# Cyber Security

## Build-up of India's National Force

2

**Gabi Siboni,**[1] Senior Research Fellow and Director,
Military and Strategic Affairs and Cyber Security Programs,
Institute for National Security Studies, Israel

Cyberspace creates countless opportunities alongside complex challenges. India, as a technologically advanced country with substantial online services and businesses, is highly dependent on computer communication and control systems. This is not unique to India alone, but is a global phenomenon. That is, the more that countries or organisations rely on developing technology in cyberspace to run, manage and control business operations, the greater their vulnerability and the greater the risk of severe disruption of these technologies.

Today, there is a common understanding that cyber security threats are one of the most serious challenges for national security, public safety and the economy for every nation and for the entire global society. There are innumerable examples of misuse of cyberspace. Events in recent years show that cyberspace has become an area of much activity and conflict; countries and organisations receive state support to act against other countries; others operate for reasons of intellectual property espionage and theft. Another group of active attackers are terrorists who use cyberspace to promote their own agenda, exploiting the ability to remain anonymous. Criminals and criminal organisations operate in cyberspace for money theft, blackmail and financial fraud. Finally, cyberspace accommodates ad-hoc individuals and groups of activists operating at any given moment against a common target. Correlating these developments with India's National Cyber Security Policy vision[2] requires the country to initiate a process that will transform India to a more secure place to do business in and to use services in cyberspace. Such a process will enhance India's resilience against cyber attacks and its abilities to better protect its interests. Moreover, it will help shape an open and stable cyberspace that would support India's economic development and help build India's cyber security knowledge base, skills and capabilities.

[1] The author wishes to thank Mrs. Hadas Klein, Cyber Forum Manager at the Cyber Security Program, INSS, for her assistance in researching and writing this article.

Over a year has passed since India set out its National Cyber Security Strategy. The release of the policy framework in 2013 was an important step towards securing India's cyberspace. However, there are certain areas that need further consideration for the actual implementation of the strategy.

This paper discusses conceptual pillars for the process of building a force for cyber security, which would focus on a high-level defence approach, with the aim of improving the security and resilience of national information infrastructures and services.

## The Five Pillars of Building a National Cyber Security Force

The process of building a national cyber security capacity would entail long-term preparation requiring various stakeholders, projects and developments to enable a sustainable systematic and targeted force build-up. This process is a significant challenge requiring a national effort.

This model comprises of five basic pillars:

- *Formulation of national strategy in cyberspace:* This is the foundation upon which the entire process of building the force rests. This will involve drafting the nation's resources and management to improve cyberspace abilities and worldwide position.
- *Technological development of cyber security capabilities:* These are needed to allow the implementation of the strategy.
- *Development of human resources and human capital:* These are needed to allow for the effective use of developed technology within the strategy framework.
- *Definition of the organisational structure:* This will support the strategy.
- *Training and assimilation of the entire force:* This will ensure that all systems function properly and will provide the opportunity to systematically refine and develop knowledge.

### *National Strategy*

The development of a national strategy is the initial phase of building the force and it must address two different perspectives:

- An offence strategy in cyberspace must be prepared, as India needs to respond to large-scale cyber attacks. It needs to have a clear strategy of how it would react to hostile action threatening the government, military, the health of its citizens or the country's economy. As an offence strategy has a distinct mission, it is not the focus of this article but should be discussed in a parallel process.
- A comprehensive defence approach must be developed that reflects India's cyberspace vision.

[2] Drafted by the Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India. The full version can be found at http://deity.gov.in/content/national-cyber-security-policy-2013-1.

The defensive strategy needs to address the unique security protection requirements of the following groups:

- National security organisations and sensitive defence industries;
- Critical national infrastructure;
- Government services; and
- The civilian sector.

It is assumed that the first three groups are more secure and regulated and that the fourth group, the civilian population, is the most vulnerable. This group includes civilian organisations, businesses and private users; typically, this group has no guidance for cyber security, and since the entities in this group are not regulated, they are the most vulnerable to attackers, who in any case prefer to target those less protected. One can only imagine the impacts of a successful terror attack occurring against one of India's large food manufacturing plants or against a private financial organisation, or the effect of an intellectual property cyber theft from one of India's technological companies. At the same time, changes in the structure of the Indian economy and privatisation processes should sharpen the understanding that cyber security needs of the civilian sector have to be addressed with greater attention.

