Cyber Warfare in the Indian Context

28 Apr, 2014 Lt Gen Gautam Banerjee, Editor, VIF View1760 Comments 0

The Cyber Space

The contemporary era is characterised by what has been described as the 'information revolution'. This is a phenomenon in which autom activated to marshal and manipulate huge volumes of digitised information as relevant to every field of human endeavours before information across a virtually unlimited realm. As human societies across the entire globe as well as the systems governing these become usage of information assets, effective harness of information infrastructure in military engagements too becomes an undeniable obligation

Information infrastructure is a chain of high-technology systems made up of sensors, transmission media, data processors, inform competent personnel to man these, all of which are coupled to form a most effective regulating medium for all global activities. Howev infrastructure rests in the all pervasive *electronic time-space continuum.* Described as 'cyber-space', this is the arena in which all e progress, peace, stability - and war, of course – must be played out. Cyber-space, therefore, is central to the information infrastructure.

Just as it is in case of all other arenas of competitive engagement – land, sea, air, space and perception - the native instinct of us resources has made it obligatory to protect one's usage of cyber-space against corruption, subversion and neutralisation by adversari friendly competitors. When this obligation is sought to be fulfilled in the realm of military operations, the concept of Cyber Warfare cryst the term 'Cyber Warfare' should be usable only in military context and differentiated from the term 'Cyber Security', the latter term be for civilian information security functions. This distinction is necessary to avoid intrusion of conceptual ambiguities into the nation's c security strategies.

The subject matter being vast, in this paper it is proposed to focus the discussion to the basic framework which dictates the terms of en Warfare.

Information Warfare

Military security of a nation is cultivated by preparing for, or activating if necessary, such extreme inflictions that make the advers unbearable animosity. In the nation's military security functions, the profound role performed by information infrastructure makes it a key to be nurtured or neutralised as the case may be. Thus, the activities undertaken to gain 'Information Superiority' over the adversary t various kinds of military operations are termed as 'Information Warfare'. Notably, while the 'hard' objects of information infrastructure protected by physical - active and passive - means, the 'virtual reality' of cyber-space needs sophisticated science and high-technolo within the overall ambit of Information Warfare, when military operations are carried out in the domain of cyber-space, the term used is is, however, important to note that while the adversary may be disabled by Cyber Warfare, he may not yet be induced to submit; w Warfare, when prosecuted, could achieve that purpose.

Measures applied to engage in Information Warfare are classified under two categories, namely, 'Information Operations – Offensiv Operations – Defensive'. These conventions help in delineating the military aspects of the information era.

Information Operations

Information Operations in either mode – Offensive and Defensive – are by convention classified under the following descriptions:-

- Command and Control Warfare (C2W): Attacking adversary's ability to generate and communicate commands to its forces is termed as C2W. adversary's Defence Information Infrastructure.
- Intelligence Based Warfare (IBW): It is the integration of sensors, processors and data-links to achieve profound and near-real time surveillan decision support, target selection and engagement, and finally, damage assessment.
- Electronic Warfare (EW): Combat in the electromagnetic medium to achieve enhancement, degradation, interruption or corruption of radiating classified as EW. In other words, it implies domination of the electro-magnetic spectrum.
- Psy Warfare: This is aimed at targeting the adversary's mental orientation and perception, and thereby influence his intention. In a larger con aimed at demoralising the hostile population.

- Hacker Warfare: This is defined as destruction, degradation or exploitation of adversary's computer data-base. Intrusion into adversary's syst 'worm', 'trojan horse', logic bomb' etc. is the mode adopted in this case.
- Infrastructural or Economic Warfare. This involves 'information blockade' and 'information hegemony' to garner undue economic advantage. U conditions, its extreme manifestation may lead to attacks on the adversary's core infrastructure – railways, power, oil sectors, for example.

It is needless to emphasise that the last three kinds of warfare are liable to transcend into the civilian domain.

Cyber Warfare

To reiterate, *Information Warfare* is resorted to gain Information Superiority by the means of Information Operations which are execu well as *Defensive* modes. There are many operating fields of Information Operations, such as human intervention, passive and weaponised attack, sabotage etc. which are executed in the physical domain. Similarly, the electro-magnetic spectrum becomes Electronic Warfare. Lastly, when Information Operations are executed in the cyber domain, the term applicable is *Cyber Warfare.*

Cyber Warfare involves targeting the adversary's military networks to induce collapse or corruption of his information-based C Communication, Co-ordination, Intelligence and Inter-operable Systems (C4I2). Point to note is that the scope of hostilities are liable to civil sector too, when the focus would be on the adversary's societal perception and his national administrative and economic infrastructu

Cyber Warfare is therefore one of the 'military operations of war'. In the Indian context, it may be used as a purely military term an manner of a military operation in the same spirit of extreme measures just as it is in the case of conventional, sub-conventional, mano mine and nuclear warfare.

