Preparing for Cyberwar - A National Perspective

26 Jul, 2012 Commander Mukesh Saini (Retd.)

On November 12th, 2011 Maj. Gen. Moghaddam, the "architect" of Iran's missile program, was showing a new type of warhead for nucle missile Sejil 2, to a group of experts for their comments, at a site about 50 Kms from Tehran. Warhead was connected to computer for si being watched on a big screen. And instead of simulation the actual warhead went off pulverising the site. Explosion was so powerful th in Tehran. Initially Iranian government refused to accept that there was any such explosion however later conceded that in the expl Revolutionary Guards have lost lives (though 36 funerals took place). Explosion was so powerful that no one was alive to narrate the ir was left at the site to provide evidence. Revolutionary Guards (IRGC) investigation pointed at two probabilities; (a) infiltration by a Moss computer controlling the missile was infected with Stuxnet (like) worm. The second probability was considered much more likely after tw infiltrations using Stuxnet and Duqu to stall Iran's nuclear ambition. Probably this incident is historic as for the first time cyber weapon real world explosion or kinetic attack. (Israel Insider, 2011)

Introduction

Cyberspace has changed many old concepts. In this globalised world everyone is neighbour of other. There is no established conc Identification of targets and what is under threat or need to be attacked in case of Cyberwar is important to segregate the facet of C using other form of attacks on ground, air and as Sea. What needs to be secured is what needs protection. Therefore definition of Cyb fair idea about the scope of Cyberwar and its targets. The Information Technology Act 2000 (India) defines Cyber Security which information, equipment, devices computer, computer resource, communication device and information stored therein from unauth disclosure, disruption, modification or destruction. Richard A. Clark in his book Cyber War defines "cyberwarfare" as "actions by a nation another nation's computers or networks for the purposes of causing damage or disruption. However things are not as simplistic and mat of mind and perception also.

To understand the real meaning of Cyberwar, it is necessary to understand the meaning of War and its import on governance and dip Parliamentary Committee in its report after Iraq war noted that "War" is a term that has both popular and legal connotations. Colloquia conflicts between the armed forces of states and, occasionally, major internal conflicts such as the British or American Civil wars. "War" a is a feature of both international and national law. In international law, the distinguishing characteristic of "war" is the legal equality of t the special status of those states not taking part in the conflict ("neutral" states). The condition of "war" could be brought about by a de one was not necessary (nor, where there was a declaration of war, were hostilities inevitable). Additionally, states could choose to regarc them as "war" and apply the legal rules accordingly, or neutrals could insist on respect for their rights. "War" as an institution of domest declaration, made in the Monarch's name but by the Prime Minister, acting under the prerogative. This action triggered domestic consequ the opponent state became "enemy aliens", liable to measures of restraint including detention. Property of enemy aliens was liable provided for emergency measures—for the call up of troops, the sequestration of property and so on. (Constitution, 27 July 2006)

To fit this definition of War the only Operation Orchard fits the bill were Air Defence System of Syria was made ineffective by Israel du alleged nuclear plant of Syria. In all other cases be it cyber-attack on Estonia, Georgia or Operations Titan Rain, Night Dragon Shady R termed as the acts of war. The case of explosion at Iran's missile site lacks affirmation and evidence.

War has International Ramifications

Various international laws and treaties especially of Paris and also Charter of United Nations prohibit use of threat or use of force in inte Prior to these developments post 1945, declaration of war was a standard practice, but today no one officially declares war to the intern This is nothing but just masking because internally a nation state has to declare war, whether limited in scope or a full-fledged war. T activate appropriate structures; authorisation to force commanders to use Rules of Engagement (R.o.E) for 'conflict'; activate provis freezing of assets of enemy aliens; mobilisation of resources; suspension of local laws against the enlisted personnel engaged in war; 'Emergency' in the country. Thus a war whether declared or otherwise is a 'structured-response' to a conflict which is expected to result enemy to the will of a nation.

National Information Security Policy & Doctrine of Cyberwar

It is necessary to define what would constitute an "attack" serious enough to precipitate into military counter offensive. It is necessary t an open stated policy, so that in case of any military retaliation, the international community can be with India. However defining this not easy. If the threshold is kept too law then breaches will be norm and finding exception where counter offensive becomes necessa manner would be difficult. If the threshold is kept too high then nation can be bled by thousand wounds rather than massive att retaliatory force can be used.