One of the key elements of the process of developing a cyber security strategy is the inclusion of national cyber security risk assessment, with specific focus on critical information infrastructures. Based on risk analysis, the strategy should define the minimal defensive measures to be taken in each of the pillars defined for building a national cyber security force. India needs to evaluate where it is standing and where it needs to focus its resources and investments in order to increase, in the global context, the resilience and security of its national information and communication technology assets, which support critical functions of the state. Such an evaluation needs to be done in four different areas:

- The nation's ability to have accurate early warnings of cyber security-related events;
- The nation's capabilities to prevent cyber incidents;
- The nation's competence to detect and identify security events; and
- The nation's response capabilities, which should be measured separately for early warnings and for a particular event or series of events to mitigate the situation, to take further corrective actions in relation to identified deficiencies and to prevent these events from recurring.

Alongside, there are two key phases in the development of a national cyber security strategy: Developing and executing the strategy, and evaluating and adjusting the strategy. A lifecycle approach needs to be adopted—i.e., the output of the evaluation phase should be used to maintain and adjust the strategy itself, and the national strategy should be able to quickly respond to emerging cyber security issues and emerging threats. The strategy objectives also need to be priorities; this is of paramount importance for successful implementation and for constant improvement.

The success of the implementation of India's national cyberspace strategy relies on the remaining four pillars of building a cyberspace force.

### *Technology and Means*

A country that leads in cyber security technology enjoys economic advantages as well as cyberspace geopolitical domination. Moreover, the application of constantly evolving defence tools is required to achieve a country's vision for cyberspace—today and in the future. It brings innovation to the protection of critical infrastructures, enhanced command and control capabilities, and high quality of intelligence, among other elements. Obviously, there are also advantages of precise and rapid attack capabilities in the realm of offence. These capabilities contribute to a nation's power, and strengthen its national security and international position.

Some of the challenges India is facing today are at the level of its cyberspace hygiene, the lack of cyber security information-sharing tools and best practice, the lack of internal cyber monitoring, and the lack of proactive cyber defence capabilities within the country's critical infrastructure.

It is important that India invest in acquiring the proper technology and means, both by internally developing new technologies and by purchasing from the private sector or allied governments. A coordinated national effort to encourage the private sector by funnelling research and development (R&D) investments to develop new cyber security-related defence tools and concepts of defence operations should be part of this phase. Investing in R&D and putting in seed money in new technological companies is one of the tools to make sure new technologies and cyber security products are synchronised with the strategy requirements. It would also serve two additional Indian objectives: Better customised products to defend itself, and the promotion of the country as an exporter of technology. For example, one of the components of India's cyberspace strategy will probably be the establishment of an integrated national Computer Emergency Response Team (CERT), as will be elaborated further on in a subsequent section. Thus, funding of R&D for dedicated early warning technologies may be required.

It is important that India should strengthen its cyber defence R&D programmes and further support and prioritise development of the cyber defence industry. The government needs to coordinate cooperation between security and defence organisations, such as military and intelligence agencies, and between high-tech R&D companies.

### *Development of Designated Human Resources*

Human resource and human capital development, together with the technological development of tools and methods, must be fully integrated and synchronised, so as to maximally utilise all national resources for the fortification of India's cyber capabilities.

For example, a cyber security workforce needs to stay up to date with emerging risks, threats and cyber security technologies that typically require frequent knowledge acquisition and extension of studies.

Another issue to be considered is innovation in cyber security, from both the offensive and defensive perspectives, to be among the world's leaders. This can be achieved by inter-sectoral partnerships and by providing flexibility to cyber security talents to move and integrate easily between sectors like high-tech, academia, government agencies and the private sector to constantly develop skills and advance India's knowledge base for the development of future opportunities.

From a long-term perspective, it is important to define the overall cyber security workforce requirements to ensure that the country is investing in the right type of education for specific types of workforces and is keeping pace with the workforce demand.

