CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 222 April 2020

India's National Cyber Security Strategy: How to Go About It

Major General PK Mallick, VSM (Retd), is an Electronics and Telecommunication Engineering graduate from BE College, Shibpore. He was commissioned in the Corps of Signals. M Tech from IIT, Kharagpur and alumni of DSSC, CDM and NDC, the officer has wide experience in CI Ops, command, staff and instructional appointments. He retired from the National Defence College as a Senior Directing Staff (Army). The officer has interest in Electronic Warfare, Cyber Warfare and Technology. He has published a large number of papers in reputed journals. He runs a popular blog on national security issues. Currently, he holds the COAS Chair of Excellence at CLAWS.

The exponential growth and rapid adoption of information and communication technologies (ICT) with its associated economic and social opportunities have benefited billions of people around the world. The Internet has become the backbone of modern businesses, critical services and infrastructure, social networks and the global economy. The confidentiality, integrity and availability of ICT infrastructure are challenged by cyber threats including electronic fraud, theft of intellectual property and personal identifiable information, disruption of service and damage or destruction of property. Cyber security is a foundational element for achievement of socio-economic objectives of modern economies. It encompasses governance policy, operational, technical and legal aspects.

A National Cyber Security Strategy (NCSS) is a plan of action designed to improve the security and resilience of national infrastructures and services. It is a top-down approach to cyber security that creates a range of national objectives and priorities that should be achieved in a specific time frame. By developing and implementing a National Cyber Security Strategy, a nation can improve the security of its digital infrastructure and ultimately contribute to its broader socio-economic aspirations. The government has a major role and responsibility in cyber security arena. About 76 countries have already published their national cyber security strategy outlining key steps that are intended to increase their national security and resilience.[1]

Key Points

- The National Cyber Security Policy (NCSP) was published in 2013 by the Ministry of Communication and Information Technology. An initiative has been taken to publish the National Cyber Security Strategy of India—2020 under the aegis of the National Security Council Secretariat.
- National Cyber Security Strategy development process should translate the government's vision into coherent and implementable policies that will help it achieve its objectives.
- Nation states all over the world have published their National Cyber Security Strategy. They need to be perused before finalising India's National Cyber Security Strategy.
- India's stance on offensive cyber operations may be included and publication of the National Cyber Strategy may also be considered.

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

CLAWS Vision: To establish as a leading Centre of Excellence, Research and Studies on Military Strategy & Doctrine, Land Warfare, Regional & National Security, Military Technology and Human Resource.

Website: www.claws.in Contact us: landwarfare@gmail.com

International Telecommunication Union (ITU) has recommended that the cyber security roles and responsibilities of government can be organised loosely into the following categories:[2,3]

- Policy-making.
- Legal Measures.
- Organisational Structures.
  - Institutional organisation and coordination.
  - Incident management and cyber security readiness assessment.
- Capacity building.
- Public-private sector cooperation and industry regulation.

The preparation of a national cyber security strategy is an essential first step in addressing cyber security challenges. Typically such a strategy:

- Highlights the importance of ICTs to the nation.
- Classifies and evaluates potential risks and threats such as cyber attacks, cyber crime, etc.
- Sets up cyber security related objectives like protection of data resources, containment of cyber attacks and detection and prosecution of cyber crime.
- Highlights the actions to be taken in order to achieve those objectives like implementation of cyber security standards, creation of incident response centres, enhancing consumer awareness, etc.
- Identifies the roles and responsibilities of all stakeholders in the process.

Indian Scenario

The Indian Computer Emergency Response Team (CERT-In) was established in 2004 and continues to act. India has undertaken several steps for the protection, detection and containment of the potentially disruptive attacks against the nation's networks. Initiatives such as Digital India and Smart City and the increasing involvement of the private sector in nation-building endeavours are progressive steps that are also increasing the scope and complexities of cyber security efforts.

The Information Technology (IT) Act was introduced as early as 2000. The National Cyber Security Policy (NCSP) was enunciated in 2013 by the Ministry of Communication and Information Technology. The National Cyber Security Policy lacked the following key elements:

- Milestones and performance measures.
- Cost and resources.
- Roles and responsibilities.
- Linkage with other key strategy documents.

