Espionage and Cyber Crime*. It can arguably be said that the world has yet to see a full scale overt cyber war with equal protagonists; covertly however, every potential adversary is in the process of developing capabilities so as to gain ascendancy through the cyber domain.

2. The term *Cyber Warfare* is used in relation to the military. However, it is gradually becoming evident that any attempt to distinguish between military and non-military activities in the cyber domain would be fraught with risks. The tools for cyber crime, cyber espionage, or any offensive cyber attack would primarily be the same. These tools are tested and perfected during normal times, so that they can be launched with devastating effect during war. Cyber warriors can consist of military personnel, members of the industry, intelligentsia, hacker community or the student community. In fact anyone having access to the ubiquitous computer can be a part of this group.

3. Cyber Warfare is offensive and defensive in nature. In India, the National Cyber Security Policy was promulgated in 2013. The Computer Emergency Response Team-India (CERT-In) under the Ministry of Communication and Information Technology is the national nodal agency for responding to computer security related incidents as and when they occur. The Armed Forces have in

turn established their own CERTs. Purely defensive mechanisms and policies to protect own assets have not and will not stand the test of time. Eventually, even the most protected system can be breached. Towards this, the concept of *Cyber Deterrence* is gaining ground which talks about building sufficient offensive capability in Cyber Security mechanisms so that a potential adversary is deterred in acting against us.

4. Cyber Warfare is a subset of the overall gambit of Information Warfare. In the net enabled world of today, it is arguably the most important component. In *Inside Cyber Warfare*, Jeffrey Carr states that any country can wage cyber war on any other country irrespective of the resources, because most military forces are network centric and connected to the Internet or have their own systems. Small nations like North Korea have demonstrated their capability to take on technologically superior nations like the United States. Stuxnet and Flame attacks against Iran and Estonia have proved the power of cyber warfare to shift focus from conventional to the 'virtual' domain. Access to the Internet and easily available cyber tools also enable Non-state Actors to launch cyber attacks. Cyber attacks are characterized by deniability and non-attributability; hence, traditional and physical boundaries are not relevant in this kind of warfare. It is characterized by extreme speed, lack of warning or indicators, ambiguity regarding the specified areas of battle, and lack of posturing. Traditional deterrence strategies are ineffective in this form of warfare.

5. The United States, Russia, Israel, and China have been known to have demonstrated advanced capability in the field of Cyber Warfare. The United States has been concerned with the attacks on their Intellectual Property and has created a new synergy between the security agencies and the industry. (This has particularly gained importance after the plans of the F-35 got leaked out, allegedly to China in the mid 2000s. More recently alleged North Korean hackers attacked Sony Corp and leaked unreleased movies.) China has gained considerable success in this field and is now considered one of the foremost players. Role of Chinese

hacking units has been detected in numerous breaches that have been reported in different parts of the world. India continues to be a prime target of the Chinese cyber warfare effort.

6. In order to debate issues related to the subject, the Centre for Land Warfare Studies conducted a Seminar on 7 September 2016 themed 'Cyber Warfare'. The participants were from the three services, strategic community, veterans, industry, consultants, Research and Development organisations, and academia. The Seminar afforded a platform to analyze existing policies, doctrines, strategy, threats, and challenges. It also aimed at evaluating capabilities, with specific reference to the role of various agencies.

7. The names of panelists who took part in the Seminar are as under:The Keynote Address was delivered by KC Verma, Former Chief R&AW.

   - Session One on Cyber Warfare: Policy, Doctrine and Strategy

     Lieutenant General Anil Bhalla, PVSM, AVSM, VSM (Retd) former DGDIA

     Colonel Inder Barara (Retd), Executive Director and CIO, Greyland Group

     Colonel S Sharma, Army War College, Mhow

     Brigadier MU Nair, DACIDS (DIARA), HQ IDS

   - Session Two on Cyber Warfare: Techniques and Challenges

     Rear Admiral Dr Sanatan Kulshrestha (Retd)

     Colonel D Bose, Senior Fellow, CLAWS

     Lieutenant General Anil Bhalla, PVSM, AVSM, VSM (Retd) former DGDIA

     Anil Bhasin, MD India and SAARC, Palo Alto Networks Pvt Ltd

8. The aspects covered and the salient observations/recommendations of the Seminar are given in the following paragraphs.

Cyber Warfare: Policy, Doctrine and Strategy

The Keynote speaker emphasized that with the evolution of Cyber Weapons which can also be termed as Zero Energy Weapons, a fundamental concept of warfare has been upset, which stated that Kinetic Energy is the most significant element of warfare. Cyber Warfare questions the basic principles of war. Cyber Warfare being contactless and borderless has resulted in the emergence of armies of Non-state Actors with a shield of plausible deniability. One fundamental question raised was the applicability of Laws of Armed Conflict and International Humanitarian Law to Cyber Warfare. While the *Tallinn Manual* exists, it is not binding as of now. The publication of *The Tallinn Manual 2.0* is eagerly awaited to address the issue of how to interpret international law in the context of cyber operations and cyber warfare. The Speaker also addressed the need to revisit the methodology of tackling cyber incidents as is being done today. He opined that mere blocking of offending sites and content would not suffice in future. There is a need to integrate the Intelligence Agencies and the Defence Forces in this task in the peace time so that actions can be perfected and implemented in war.