The development of a workforce for cyber security needs to address the typical duties and skill required. In 2013, the National Institute of Standards and Technology (NIST) of the US Department of Commerce released a workforce framework[3] identifying seven cyber security workforce categories:

- *Securely Provision:* Workers are responsible for conceptualising, designing and building secure information technology (IT) systems (i.e., responsible for aspects of systems development).
- *Operate and Maintain:* Involves workers who specialise in areas of providing support, administration and maintenance, necessary to ensure effective and efficient IT system performance and security.
- *Protect and Defend:* Workers are responsible for identification, analysis and mitigation of threats to internal IT systems or networks.
- *Investigation:* Involves workers who specialise in investigation of cyber events and cyber crimes.
- *Collect and Operate:* Personnel are responsible for specialised denial and deception operations and collection of cyber security-related information that may be used to develop intelligence.
- *Analyse:* Analysts are responsible for highly specialised review and evaluation of incoming cyber security-related information to determine its usefulness for intelligence.

[3] The National Cybersecurity Workforce, National Initiative for Cybersecurity Education (NICE), 2013, http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf.

- *Oversight and Development:* Workers are responsible for providing leadership, management, direction and advocacy, so that individuals and organisations may effectively conduct cyber security work.

These categories, presented by the NIST, may not be fully in line with India's cyber security strategy. India should identify its professional cyber security needs in a way that would support the technological advances being encouraged in the country. This requires coordinated staff work and long-term educational planning (for all levels of education, from early schooling to advanced academia programmes) across all relevant cyber security categories mentioned above. For example, the need to develop civil cyber defence requires the academic development of designated human resources; these will fill positions in the civil defence sector in technology development, security consumer organisations, as well as the country's national regulatory bodies that will comprise the civil defence force.

### *Organisation: Utilising the National Potential*

Most of the organisations in India have naturally developed some preoccupation with cyberspace and it is assumed that security organisations are building their own cyberspace capabilities to support their basic tasks. However, there is work to be done in two dimensions:

1. The first is the need to conduct a macro-analysis of the nation's cyber security needs, and accordingly build the nation's cyber security ecosystem and define the roles and responsibilities of the various relevant entities. A good starting point is the initiation by the Government of India of the National Critical Information Infrastructure Protection Centre, which is becoming more active and relevant. This should be followed by the establishment or further strengthening of other bodies and initiatives such as:

- The National Computer Emergency Response Team–India: This will improve national coordination of cyber incidents, and act as a focus point for international sharing of technical information and feeds on cyber security. A CERT unit also needs to include a national Security Operation Centre (SOC), which would function as a hub for monitoring the network and detecting anomalies. An SOC would also be responsible for issuing alerts to users and providing advice on best security practices. Such an entity has a great impact on the defence strategy iterative cycle—i.e., early warning, prevention, detection and response, as stated above. Establishment of a national CERT will promote India's resilience to cyber attacks and maintain its interests in cyberspace.
- National Cyber Crime Unit: This will further develop India's capabilities to combat the threat from cyber criminals. Such a unit will make India a more secure place to conduct online business.
- India also needs to consider developing initiatives that would enhance collaborations between government, industry, academia and law enforcement agencies to better coordinate efforts to reduce cyber crimes. Such collaborations will raise awareness, improve reporting and help the industry become more resilient to threats.

- Law enforcement capabilities need to be further developed to tackle cyber crime and enhance the society's confidence in conducting online business and using online services.
- Initiatives for international cooperation will promote India's interests in cyberspace. This should include cooperation with UN committees, regional (South Asia and Asia Pacific) politico-economic unions and the Commonwealth of Nations. India also needs to promote international cyber conferences. Such initiatives will help shape an open, vibrant and stable cyberspace that would support the nation's needs and the global community.
- It is advisable to establish regulators for the protection and guidance of the government ministries and authorities, and the exposed civilian sector.
- India needs to run an awareness campaign reaching out to the private sector to raise awareness of threats and to encourage business, as well as to embed effective cyber security risk management practices.

The above are a few examples of required cyber security initiatives and missions at the national level. It is highly important to plan India's cyber security organisational structure by mapping the cyber security strategy objectives. This will ensure that all activities and cyber security operations are aligned with the strategy.