Since the adoption of NCSP 2013, the technologies, platforms, threats, services and aspirations have changed tremendously. The present cyber threat landscape poses significant challenges due to rapid technological developments such as Cloud Computing, Artificial Intelligence, lnternet of Things, 5G, etc. New challenges include data protection/privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms, international cooperation on cyber crime & cyber terrorism, and so on. Threats from organised cybercriminal groups, technological cold wars and increasing state sponsored cyber attacks have also emerged. Existing structures may need to be revamped or revitalised.

The Indian Government under the aegis of National Security Council Secretariat through a Task Force is in the process of formulating the National Cyber Security Strategy 2020 (NCSS 2020) to cater for a time horizon of five years (2020-25). Its proposed vision is to ensure a safe, secure, trusted, resilient and vibrant cyber space for our Nation's prosperity.

The comments have been sought through internet on three pillars of cyber security: secure (national cyberspace), strengthen (structures, people, processes, capabilities), and synergise (resources including cooperation and collaboration).[4]

Policy or Strategy

The document published in 2013 by the Ministry of Communication and Information Technology was a policy statement. The proposal is now to make a National Cyber Security Strategy. In management jargon there are differences between policy and strategy.

Difference between Policy and Strategy

The term 'policy' should not be considered as synonymous to the term 'strategy'. Policy is a guide to the thinking and action of those who make decisions, while strategy concerns the direction in which human and physical resources are deployed and applied in order to maximise the chance of achieving a selected objective in the face of difficulties. A policy embraces both thought and action, while strategy concentrates mostly on action, i.e. it is mostly 'action-oriented'.

Policy is a contingent decision, whereas strategy is a rule for making decision. A contingent even is recognised because it is repetitive, but the time of its specific occurrence cannot be specified. It is not advisable to require a new decision on what should be done each time when a contingency arises.

It is better to prescribe, in advance, the response to be made whenever a specified contingency occurs. This is done through policy formulations. Specification of strategy is forced under conditions of partial ignorance when alternatives cannot be arranged and analysed in advance. The strategy decision is taken under the conditions where all the facts are not known, which may not be lasting because of the further knowledge of the facts.

The following are the major differences between strategy and policy:[5]

- The strategy is the best plan opted from a number of plans, in order to achieve the organisational goals and objectives. The policy is a set of common rules and regulations, which forms as a base to take the day to day decisions.
- The strategy is a plan of action while the policy is a principle of action.
- Strategies can be modified as per the situation, so they are dynamic in nature. Conversely, policies are uniform in nature. However, relaxations can be made for unexpected situations.
- Strategies are associated with the organisational moves and decisions for the situations and conditions which are not encountered or experienced earlier. On the contrary. policies define the rules for routine activities, which are repetitive in nature.
- Strategies are concentrated toward actions, whereas policies are 'decision-oriented'.

We should be careful about the terminologies being used. Since strategy follows the policy, does the NCSP 2013 hold good for the National Cyber Security Strategy 2020 (NCSS 2020) being formulated? Are there any changes in the policy?

However, nation states normally do not publish their cyber security policies. A simple google search would indicate that. However most of the countries have now enunciated their NCSS.

Cyber Security Strategy

Cyber security is a complex subject whose understanding requires knowledge and expertise from various fields, including computer science and information technology, engineering, decision sciences, psychology, sociology, economics, organisational behaviour, political science, international relations and law. Cyber security is not primarily a technical matter though technical measures are an important element. There is a tendency for policy analysts and others to get lost in the technical details.