Another challenge is attribution. Cyber-attack may appear to be originated from one or multiple countries but actual culprit may be a thir in April 2012, National Informatics Centre has told the press that some unknown third country has used its servers to attack other countr (Joseph, 2011) This statement had two immediate adverse effects on our cyber war preparedness, firstly it has exposed our vulnerabili have sufficient capacity to identify originating country despite servers and logs are under our control and secondly it has provided a enemies to attack us and deny ownership of such attacks. Can we now blame China for attacks on Indian cyberspace?

Thus attribution is critical for appropriate response. In fact noting this fact, Annual Report 2011-2012 by Intelligence and Senator Co termed cyber attack as a 'Tier One threat to UK and has direct to government to inter-alia develop capabilities of cyber-attack without de without attribution). The UK government has been allocation of funds equivalent to Rs. 5720 Crores over next 3 years for National Cybe to prepare for cyber-attack. The committee has also advised the intelligence agencies to not to use such technologies against own c specific approval. (Intelligence and Security Committee, UK, 2012)

In 2005, after 2 years of extensive deliberations between 21 ministry/departments of the government and industry confederations, N Board under NSA Sh. JN Dixit had approved the draft National Information Security Policy (NISP), it is yet to be approved by the goverr while Department of Electronics & IT drafted another NISP (apparently without wider consultation) and sought public opinion in 2011 heard of new NISP since then. Due to this intervening period on this front we moved from leader to laggard. Without such policy d Warfare Doctrine for nation (not a doctrine by Armed forces) will be distant dream. Therefore to fight as well defend against future paramount that a good quality and well consulted over-arching NISP is finalized and formally declared. And based on this IW Doctrine fo Intelligence Services as well as private sector) be developed.

Amendment to National War book

Once as a policy India declares the existence of cyber war and its contours, and also develop cyber war doctrine, the war book requi accordingly. The role and responsibility required to analyze and articulated to prevent confusion and fratricide at the time of war. It i efficient and effective conduct of war including cyber-war. The war book therefore needs to specify as how to maintain no-contact cybe government decide to go for full-contact or partial-contact war then how cyber war will be integrated to meet overall war objectives. T place which mandates the change in command and control structure and transfer of certain powers to military. It is the war-book which v government relationship and any failure to do so can lead to turf war and chaos at the time of crisis.

Rule of Engagement

The offensive Cyber operations by the enemy will be swift and paralyzing. Therefore central control of conduct of cyber war may not be necessary to define as unambiguously as possible Rule of Engagement for cyber warriors (whether uniformed or militia). Uncontrolled off hurt in retaliatory fire against unplanned defensive measures but also can isolate us in community of nations. The role of diplomatic c never to be underestimated in events leading up to full scale cyber war. The National Internet Exchange (NIXI) is up and running to def Internet in case of worst situation, isolation but poor defensive mechanism, lack of capacity can paralyze us and can cause loss of ou Therefore it is necessary to coordinate not only with in the government and armed forces but also with private sector as well as patriotic government and RoE for everyone should be articulated. While preparing RoE the issues highlighted in following paragraphs must be addr

According to RoE of most of the Armed Forces of the world, Line of Communication and nodes which directly or indirectly supports m belligerent nations are valid military targets. By this Rule of Engagement all telecommunication and internet service providers are legitir any Cyber war. However when the Hague rule (1923) of Air warfare article 24(2) was prepared the dependency of life of masses structures was not as heavy as it is today. Not even at the time when in 1956 New Delhi Draft rules were prepared, which clearly es objectives belonging to the following categories are those considered to be of generally recognized military importance: ... (7) T broadcasting and television stations; telephone and telegraph exchanges of fundamental military importance." there was no Internet. N possible to mount unbearable misery on masses through attacking on Critical Information Infrastructure. The question is that if undertaken, will it amount to war-crime?

While dealing with IHL /LOAC, the British Parliamentary Committee felt, "The situation is different, however, in the case of breaches of I State for the armed forces told us that "once a conflict actually begins, whatever the legal basis for this participation, it is conduct by required by the body of law in rules known as the International Humanitarian Law. The four Geneva Conventions of 1949 are a part of t Kingdom is also bound by a number of other conventions and protocols, such as the first additional protocol to the Geneva Conventions . laws. We apply them. Those have been defined elsewhere and we simply live within them, so to speak". Mr. Ingram added that "all of o trained in understanding the basis upon which they are having to conduct themselves in a conflict situation and it is very much part of process". Individuals (and in some cases their commanders) suspected of violations of IHL such as killing prisoners of war, the ill-treatm occupied territory or the use of prohibited weapons must be considered for prosecution in national courts. The Government has said, ir ICC, that all allegations of this kind would be stringently investigated and, where appropriate, criminal proceedings instigated. This derives from the Geneva Conventions, has gained in importance following the United Kingdom's acceptance of the Statute of the ICC.