Appraisal of National Cyber Policies and Laws

It was stated that there are more than 35 different agencies operating under the PMO, MHA, MEA, the Ministry of Defence (MoD), MCIT, and non-government organizations (NGOs) which have a role in the overall national response to cyber incidents. There are six different Apex Level agencies for management, co-ordination and supervision. The ambiguity in the protection of critical infrastructure emphasizes the case for synergy. CERT-IN, formed in 2004 vide the Information Technology Act 2000 (70B) under MCIT, was initially mandated to ensure cyber security of critical infrastructure, which was later limited to only non-critical structures. The National Critical Information Infrastructure Protection Centre (NCIIPC) formed under NTRO vide the Information Technology Amendment Act 2008, was later mandated with protection of critical infrastructure. Today the NDMA which is under MHA, has also been assigned the responsibility for protection of cyber critical infrastructure. Hence, three different

agencies under different ministries are operating towards the singular objective of securing critical infrastructure. While the lead agency in formulating national policy is the DEITY/MCIT, this Ministry does not have jurisdiction over influential ministries and departments like the MoD, MHA and NSCS/NTRO. It emerged that the interaction, sharing of information, earmarking of specific roles and assignment of responsibility is nebulous. The appointment of the National Cyber Coordinator under the PMO is a positive development and expected to give fillip in this direction.

The Information Technology Act 2000 duly amended in 2008-09 and the National Cyber Security Policy 2013 do not address critical new technologies like the social media and cloud computing. It is significant that data is no longer in the custody of the users. Data custody is being outsourced and presently there are no laws to regulate and enforce the same. It emerged that existing laws and policies do not touch on the Dark Web and consequently most of the cyber crime incidents including ransom ware attacks are not reported to the enforcing agencies. At the international level, no cyber war agreements exist between countries; hence, there is no road map for an international response in the event of a cyber war.

Cyber Capabilities of Neighbours

Pakistani hackers have been active on the Internet and incidents of defacements, vandalism, and cyber espionage were identified as the main activities. The role of Pakistan as a nation, indulging in cyber attacks, is however, not clear. Names like Zubair Khan and Hamza Qamar are known in the community for India specific attacks. What is of concern are the exploits achieved by Pakistani agents using social engineering for espionage related tasks. Social media and matrimonial sites are active playgrounds of Pakistani agents. China, on the other hand, is indulging in cyber activities which have a long gestation period and targeted at the strategic level. Instances of attacks on the MEA, MoD and the Tibetan government in exile have been attributed to Chinese actors. China is approaching cyber warfare by means of the organised sector as well as the unorganised sector, according to the tenets of the people's war. The role of the People's

Liberation Army (PLA) is primary and cyber warfare is being treated as special operations. The role of Chinese multinational players like ZTE and Huawei, is evident, in the quest to achieve military and economic advantage through the cyber medium.

Synergy Between Organisations

It was opined, that to evolve an effective cyber response which involves the development of offensive capability, the lead agency role should be entrusted with the Armed Forces. The complete manifestation of cyber war would be seen in case of an all out war, wherein the responsibility of Indian response in all offensive and defensive domains would rest with the Armed Forces. Hence, to have a different approach in peace time and in war may not be entirely logical. The deliberations during the Seminar suggested that all non-military agencies should be placed under the National Cyber Coordination Centre (NCCC) while the military agencies should be coordinated by DIARA under HQ IDS. A joint services team could be deputed to co-ordinate between the NCCC and DIARA. The military organisations should focus on CNO/IO, deterrence, protection of own assets, develop offensive tools, testing and certification. The role of the DIARA could be taken on by the Cyber Command on its raising.

The under mentioned aspects also emerged:

- There is a need to establish organisations and structures within the Armed Forces to steer issues related to cyber warfare.
- There is a need to expedite the process of laying down standards, certification and definition of yardsticks for both hardware and software, being used for Information and Communications Technology (ICT) applications in the Armed Forces.
- Organisations raised for cyber warfare should be permitted to adopt a tailor made approach for procurement and management of resources to enable continuous technology updates and avoid obsolescence, while maintaining confidentiality.

Cyber Warfare: Techniques and Challenges

Technology is leading to sophistication in cyber attacks. Present day cyber weapons are characterized by their transience. The Mandiant Report 2016 states that the median number of days an organisation was compromised in 2015, before the organisation discovered the breach, was 146. While cyber security teams are getting better at detecting and resolving breaches, this period of almost 5 months of undetected state, is alarming. Despite the sophistication of cyber weapons, it remains to be seen whether these alone can lead to victory in battle. The role of the human element also came for discussion. It emerged that the quality of manpower is as crucial as the access to technology. The extent, frequency and range of cyber attacks in the future will make it impossible for humans to detect and tackle all threats. There is a need to develop AI based systems which can supplement the human effort.