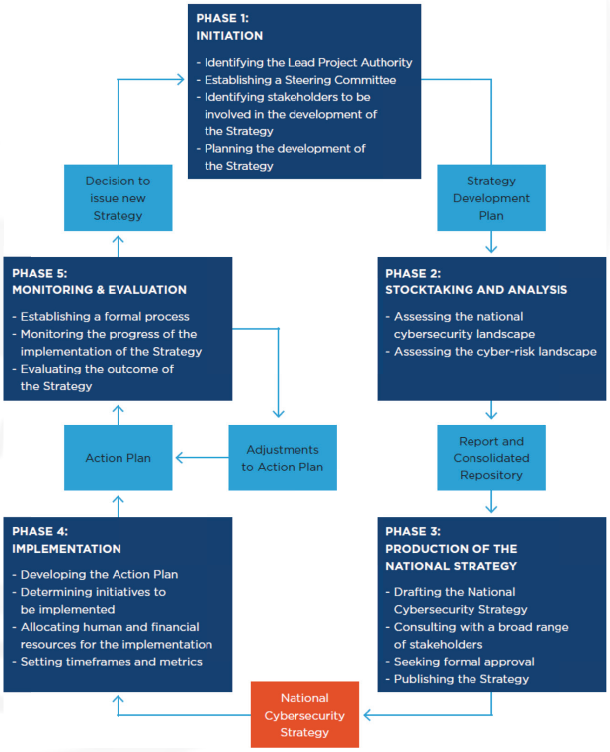
The national cyber security strategy should enable government entities to identify strategic objectives, translate this vision into coherent and implementable policies, to pinpoint the resources necessary for achieving such objectives and provide guidance for the use of these resources and explain how the NCSS is linked to other related strategies.

Should the complete document be open to public or some sections which are of classified nature should remain undisclosed? Since so much efforts are being put in, therefore, it will be a good idea to keep a classified part separate which will assist in coordination and synchronisation of the defence organisations, intelligence agencies and law enforcing authorities operating in cyber domain.

The Process of Making a National Cyber Security Strategy

National Cyber security Strategy development process should translate the government's vision into coherent and implementable policies that will help it achieve its objectives. This includes not only the steps, programmes and initiatives that should be put in place, but also the resources allocated

Figure 1: The Process of Making a National Cyber Security Strategy


PHASE 1:
INITIATION
- Identifying the Lead Project Authority
- Establishing a Steering Committee
- Identifying stakeholders to be involved in the development of the Strategy
- Planning the development of the Strategy
Decision to issue new Strategy
Strategy Development Plan
PHASE 5:
MONITORING & EVALUATION
- Establishing a formal process
- Monitoring the progress of the implementation of the Strategy
- Evaluating the outcome of the Strategy
PHASE 2:
STOCKTAKING AND ANALYSIS
- Assessing the national cybersecurity landscape
- Assessing the cyber-risk landscape
Action Plan
Adjustments to Action Plan
Report and Consolidated Repository
PHASE 4:
IMPLEMENTATION
- Developing the Action Plan
- Determining initiatives to be implemented
- Allocating human and financial resources for the implementation
- Setting timeframes and metrics
PHASE 3:
PRODUCTION OF THE NATIONAL STRATEGY
- Drafting the National Cybersecurity Strategy
- Consulting with a broad range of stakeholders
- Seeking formal approval
- Publishing the Strategy
National Cybersecurity Strategy

Source: The International Telecommunication Union (ITU), The World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), 2018, Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity, Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

for those efforts and how these resources should be used. Similarly, the process should identify the metrics that will be used to help ensure that, the desired outcomes are achieved within set budgets and timelines.

There is a clear distinction between the process adopted by countries for making a National Cyber Security Strategy and the content, the actual text that would appear in a National Cyber Security Strategy document. National Cyber Security Strategy development process should be able to translate a government's vision into coherent and implementable policies that will help it achieve its objectives. For this, the resources should be allocated and guidelines must be issued for utilisation of these resources. The process should make out the metrics which will be useful to ensure that desired outcomes are achieved within set budgets and timelines.

Figure 1 illustrates the lifecycle of strategic thinking about cybersecurity at the national level.

Generally, a National Cyber Security Strategy should have:

- Vision, objectives, principles and priorities to address cyber security.
- Roles and responsibilities of the respective stakeholders tasked with improving cyber security of the nation.
- The plan, steps and initiatives that a country should undertake to protect its national cyberinfrastructure and increase its security and resilience.
- National cyber security strategy is typically developed through consultation with all relevant stakeholders, including government institutions, industry, academia and civil society. In order to get the attention of all stakeholders and the importance of national cyber security strategy, normally it is promulgated at a very high level of government, often by the head of government. This indicates that governments do not regard cyber security as a narrowly defined question of national security or a security issue, but a socio-economic concern which affects the whole of society.

