VIVEKANANDA INTERNATIONAL FOUNDA
Seeking Har

Dimensions of Cyber Security in India

7 Feb, 2014 Lt Gen Gautam Banerjee, Editor, VIF View6582 Comments 0

Preamble

This is the information age and therefore like all lucrative assets of the past ages, information assets must be an object of competition a
extreme cases, warfare. This conflict is being played out in a new domain: the cyber-space. With increasing dependency on the cybe
aspect of human endeavours, it is obvious that like all national assets, India's cyber-space has to be secured against all forms of esp
sabotage and attack.

In this article, it is proposed to discuss the theology of cyber security and the fundamental considerations that might lead to its effective
the Indian context.

Civil and Military Functions of Cyber Security

There are five domains in which the civil as well as military functions of national security have to be performed, viz, land, sea, air, space
In reference to the last named, it is a common supposition that there is singular convergence of civil and military functions. The misconce
the use of undefined terminologies and loose semantics which lead to confusing juxtaposition of concepts that govern the issue of cyber
though, the said convergence is no more prominent than it is in the context of civil-military interplay in all of the other domains of inte
and conflict. In order to make the best use of our resources in achieving a fair degree of cyber security therefore, it is important to p
consistency in ruling definitions and concepts in the Indian context.

We understand that every nation nurtures its own set of specific aspirations in consonance with a given set of geo-political, social and na
aspirations go to define the path for national prosperity which are then sought to be protected by the triumvirate of national power,
economic and military security. The first two of these aspects of security are civil functions whereas the third takes recourse to warfare
The distinction to note here is that the civil functions of socio-political and economic security of a nation is bound by inter-state ideologic
political adversities, competition for resources and business rivalries - all aimed at extracting more and more self-advantages. This is a c
Military security, on the other hand, is an extreme step that is performed as a last resort to force the adversary to desist from his un
either by threatening to, or by actually inflicting physical punishment on him. For the intervening periods of no-war, the purpose of the m
to prepare for that extreme eventuality called 'war'. This distinction between the civil and military functions of national security influence
cyber-space just as it does in others domains of competition and conflict; it has universal applicability.

Appreciation of the afore-stated distinction is more relevant in the Indian context. This is so because in the Indian dispensation, military
as a fulcrum of nationhood as it is in the case of America or China and a host of other countries. Recognition of the distinction would ob
discrepancies between the civil and military functions that is caused by use of undefined phraseology like 'cyber security', 'cyber-atta
etc.; our cyber policies must clearly convey as to what is intended to be accomplished.

Cyber Security and Cyber Warfare

In general, civil functions of national security involve fierce inter-state machinations that are marred by economic usurpation, in
technology denial, geo-political ganging etc. – all carried out under a façade of civility. These machinations, vicious as these may be, ar
as 'warfare' simply because there is no element of force-imposition here. In the civil domain therefore, cyber-intrusions, disablers
sabotage etc., and the counter-measures against these, may not be termed as cyber warfare. Conversely, 'cyber warfare' is a milita
prosecution is but a military operation, to be conducted in the spirit of extreme measures - just as it is in the case of conventional, s
nuclear warfare. Notably however, when it comes to cyber security skills and resources, there is near-total commonality between th
domains. In view of these subtle-yet-salient distinctions, formal apportionment between the civil functions of 'cyber security' from its m
'cyber warfare', is obligatory to obviate emergence of policy irrationalities.

Civil Functions of Cyber Security

Civil functions over the cyber-space have four denominators :-

- Public Services (health, education, civil-supplies, social security schemes, essential services),
- Financial Services (banking, subsidy funding),
- Industry (manufacturing, service sector, R&D, trade),
- Governance (policy, procedure, statistics, survey, records, administration).

The burden of cyber security is driven by inter-state political and ideological differences, competition for resources including 'knowlec rivalries and even terrorism. Accordingly, civil functions of cyber security aim at securing the cyber-space in a manner as to prevent following kinds :-

- Sabotage of 'National Information Infrastructure' (NII) through intrusion into electro-magnetic spectrum,
- Inducing collapse, corruption or diversion of the nation's Information Technology (IT) driven public service, administrative, economic, technical infrastructure.
- Psychological subversion of the society to manipulate public opinion.

Cyber-threat in civil domain may emanate from foreign or domestic sources, both adversarial or friendly. These sources could be state in economic and technological competitors, foreign military establishments as part of their war preparedness, and lastly, rogue r perpetrating acts of cyber-terrorism. The threats are characterised as follows:-

- Paralysis of cyber intensive systems at the national level to freeze the adversary's ability to function unencumbered.
- The saboteur may not be easily identifiable. Even if identified, the perpetrator's system architecture may be difficult to decipher, thus hamperinç action.
- Once triggered, even the perpetrator will not be able to control the intended degree of paralysing effects upon the adversary, neither is it possit damage from affecting unintended parties. To that extent cyber-sabotage is like terrorism.
- It would be banal to expect a nation to submit to launch, or the threat of launch, of cyber-sabotage. Therefore, it is not a civil deterrence like ec technology denial etc.
- Dependence on global cyber-assets like the Internet, GPS, digital information, satellite images etc. has some advantages too. Due to its world-v cyber-sabotage on one party would also cause collateral damages to the cyber-assets of unintended public and private sectors at the global arena caution upon the saboteurs.