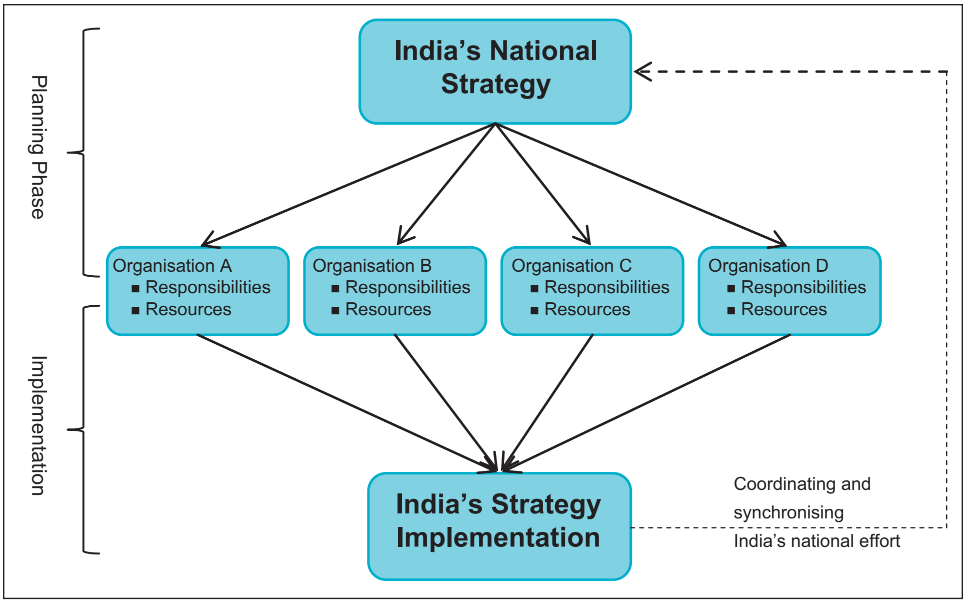
2. The second dimension is the need to define the relationships between the organisations and establish the parameters of authority of each one. This step will be the culmination of the process of building a cyber security force (see diagram on next page).

### *Drills, Training and Assimilation*

Drills are a core component of the proposed cyber security force build-up to generate know-how and enable organisations to better prepare themselves for various scenarios. Though operational drills usually address specific scenarios (readiness for cyber attacks, IT incidents, equipment failure and more), the know-how developed as a result of these drills always exceeds the narrow limits of the specific scenario. Typically, operational drills are conducted at all levels of the organisation, up to the supreme command level. Security organisations routinely carry out training, exercises and drills. It is important to adopt the concept in the civilian sector, which is known to be the most exposed to damage caused in cyberspace.

National training programmes should be established and should focus on improving the civilian sector and the individual's knowledge of risks and vulnerabilities in cyberspace. They should also help the public learn how to deal with intrusions on their computers and devices, and encourage and promote the use of cyber security resources and tools.

In addition, there should be an annual national cyber protection exercise featuring a scenario of several cyber security incidents in a simulated environment, with clear objectives of testing escalation processes and national level coordination procedures. The exercise must challenge all pillars listed for the force build-up to regularly improve and



enhance the national response. The exercise will serve as a basis for the development of operational plans that will improve India's readiness to respond to cyber attacks.

## An Overall View

The National Cyber Security Strategy will be the keystone of the national force build-up. Once this has been formulated, two main efforts need to be launched and synchronised: The development of technology and means, and the development of human resources. Those two are to be funnelled into organisations, each of which has predefined responsibilities (and authority) and is allocated required resources, such as budgets, tools and people. Drills and exercises, both in the local and the national arena, must be part of the strategy implementation. Of course, the government will need to continuously monitor and synchronise the national force build-up process, and will have to take required measures to make necessary corrections.

In July 2013, India declared its National Cyber Security Strategy. Now it is time to move to the next phase and formulate a comprehensive force build-up process. India needs to establish key elements of the planned activities over the short, intermediate and long term in support of the strategy. The strategy assessment process should be undertaken to verify progress and make adjustments as necessary, in response to changes in the technological and threat environments. This should be done on an iterative basis to make sure that the level of cyber security is constantly enhanced. Implementation of such a process could move India to the next generation of cyber security readiness and position it with leading nations in the arena of cyber security preparedness.