Principles of National Cyber Security Strategy

The strategy should**:**

- Set a clear 'whole-of-government' and 'whole-of-society' vision.
- Result from an 'all-encompassing' understanding and analysis of the overall digital environment, yet be tailored to the country's circumstances and prioritised.
- Develop with the active participation of all the relevant stakeholders. It should address their needs and responsibilities.
- Foster economic and social prosperity and maximise the contribution of ICT to sustainable development and social inclusiveness.
- Enable an efficient management of cyber security risks and drive the resilience of the economic and social activities.
- Utilise the most appropriate policy instruments available, to realise each of its objectives, considering the country's specific circumstances.
- Set at the highest level of the government, which will then be responsible for assigning relevant roles and responsibilities and allocating sufficient human and financial resources.
- Help build a digital environment that citizens and businesses can trust.

Learning from Best Practices

The process of making a national cyber security strategy has been explained by different reputed organisations. Some of them are enumerated below.

What is a National Strategy for Cyber Security?

The IT giant Microsoft corporation has published a remarkable document on *Developing a National Strategy for Cyber security: Foundations for Security, Growth and Innovation.*[6] It states: a national cyber security strategy outlines a vision and articulates priorities, principles and approaches for understanding and managing risks at the national level. Priorities for national cyber security strategies will vary from country to country. The most successful national strategies share three important characteristics.

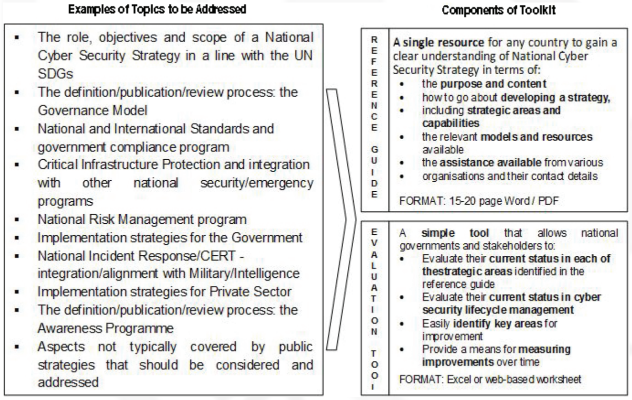
- They are embedded in 'living' documents that have been developed and implemented in partnership with key public and private stakeholders.
- They are based on clearly articulated principles that reflect societal values, traditions and legal principles. Programs created by government in the name of security can potentially infringe on these rights and values if not articulated and integrated as guiding principles.
- The strategies are based on a 'risk-management approach' where governments and private sector partners agree on the risks that must be managed or mitigated, and even those that must be accepted. A national strategy, if developed correctly, can meet many needs of government, the private sector and the citizens of the country.

Microsoft recommends the following six foundational principles as the basis for a national strategy:

- **Risk based:** Assess risk by identifying threats, vulnerabilities and consequences, then manage it through mitigations, controls, costs and similar measures.
- **Outcome focused:** Focus on the desired end state, rather than prescribing the means to achieve it and measure progress towards that end state.
- **Prioritised:** Adopt a graduated approach to criticality, recognising that disruption or failure are not equal among critical assets or across critical sectors.
- **Practicable:** Optimise for adoption by the largest possible group of critical assets and implementation across the broadest range of critical sectors.
- **Respectful of privacy and civil liberties:** Include protections for privacy and civil liberties based upon the established privacy and civil liberties policies, practices and frameworks.
- **Globally relevant:** Integrate international standards to the maximum extent possible, keeping the goal of harmonisation in mind wherever possible.

The International Telecommunication Union (ITU) has suggested the heading and contents for a Draft National Cyber Security Strategy.[7] The suggested toolkit is given below.