Notably, in the matter of cyber security, only a thin line separates the passive and defensive measures with the active and offensive one must be a strong pro-active as well as reactive element of offensive built into the civil functions of cyber security. However, in institutir the problems of role-overlap and mix-up of organisations would arise. It would therefore be necessary to formally define the civil functio activities to distinguish these from their more intense and destructive military counterpart, and so obviate defocus and redundancy. Thi through promulgation of a comprehensive 'National Cyber Security Protocol' (NCSP), a part of which may remain confidential.

Cyber Security Mechanisms

Considering India's policy orientations, protection of the cyber-space from manipulations and intrusions from inimical parties would mos achieved through passive measures; execution of pro-active disabling actions seems to be rather farfetched in our context. Accordingly, t cyber security in our context would involve the following mechanisms:-

- Warning and response to cyber-attacks,
- Retrieval of cyber-assets – primary, secondary and tertiary data, protocols and processes, and,
- Restoration of the compromised cyber driven systems – economic, industrial, technological, societal systems.

It will be noticed that first of the three mechanisms involves adoption of pre-emptive and retaliatory counter-measures. The problem, hov cyber domain, defensive actions come the cropper unless coupled with pre-planned, debilitating cyber-intrusions. Therefore, notwithstan over policy endorsement, the mechanism must have an element of pro-active offensive to be able to warn and respond to an impendin other two mechanisms are skill, process and resource intensive in nature. Obviously, all three mechanisms have to be operative at full ge

For judicious and overarching control over these complex and widespread mechanisms, India will have to go beyond just promulgati security policies. Indeed, formal enunciation of an elaborate NCSP would meet that end. Further, to implement and control the NCSP, it v construct an organisation, duly empowered in terms of authority over policy direction, coordination, legal scrutiny and enforcement acros as private sectors.

Cyber Warfare in the Military Domain

In the military domain, operations that are undertaken to gain information superiority fall under the ambit of 'Information Warfare' (IW) offensive and defensive 'Information Operations' (IO) are waged by means of weaponised intervention, electronic warfare etc., 'cyber such mean that is prosecuted in the cyber-space. Cyber warfare therefore is truly a 'military operations of war', to be conducted as an e and defensive IO, and waged in the same spirit of ultimate measures. It is distinguished by predominance of offensive content and i through military-dedicated IT-based satellites, data warehouses, maps, communication net-works, GPS, UAV, AWACs, PGM etc. H functions are to be operational at all times, the military function during peace-time is to prepare and test continuously, letting go at war opponent's military, quasi-military and civil infrastructure. Herein lies the distinction between the civil and military functions of cyber se there are many commonalities between the two functions with respect to the above discussed civil cyber security mechanisms as well as hardware and processes.

Objectives of Cyber Warfare

The purpose of cyber warfare is to degrade the adversary’s surveillance, reconnaissance, command, control, communication and ir through cyber-attacks on his operational nerve centres. These are ‘disabling’ attacks which must be complemented with ‘disorienting aimed at registration of false information to the enemy and make him 'see' non-existent battle groups, missiles, bridges, etc, thus irrelevant committal of his forces. The combined result is expected to lead to disruption and dislocation of the enemy’s orchestration for w

As an element of IO in defensive as well as offensive modes, cyber warfare would focus upon the following aspects: -

- Command and Control Warfare (C2W): The objective is to attack the adversary’s ability to generate and communicate commands to its forces a his Defence Information Infrastructure (DII).
- Intelligence Based Warfare (IBW): It is the integration of sensors, processors and data-links to achieve efficient reconnaissance, surveillance, ta target engagement and finally, damage assessment.
- Electronic Warfare (EW): Communication as well as non-communication combat to achieve degradation, disorientation, interruption and corrupt adversary’s electro-magnetic emissions is classified as EW. In other words, it implies domination of electro-magnetic spectrum.
- Psychological Warfare: This is aimed at targeting the adversary's mental orientation and perception, and thereby influence his intent.
- Hacker Warfare: This is defined as destruction, degradation or corruption of adversary’s computer data-base and automated decision support ar processes.
- Infrastructural Warfare: Under the civil functions, this involves ‘information blockade’ and ‘information imperialism’ to derive political and econo Under warlike conditions, its extreme manifestation leads to attacks on the adversary’s primary infrastructure – railways, power plants, oil sector e