Objectives of Cyber Warfare

The purpose of Cyber Warfare is to undertake defensive and offensive Information Operations in the cyber-space to degrade the advers warning, data analysis, intelligence exchange, decision support, and command, control and communication network – the entire syst centricity in short - while at the same time protecting own information assets from hostile intrusion. In offensive operations, that g intrusion into the adversary's vast volumes of digitised information that circulate in the cyber-space. Notably however, in defensive mod of general security measures, the effort cannot be so much in locking up own volumes of information simply because in the cyber domai to achieve. The effort therefore is to identify the algorithms and processes of the adversary's offensive Information Operations and neutr corresponding counter-offensive measures - preferably proactive.

Objective of Cyber Warfare therefore is to gain information superiority in the aspects of surveillance and reconnaissance, data a exchange, command and control of battle elements and flow of communication, and thereby protect own net-centric systems while dis adversary.

Science of Cyber Warfare

Automated exploitation of information in the cyber-space covers the entire gamut of communication, computation and transmission n Warfare, the process of extracting information from vast array of data, converting these into intelligence and then deriving tactical int decision making is a highly complex matter. Even if humans naturally do so remarkably well, there are limitation of volume and speed th Here science comes to the rescue, to define and quantify information, analyse input-data and facilitate decision making.

The matter of the science of Cyber Warfare is vast. It would therefore suffice here to just mention the core aspects of mathematical ana identification, selection and targeting in the cyber-space. This process is carried out through algorithms based on mathematical logic ar and involves the following defensive-offensive steps in continuum:-

- Sensor based detection of presence, identification and tracking of cyber-entities (e.g. personnel and equipment, radiation pattern, etc.) by the p and intrusion of the cyber-space. This involves mathematical derivation of 'inductive' and 'deductive' logic to select relevant signatures or data-inp
- Determination of inter-relationships and activities (e.g. data-mining, computation, data-transfer etc.) of the targeted cyber-entities. Comparisor with help of 'data ware-house' and 'data-fusion' is resorted to chart the adversary's possible options thus. Application of information theories to sift identification of the target cyber-space and inference of intelligence are carried out through processes known as 'abduction' and 'deduction' of infor
- Inference of plausible objectives of the adversary (e.g. dissemination of intelligence, command or engagement instructions etc.) through activat entities. This is accomplished by means of 'indicator-data analysis'
of the detected cyber-hierarchy and the deployment pattern of the cyber-entities. 'Decision theories' are applied to analyse and evaluate the alterr
- Determination of the likely courses of Cyber Warfare, reactive or proactive, available to the adversary. This is a technical appreciation, assisted military logic.
- Assessment of own possible Cyber Warfare options and objectives. This too is a process of technical appreciation, duly narrowed down by pre-lo The assessment is contingent upon right evaluation of the utility of intelligence and its exploitation in effective conduct of Cyber Warfare.
- Decision support, passage of orders and monitoring of Cyber Warfare, and feedback. This may include automated target fixation, selection of th of Cyber Warfare, media selection, generation of engagement and manoeuvre instructions and fixation of the parameters of time and space (e.g. a and other cyber-entities, followed by passage of orders).

The point to note is that Information Technology is the creator of cyber-space and also the core resource in the conduct of Cyber therefore, it is also the most lucrative target of Information Warfare, cyber-attack included.

Features of Cyber Warfare

Having seen that it is impractical to establish any clear distinction between the conduct of offensive and defensive Cyber Warfare, it w touch upon the mutually shared qualifying features. Accordingly, an overview of the likely 'approaches', 'targets' and 'points' of Cybe order.

Approaches of Cyber Attack: The approaches that could be adopted to carryout Cyber Attacks could be as follows:-

- Direct or Penetration Attack: This involves penetration into adversary's communication links, computer net work or data-base to steal or compro information in favour of the attacker.
- Indirect or Sensor or Media Attack: Insertion of false inputs into the adversary's observation sensors or sources to achieve counter-information of attack in this case.
- Hybrid Attack: This will be a combination of the above mentioned two types of attacks – a most likely approach.
- Cryptographic Attack: This involves one-time intrusion to locate vulnerabilities in the adversary's system of cryptography, for manipulation whe aim is achieved by breaking the 'key programme' which is the heart of the system's security.
- Net Exploitation: This is an extension of 'NETINT' (Network Intelligence) aimed at compromising or corrupting the adversary's information netwo malicious software executing agents, data scanners, 'Radio Frequency Interception' through wire tapping or remote 'sniffing', and software tools to synchronised attack upon multiple cyber-entities are the means to do so.