Figure 2: A Toolkit to Help States to Develop National Cyber Security Strategies



Examples of Topics to be Addressed

- The role, objectives and scope of a National Cyber Security Strategy in a line with the UN SDGs
- The definition/publication/review process: the Governance Model
- National and International Standards and government compliance program
- Critical Infrastructure Protection and integration with other national security/emergency programs
- National Risk Management program
- Implementation strategies for the Government
- National Incident Response/CERT - integration/alignment with Military/Intelligence
- Implementation strategies for Private Sector
- The definition/publication/review process: the Awareness Programme
- Aspects not typically covered by public strategies that should be considered and addressed

Components of Toolkit

REFERENCE GUIDE

A single resource for any country to gain a clear understanding of National Cyber Security Strategy in terms of:

- the **purpose and content**
- how to go about **developing a strategy,**
- including **strategic areas and capabilities**
- the relevant **models and resources** available
- the **assistance available** from various
- organisations and their contact details

FORMAT: 15-20 page Word / PDF

EVALUATION TOOl

A **simple tool** that allows national governments and stakeholders to:

- Evaluate their **current status in each of thestrategic areas** identified in the reference guide
- Evaluate their **current status in cyber security lifecycle management**
- Easily **identify key areas** for improvement
- Provide a means for **measuring improvements** over time

FORMAT: Excel or web-based worksheet

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) has published a detailed procedure for making a national cyber security strategy. The check list for preparation of national cyber security strategy is given at Appendix.[8]

One of the Israeli think tanks has suggested the following process for cyber security strategy making.[9]

Boundaries of the Policy and Strategy Papers on a National Level

- **National Cyber Security Strategies Published by Different Countries:** Nation states all over the world have published their National Cyber Security Strategy. These are available at: https://ccdcoe.org/library/publications/. All the above documents are recommended to be perused before finalizing the national cyber security strategy.

Questions to be Considered When Developing the Cyber Security Strategy

- **The Role of Government and the Private Sector:** There is a need for the private sector to take up responsibility of national cyber security. There is a need for more engagement with the private sector and consider specific areas of responsibility. There must be a clear mutual understanding as to where the government responsibility ends and private sector accountability begins.
- **Raising Cyber Security Standards:** There is a need for indigenisation in the core network infrastructure. Government should encourage more Indian companies who should be able to offer cyber security advice, products and services.
- **Role of Regulators:** Regulators can enhance security standards. Regulators will need to be equipped with the skill and capability to play their role. Private sector will resist this move. There is a need for close engagement with relevant sectors if this route is to be followed.
- **Dependence on International Technology:** Supply chains raises strategic security issues for government. A hostile state can manipulate technology developed by its companies, enabling them to use it for surveillance or to disrupt key parts of critical infrastructure. However, countries like Russia, North Korea and Iran, not known as significant global tech players, have achieved success without needing to exploit this sort of advantage.

  Telecommunications, energy, health, civil aviation, manufacturing and many other sectors are all likely to have digital products that have some Chinese dimension. Despite the concern with Chinese equipment, is it realistic to ban all technology with a Chinese connection from all parts of our national infrastructure? Most appropriate answer is a 'risk-management approach'.
- **How to Implement the Cyber Security Strategy:** For effective implementation and impact, an organisation is vital. There should be a central authority to implement strategy across different ministries. Roles and responsibilities should be clearly defined and information on the resources are needed to carry out the goals and objectives. It should have metrics and ways of measuring the effectiveness of the programme.[10]
- **Budget for Implementing National Cyber Security Strategy:** Generally nation states do not publish the exact amount of their cyber security expenditure. Cyber security is a cross-sectoral issue, distributed across

several ministries and organisations. This fragmentation as well as different definitions of cyber security make it difficult to evaluate state expenditure in this domain. In UK £1.9 billion was allotted for the Cyber Security Strategy. It was found that a business case for the Strategy or the Programme, was not developed.

The Strategy should allocate dedicated budget and resources for its implementation, maintenance and revision. Resources should be defined in terms of money, people, material, as well as the relationships and partnerships and continued political commitment and leadership required for successful execution. Resources can be allocated by task or objective or by a governmental entity. The government may also consider the establishment of a central budget for cyber security, managed by a central cyber security governance mechanism. Resourcing should not be viewed as a one-time initiative. The overall programme should be managed and tracked by milestones to ensure successful implementation of the Strategy.