The Regime of Cyber Security

Most advanced countries have instituted robust mechanisms to protect their cyber domain. In this respect, USA enjoys overwhelming sup takes care to keep her elaborate activities under wraps. Besides passive measures, she secures her cyber-space by technology drive complex cyber-intrusions and backs it up with deliberate enticement of cyber-attacks from adversaries and friends alike to break into th so, civil and military functions of cyber security are seamlessly enmeshed to produce the best results, cyber- attacks like ‘Gauss’, ‘Stuxn etc. being a few known ones. China, on the other hand, depends upon her innovative mass of cyber operatives, reportedly two million str cyber security regime, much of which is committed on internal surveillance and the rest being devoted to intrusive hacking. The scor nations stands even despite many reported hacking attacks from China and Russia, not to speak of their all-weather ally, the US. In any the centre-stage of global circus, the European stakes are mainly limited to economic cyber-assets.

India is a novice in comparison, even if there have been some tentative attempts made to venture into the realm of cyber security. however, more or less confined just to work-station access-denials, blocks against hacking and back-up storage. Whereas the private se baby-steps to maintain a facade of security of its IT-based assets, the state, nonplussed as it seems to be in the matter, is not motivated beyond promulgating a policy-outline that cries out for more serious substance. Of course, certain laudable efforts have been made ir intelligence set up and the ‘Department of Electronics and Information Technology’, but these are individual rather than institutio therefore confined just to specific bands of the threat-spectrum.

A Structure for Cyber Security

Having discussed the functions of civil cyber security and military cyber warfare and the differences as well as commonalities between t apparent that: One, there would have to be a substantial degree of congruence of resources and efforts in protecting the Indian cyb when it comes to prosecution of cyber warfare, it would have to be a purely military venture. Thus appears the necessity for an apex these primary and secondary functions at the national level. Accordingly, we may conclude the discussion with a brief look at some of might afford the desired level of protection to the indigenous cyber-space. These measures could be:-

- Establishment of a ‘National Cyber Regulatory, Control and Security Authority’ (NCRCSA), to coordinate between the civil NCSP and the military Incorporation of a ‘Cyber Research Department’ would also be necessary.
- Regulation, coordination and strengthening of the civilian cyber activities of the ‘National Information Centre’, ‘National Crisis Management Cent Response Centre’, ‘National Information Infrastructure Protection Centre’, ‘Computer Emergency Response Teams’, NDMA, NTRO, Department of IT and the private sector under the aegis of the proposed NCRCSA. The responsibility and wherewithal for cyber security is too diffused at present to cyber-attack, and respond to it quickly and effectively.
- ‘Cyber Command’ may be formed to plan and prepare prosecution of Cyber Warfare across the service barriers, and in coordination with the nat A ‘Cyber Warfare Research Establishment’ must form part of this Command. NCSP and Cyber Warfare must be permanent and continuously perfor with permanent set ups and flexible recruitment and training rules, and as stated, function under the overarching management of the proposed NC

Conclusion

The stage when creation of cyber-assets becomes contingent upon its robust protection has arrived in India. It is time therefore to acc cyber security even if it means some compromise with proliferation of the nation’s cyber domain. The foremost consideration in seeking our cyber security has to remain inviolable, the security measures have to be tailored to Indian conditions and devised by native genius further reinforces the cause of formal apportionment of roles and responsibilities between the civil and military functions of cyber security

Published Date: 7th February 2014, Image source: http://1.bp.blogspot.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

Commentary : Australia Defines Priorities of National Securi

The Government of Australia, on May 1, 2018 (Australian Governmen

नीला हौज़ निर्मित झील प�

22 मार्च, 'विश्व जल दिवस' क

The Future of Ba to China

China's rap become t largest econ

Commentary: The Neela Hauz Constructed Wetland System

22nd March is commemorated as 'World Water Day'. O

Commentary: International Solar Alliance - India's Radiant

On March 11 ,2018 India led the world into a new era of mutually

Commentary: Sc in Unmanned O Tech

Propelled enabling co like all-weat

India should take up challenge of Lethal Autonomous Weapons

हंटर किलर से मौतें अपर�

दुनिया के विभिन्न हिस्स�

Commentary: Fi Attack has Happ

'We knew i coming' – sources are

About Us

The Vivekananda International Foundation (VIF) is a New Delhi-based think tank set up with the collaborative efforts of India's leading security experts, diplomats, industrialists and philanthropists under the aegis of the Vivekananda Kendra. The VIF's objective is to become a centre of

Contact Us

Name*

Email Id*

Phone Number*

Message*

Tweet With Us

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 charioteе
the rider, and the body is the ch
master of the household, the Ki
of man, is sitting in this chariot.'
#SwamiVivekananda