Targets of Cyber Attack: Unlike other forms of attack, in Cyber Warfare, there is no scope of achieving any residual consolatio Therefore, whatever be the approach adopted, a Cyber Attack has to be focused on a specific target. These targets could be:-

- Content Attack: In this case, content of the information is targeted for disruption or denial with the purpose of misleading the adversary's decisi
- Dislocating Attack: In this form of attack, the location of data or its route for access is targeted to cause confusion, delay or corruption of inform
- Temporal Attack: Here, either the retrieval of information is delayed till it is too late or a pre-conceived notion is reinforced well ahead of the ac the timeliness of information is subjected to disruption, thus diverting the adversary's process of decision making.

Cyber Attack Points: Data or network level Cyber Attacks may be directed at any of the following vulnerable points:-

- The adversary's input sources or reporting links, by means of electronic warfare, irrational visuals and deception. The other option is to alter the focus of input sensors by steering away the control mechanism.
- The process of object identification or tracking may be truncated by placement of hostile radiators.
- The adversary's sensor behaviour may be put through analysis to infer his focus of information query, and so gain insight of his objective.
- Degradation or deception of the adversary's deductive process may be achieved through network interference devices.
- The adversary's system design may be stolen, so as to acquire the capability of accessing his data base. This facilitates launching of Cyber Attac necessary.

Imperatives of Cyber Defence

It is seen that when it comes to planning and execution of Cyber Warfare, there is little to distinguish between attack and defence. The f Cyber Defence is difficult to achieve even after committing enormous resources unless it incorporates the ingredients of Cyber Attack prosecution of Cyber Warfare, there are certain defensive obligations to be adopted. These, in brief, are:-

- Warning mechanism for impending Cyber Attack, to trigger security drills including the automated response for safety or shut down.
- Retrieval of corrupted, diverted, destroyed or captured assets - such as primary, secondary and tertiary data, the operating protocols, automate
- Restoration of the compromised cyber driven systems - fiscal, transportation, power, industrial, technological and societal programmes, for exa

It will be noticed that only the first of the three responses has any room for retaliatory action, the rest being in-house measures. This l the fact that in the Cyber Warfare, defence comes a cropper unless its execution is facilitated by pre-planned intrusions into the adv establishment.

Conclusion

Being a relatively new form, it is important to develop indigenous postulations, concepts and practices of Cyber Warfare in the Indian suggests that the term 'Cyber Warfare' be usable in the context of military operations, as distinct from the overarching scheme of 'Cy national level. It also posits that when prosecuted under the overall ambit of Information Operations, Cyber Warfare is predominant in of may be conducted from space, earth and cyber-space. Further, it implies that: firstly, continuous engagement in Information Operation the system fully updated and promotes experimentation and the spirit of innovations; and secondly, readiness for instant engagement Cyber Warfare.

It is also reiterated that most of the principles and activities associated with Cyber Warfare are applicable, with certain reorient information infrastructure too. Indeed, since the state of war engulfs the entire nation, targeting the adversary's quasi-military and ci disrupt his national functioning may be an ultimate objective of Cyber Warfare. It is therefore absolutely necessary to adopt similar r sanctity of the nation's civil infrastructure, and so foster a regime of 'Cyber Security' at the national level.

"The wise man does at once what the fool does finally" – Niccolo Machiavelli.

References

"Information Warfare: Concept and Development", 21st Century Army: Strategies for Future, Lt Gen (Retd) Gautam Banerjee, Manas Publications, Waltz, Edward, "Information Warfare Principles and Operations" : ARTECH House, London, 1998. Fialka, JJ, "War by Other Means", New York: WW David and Katherine Hollis, "The Cyberspace Policies We Need", Armed Forces Journal, USA, 2010.

"Stray Voltage: War in Information Age", WM Hall, Naval Institute Press, USA, 2003. http://www.vifindia.org/article/2014/february/07/dimensions-of

Published Date: 28th April 2014, Image source: http://economictimes.indiatimes.com

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

Cyber Warfare in the Indian Context

The Cyber Space The contemporary era is characterised b

PLA's Information Warfare Capabilities on an Upward Trajec

In end February this year, Chinese President Xi Jinping formed a

Dimensions of C India

Preamble information therefore like

Preparing for Cyberwar - A National Perspective

On November 12th, 2011 Maj. Gen. Moghaddam, the "architect" of Ir

excellence to kick start innovative ideas and thoughts that can lead ...

Read More

I'm not a robot

reCAPTCHA
Privacy - Terms

Submit

VIF India
@vifindia
'The organs are the horses, the rein, the intellect is the charioteer the rider, and the body is the cha master of the household, the Kin of man, is sitting in this chariot.' #SwamiVivekananda