Dr. Ajeet Bajpai, Director General of the National Critical Information Infrastructure Protection Centre, on the requirement of a huge budget to successfully implement cyber security at all levels said, even a small country like Israel had allocated US $20 million as the annual budget for cyber security. Considering the size and scale of our nation, we need approximately Rs 25,000 crore budget for the same. The biggest question is where this money will come from?[11]

- **Law Enforcement:** Law enforcement authorities are involved in cyber security issues, as they investigate and fight cyber crime and cyber enabled crime. There are jurisdiction issues between different ministries.
- **Crisis Management:** There are interrelated challenge, viz., building clear structures for crisis communication, maintaining efficient crisis communication and developing adequate capacities for responding to incidents. In the event of a major cyber crisis, the efficient, continuous flow of information between the responsible public and private bodies is extremely important.[12]
- **Deterrence:** The key to a cyber security strategy that moves beyond a defence of individual networks lies with changing the behaviour of hostile states. This requires norms for responsible state behaviour, building cyber crime cooperation and shaping behaviour of adversary through interaction and consequences. Changing the behaviour of our state and non state adversaries will require a serious and sustained effort at national level.
- **Resilience:** There is no 100 percent security. Defences against cyber intrusion and attack are not perfect, they cannot be blocked with confidence, security breaches will take place. We must invest in resiliency. The general aim should be to decentralise potential points of failure, to deploy backup capabilities and plans, to prepare users of systems for the possibility of disruption and to plan contingencies accordingly.
- **Law:** Periodically the criminal law, procedures and policy should be reviewed to ensure the prevention, investigation and prosecution of all forms of cyber crime as the scope of cyber crime is changing very fast. Cyber security laws must also be effectively enforced. An effective anti-cyber crime effort will require the modernisation of law-enforcement agencies, the establishment of dedicated cyber crime units and the training of prosecutors and judges.
- **The Role of Intelligence Agencies:** Due to the sensitive nature of their activities, the role of intelligence agencies is not often explicitly stated in national cyber security strategies. The most effective way to reduce risk of cyber attacks is the creation of consequences for cyber crime, espionage and making these consequences clear to malicious actors. Non state actors, such as terrorist organisations and criminal syndicates have become tech-savvy. Terrorist organisations leverage the benefits of cyberspace, harnessing it for ideology propagation, recruitment, fund raising and communication. Intelligence agencies have a major role to play to thwart these activities.
- **Defence Cyber Strategy.** India does not have an effective National Security Strategy, a National Defence Strategy or a National Military Strategy. Rightly, that has not stopped Headquarters Integrated Defence Staff (IDS) to publish the Joint Doctrine of the Indian Armed Forces. Similarly, the Joint Doctrine on Cyber Operations, or at least Cyber Defence should be published. Reasonable assumptions can be made. Nation states have documented their Cyber Strategies and executed them in the form of Cyber Commands. The military dimension has seen cyberspace witnessing the beginnings of a race for the development and deployment of cyber weapons.
- **National Cyber Strategy:** The Trump Administration released the 'National Cyber Strategy' on 20 September 2018. One key aspect of the National Cyber Strategy is: All tools of national power – diplomatic, law enforcement, economic, cyber and military – can be used to respond to a cyber incident. Offensive cyber operations are an important part of this arsenal.

Around the same time, the 'Defense Department Cyber Strategy 2018' was also published. Some key themes of the Defence Strategy are: using cyberspace to amplify military lethality and effectiveness and defending forward. It states, "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." 'Defend forward' suggests a preemptive instead of a reactive response to cyber attacks. The strategy asserts that the U.S. will be willing to take these actions before or after an armed conflict.

Several nation states have stated the need to develop an offensive cyber capability to effectively 'defend and deter' other actors. Some example are:

- The British National Cyber Security Strategy 2016-2021 states that: "Offensive cyber forms part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere". The UK aims to become "a world leader in offensive cyber capability"; and to establish "a pipeline of skills and expertise to develop and deploy our sovereign offensive cyber capabilities."
- In February 2018, France published its first National Strategy for Cyber Defence clarifying how cyber operations are organisationally integrated as well as the legal framework surrounding their use. In January 2019, France unveiled its first offensive cyber doctrine.
- Netherland's *Defence Cyber Strategy 2018, subtitled Investing in cyber striking power* states that nations should be prepared not only to use military cyberspace forces in peacetime but to actively foster these capabilities as an alternative to armed conflict: "Cyber is no longer a mere enabler of joint operations, but instead a viable strategic option for confronting adversarial societies".
- In its 2012 National Cyber Security Strategy, Spain writes that one "line of action" is to "boost military and intelligence capabilities to deliver a timely, legitimate and proportionate response in cyberspace to threats or aggressions that can affect National Defence".
- In 2011, Turkey revealed plans to establish a Cyber Command, which was officially established a year later called the General Staff Warfare and Cyber Defense Command.