those alleged to be responsible for serious violations of IHL is within the jurisdiction of the ICC, but only where the proceedings in nati unsatisfactory or non-existent. The Government's position has been that there will never be prosecutions against British servicemen befc there always will be adequate national investigations, followed, where required, by prosecutions. (Constitution, 27 July 2006)

Need for Coordination and Control

The cyber-attack on Iran in form of Stuxnet, Duqu and Flamer are just peek into the future. US President has repeatedly stated that cyb serious economic and national security challenge that America faces. To meet this challenge US has introduced Cyber security Act 2012 July 2012. (BBC, 2012). US conducts exercise 'Cyber Strom' every alternate year. NATO, Australia and many European countries underta security exercises to improve command, control and coordination. A formal Cyber command and control structures have been established world countries and China.

Unlike military war, the non-state actors such as terrorist organization, large corporate houses, hacktivist, cyber privateer and cyb capacity and will to take on nation states. Wikileaks, Anon, Luzesec were some of the non-state players who have challenged the might c the United States of America. Large organizations such as Intel, Microsoft, Huawei, etc can also play role to support their respective gov 'Flamer' virus original Microsoft Digital Signature was misused. (Adhikari, 2012; Adhikari, 2012).

It is myth that hackers will win or lose the cyber war. Hackers (with due respect) are just foot soldiers, and wars are fought by General know their forces, understand enemy forces as well as mind of their commander, can coordinate with other wings of the government a leader who draws respect from his soldiers (Hackers).

In India we are yet to formally recognize the dangers, not because it is not so recognized in the power circle but just because it is so re the most powerful tool that everyone wants to play the lead role and turf war has broken out. Institute of Defence Studies and Analyse give some course correction to this rudderless situation through its recently released book 'India's Cyber Security Challenges'. (IDSA Force, March 2012) However overall paralysis is continuing and well planned structure such as CERT-IN, NTRO and NSCS are undermined. It is therefore necessary the National Information Board (a board of score of secretary ranked officer) be resuscitated and held at least every quarter till things stabilise and we as nation become competent to defend our cyberspace.

Role of Defence Forces

Role of defence forces in case of Cyber war is limited. They are required to protect only its own domain and at the most government dom .mil.gov.in, army.in etc. But if this control is not practiced in peace time same cannot be undertaken in war time. In fact probably intelli CERTs are better positioned to take on such tasks. However IHL and LOAC neither cover nor envisaged to cover the activities of Int Similarly for offensive operations, intelligence agencies that had undertaken surveillance of enemy networks and probably placed backd the target network may be more suitable for offensive action. For example if National Security Agency of US have deployed the lau weapons then NSA alone will be in better position to arm and launch cyber weapons from these pads. In case of Duqu probably some was controlling the Command & Control centres of Duqu. Non applicability of IHL / LOAC on such agencies is a glaring flaw in sc containing any Cyberwar. And also launching Cyberwar on other nation without adequately protecting own cyberspace will be simila Assured Destruction / Disruption) of nuclear war.

Cyberwar also challenges some of the basic tenet of armed conflict. What is use of fighting personnel to wear uniform when the oppc going to be physically present in front of each other? How would belligerent forces know that attacking party is enlisted or a civilian? Sup of one of the belligerent nations are encrypted and made unusable, will the data which may be very vital for the survival of the po prisoner-of-war? If collision of train takes place due to intentional malfunctioning of signalling system leading to death of masses, wil Crime?

Conclusion

War is serious matter which involves lives of all citizens. Even if external declaration of war has become redundant, this is required resources for fighting the war. When war get (internally) declared there are changes in organisational structure of governance; War Boo Rules of Engagement changes; financial allocation made; civilian criminal laws stand suspended for actions taken in pursuance of Emergency may be declared. These are too profound changes which cannot be taken lightly. Therefore every cyber-attack does not am Involvement of defence forces along with enlisting of hackers and allocation of cyber-targets for proper coordination is required. The ir and conventions such as IHL and LOAC come into force. Wars are not limited to action on ground but diplomatic struggle also begins. No the ability to stand winnable chance against a nation state. Therefore it recommended that Cyberwar be looked at with all seriousness should be take-up in double quick time to prepare our nation for Cyberwar:

a. Declare National Information Security Policy after wide consultation with all stake holders. Such policy should be as much as possible overarching and long lasting;

b. Evolve Cyber warfare doctrine and develop capacity to implement such doctrine;

c. Modify National War-Book to include this new form of war and its peculiar characteristics such as no-contact war and role of non-actors

d. Define Rule-of-engagement for Cyberwar to prevent unintended escalation of war and unintended Human Rights violations;

e. Establish command and control structures for efficient and effective conduct of Cyberwar and prevent turf war within during the period

f. And to do all this and much more, National Information Board should meet at frequent interval; else Cabinet Committee on Secu alternative.

Bibliography

Adhikari, R., 2012. *Flame Singes Microsoft Security Certificates*. [Online]
Available at: http://www.technewsworld.com/story/75289.html [Accessed 20 June 2012].

BBC, 2012. News Technology. [Online]
Available at: http://www.bbc.co.uk/news/technology-18928854 [Accessed 21 July 2012].

Constitution, S. C. o. t., 27 July 2006. Waging war: *Parliament's role and responsibility Volume I: Report,* London: HOUSE OF LORDS.

Hague Convention V, 18 October 1907. *Hague Convention V.* [Online]
Available athttp://avalon.law.yale.edu/20th century/hague05.asp [Accessed 05 May 2012].

IDSA Task Force, March 2012. *India's Cyber Security Challenges*, New Delhi: Institute of Defence Studies and Aanlysis. IDSA, 2012. *Inc Challenge*. First ed. New Delhi: IDSA.

Intel Technology Brief , 2011. *Protect Laptops and Data with Intel® Anti-Theft Technology*. [Online] Available at: http://www.intel.c theft/anti-theft-tech-brief.pdf [Accessed 24 May 2012].

Intelligence and Security Commitee, UK, 2012. *Annual Report 2011-2012,* London: Controller of Her Majesty's Stationery Office.

Israel Insider, 2011. Suspicion in Iran that *Stuxnet caused Revolutionary Guards base explosions.* [Online]
Available athttp://israelinsider.net/profiles/blogs/suspicion-in-iran-that-stuxnet-caused-revolutionary-guards-base-e [Accessed 24 July 2012].

Joseph, J., 2011. *Govt servers used for cyber attacks on China, other countries' networks*. [Online http://timesofindia.indiatimes.com/tech/news/internet/Govt-servers-used-for-cyber- attacks-on-China-other-countries-networks/articles [Accessed 24 July 2012].

Quintin, K. J. a. A., 18 November 2011. *The Internet in Bello: Cyber War Law*, Ethics & Policy. Berkeley, UC Berkeley School of Law.

Published Date: 26th July 2012

Post new comment

Your name: *

Anonymous

E-mail: *

The content of this field is kept private and will not be shown publicly.

Comment: *

Message*

Input format

I'm not a robot reCAPTCHA Privacy - Terms

Save Preview

Related Articles

Commentary: 20 Years of India's Nuclearisation: Retrospect

On 11th & 13th May 1998, India surprised th

एयर चीफ मार्शल बीएस धन

विवेकानंद इंटरनेशनल फाउ

Commentary: In Largest Military

The latest re military published by

DEFENCE IMPLICATIONS OF KEY EMERGING TECHNOLOGIES

Commentary: Why S-400 Will Make Sense Despite (Un)Likelihood

The open source is abuzz with the news that India and Russia are

Commentary: Si Exercise 'Gagan

The Indian A carried out pan-India Ex

Achieving self-reliance in defence pr require a

Commentary: Constitution of the new Defence Panel Chaired by

Recently, the Ministry of Defence (MoD) has constituted a Defence

Testimony of Admiral Michael S. Rogers and Implications for

About Us

The Vivekananda International Foundation (VIF) is a New Delhi-based think tank diplomats, industrialists and philanthropists under the aegis of the Vivekananda k start innovative ideas and thoughts that can lead ...

Read More

Contact Us

Name*

Email Id*

Phone Number*

Message*

I'm not a robot

reCAPTCHA
Privacy - Terms

Submit

Tweet With Us

VIF India
@vifindia

'The organs are the horses, the mind is the rein, the intellect is the charioteer, the soul is the rider, and the body is the chariot. The master of the household, the King, the Self of man, is sitting in this chariot.' #SwamiVivekananda

3h