Latest Tools and Techniques in Cyber Warfare

Two trends in the cyber domain have contributed significantly to cyber attacks and crimes. First is the evolution and acceptance of the Bit-coin currency and second is the outsourcing of IT services to other parties, who may be compromised. Cyber attacks are also shifting from targeted attacks to disruptive attacks like ransom ware, deletion or encrypting of data, modification of critical business data, etc, which require immediate attention.

The Stuxnet malware attack is a defining moment in the evolution of cyber warfare techniques. The period before Stuxnet can be characterized by Denial of Service attacks, defacements, unauthorized access and stealing of data (essentially low technology and high visibility techniques with limited impact). Stuxnet brought in the phase of Intelligent Malware, which can adapt, is stealthy, can cover its tracks and can modify itself. These complex and technology driven malware is selective about its victim and generally also associated with multiple modes of execution, some of which may never get executed in the lifetime of the code. In 2013, Mandiant released a report in which certain cyber espionage activities were

attributed to Chinese hackers. Specifically, the PLA Unit 61398, operating out of Shanghai and code named APT1 by Mandiant was implicated. The advanced techniques used by APT1 were a mix of spear phishing, breaching of a beachhead backdoor, and use of covert channels masquerading as legitimate and privilege escalation. The spy codes were capable of internal reconnaissance, lateral movement and completion of mission by archiving, splitting and finally transferring data. The Edward Snowden incident has brought into the open domain, certain techniques used by the NSA. The Tailored Access Operations units were manned by the best brains and had obtained backdoors into encryption standards, had arrangements with leading technology companies to monitor private networks and stored a stockpile of zero day exploits. It emerged during the deliberations that future cyber attacks would be extremely difficult to detect and could attack multiple nations at the same time. The real world sectors like banking, national data repositories, e-commerce, transportation and connected weapon platforms would continue to be the most vulnerable.

Intelligence-based Operations: Data Mining and Applicability to Defence Forces

Data gathered from the CERT-In website shows an increasing trend in reported cyber incidents. It is anticipated that the increase in the scope, types and frequency of attacks will soon render traditional data analysis methods redundant. This brings in the need to implement Big Data techniques in the quest for achieving a credible response strategy. Timely and accurate data mining can reduce the effective time span of malicious code. It would also assist in the development of offensive cyber weapons with a low degree of detection. However, this will require a complete shift from the present day incident driven response strategy. It would require national level guidelines for incorporation of Data Mining in future ICT projects, skill development, implementation of pilot projects for ascertaining the efficacy and a complete realignment of intelligence processes.

Cyber Threats to Business and the Way Ahead

Three trends of the modern world, ie digitisation, globalisation and mobility cannot be reversed or slowed down. These growing trends will also see the emergence of unknown threats. To tackle these unknown threats, security needs to be a part of life. However, in the business world, despite the knowledge of the imminent threat, there is a lack of tools and intent. The need of the hour is to have a partnership between the user and the OEM, since security cannot be just left to an external party in the present context. The new normal should be prevention rather than remediation. The cyber security tools of the future should anticipate the likely actions of the attacker and proactively secure own systems so as to frustrate the attacker. In doing so, performance and ease of doing business cannot be compromised.

It emerged during the discussions that a major part of the industry is still using tools of the previous generation to tackle threats of the future. The industry still has a dependence on legacy systems where modern security solutions do not work. The key aspects which are desired in modern day cyber security solutions could be identified as detection and prevention, constantly working at the level of the mobile device, the Internet edge, wireless connect, LAN, at the data centre and in the cloud or in other words cover all the bases of the enterprise. The capacity of these solutions to convert the unknown threat to a known in the quickest possible timeframe would be the key to success.

While the businesses would continue to focus on cyber security, there is a growing trend also being seen within the industry to evolve niche expertise in development of cyber tools, including offensive weapons, which are being developed in partnership with the Intelligence Agencies and the Armed Forces. There is a critical need to increase the level of partnership and collaboration so that cyber armies consisting of both uniformed and non-uniformed personnel are able to deliver the desired 'payload' during war.

Conclusion

Wars will be fought differently in future. Hacking and virtual sleuthing would be integrated into all future operations, as indispensable as the weapons and ammunition soldiers carry into battle. To cripple a country during cyber war, critical infrastructure will be targeted. This will include power, banking, water systems, health, agriculture and transportation. To do so, relentless peace time cyber activities looking for vulnerabilities in target networks needs to be carried out so that the systems can be hijacked and injected with cyber tools for use in future operations. To ensure the survivability of own critical assets, a vulnerability assessment would be in order at the national level so that necessary corrective action can be undertaken in time.

In consonance with the tenets of conventional warfare, the militaries now need to draw up a list of overseas targets of national importance, where it would make more sense to attack with a cyber weapon than a conventional one. Overall, there is a pertinent need to integrate cyber warfare into military doctrine.


CENTRE FOR LAND WARFARE STUDIES
NEW DELHI
CYBERWAR
INDER BARARA
ANIL BHALLA
M U NAIR
S SHARMA


PHILIP CAMPOSE