India's national security establishments and the armed forces need to read these documents carefully and take appropriate actions wherever required to improve India's posture in the cyber domain. Generally, offensive cyber operations are not being talked about in the open domain in India. Since the initiative of writing a National Cyber Security Strategy has been taken, it may be a good idea to include India's stance on offensive cyber operations. Publishing a National Cyber Strategy for the Ministry of Defence will be a good beginning.

Appendix

Checklist for National Cyber Security Strategy Development

The checklist for National Cyber Security Strategy development is complementing the Guidelines, by offering a condensed list of aspects to be taken into account during drafting, reviewing and evaluation of a National Cyber Security Strategy.

General Principles and Considerations

- Defining the rationale for developing National Cyber Security Strategies.
- Defining the purpose, aim and objectives of a National Cyber Security Strategy.
- Defining main terms, concepts and their interrelationship.
- Identifying the relation of cyber security to other national strategies, such as the national security strategy.
- Reviewing other relevant national policies, laws, regulations, decision-making processes and other aspects regarding national cyber security.
- Balancing different aspects related to national cyber security such as openness for innovation and requirements for public security; data protection and information sharing; and Internet freedoms and public safety.
- Determining the scope of NCSS by:
  - Identifying governmental, national, international and other actors involved in national cyber security.
  - Weighing different approaches to developing a strategy.
  - Identifying target groups for NCSS.
  - Outlining the subject areas to be addressed.
- Determining the principles for a NCSS.
- Outlining the national position regarding cyber in international affairs and in the context of relevant international organisations.
- Balancing the interests of different stakeholders.
- Portions of Microsoft, Spain, etc., could be taken inspiration from.

Notes

1. From the ITU Global Cybersecurity Index (GCI) 2017.
2. 'Information on the Global Cybersecurity Agenda (GCA)', available at http://www.itu.int/cybersecurity/gca/

3. 'ITU National Cybersecurity/CIIP Self-Assessment Tool, ITU', 2009 available at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

4. 'National Cyber Security Strategy 2020, Call for Comments', available at https://ncss2020.nic.in/

5. 'Differences Between Policy and Strategy', available at http://www.differencebetween.net/business/differences-between-policy-and-strategy/#ixzz6Bn1blxwe

6. Cristin Flynn Goodwin and J Paul Nicholas, 'Developing a National Strategy for Cybersecurity', October 2013, available at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW5Aly

7. Dr Frederick Wamala, 'The ITU National Cybersecurity Strategy Guide', September 2011 available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

8. National Cyber Security Strategy Guidelines, Tallinn 2013, available at https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

9. Gabi Siboni and Ofer Assaf, 'Guidelines for a National Cyber Strategy', Institute for National Security Studies, March 2016, available at http://www.inss.org.il/publication/guidelines-for-a-national-cyber-strategy/

10. Conrad Prince and James Sullivan, Briefing Paper, 'The UK Cyber Strategy Challenges for the Next Phase', Royal United Services Institute for Defence and Security Studies, Whitehall, 2019, Royal United Services Institute for Defence and Security Studies.

11. 'India to Unveil Cybersecurity Strategy Policy in January', Press Trust of India, 29 August 2019, available at https://yourstory.com/2019/08/india-new-cybersecurity-strategy-policy

12. Center for Security Studies (CSS), ETH Zürich, National Cyber Security Strategies in Comparison – Challenges for Switzerland, March 2019, available at https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

The contents of this Issue Brief are based on the analysis of material accessed from open sources and are the personal views of the author. It may not be quoted as representing the views or policy of the Government of India or Integrated headquarters of MoD (Army).

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, Email: landwarfare@gmail.com
Website: www.claws.in
CLAWS Army No. 33098