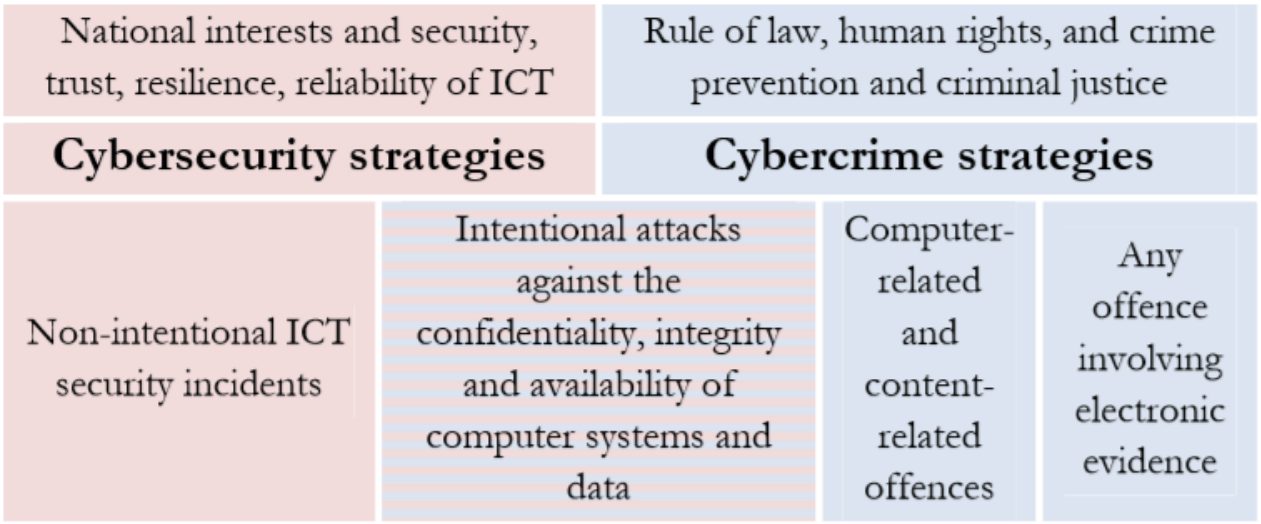
Insights into Editorial: The status of India's National Cyber Security Strategy

insightsonindia.com/2022/04/21/insights-into-editorial-the-status-of-indias-national-cyber-security-strategy/

Insights Editor April 21, 2022



Context:

Amid a surge in cyberattacks on India's networks, the Centre is yet to implement the **National Cyber Security Strategy** which has been in the works since 2020.

What is the National Cyber Security Strategy?

Conceptualised by the **Data Security Council of India (DSCI**), headed by Lt General Rajesh Pant the 22-page report focuses on 21 areas to ensure a safe, secure, trusted, resilient, and vibrant cyberspace for India.

The main sectors of focus of the report are:-

1. **Large scale digitisation of public services:**

Focus on security in the early stages of design in all digitization initiatives, **developing institutional capability** for assessment, evaluation, certification, and rating of the core devices and timely reporting of vulnerabilities and incidents.

2. **Supply chain security:**

Monitoring and mapping of the supply chain of the Integrated circuits (ICT) and electronics products, scaling up product testing and certification, leverage the country's semiconductor design capabilities globally at strategic, tactical and technical level

3. **Critical information infrastructure protection:**

Integrating Supervisory control and data acquisition (SCADA) security with enterprise security, monitoring digitisation of devices, evaluating security devices, maintaining a repository of vulnerabilities, preparing an aggregate level security baseline of the sector and tracking its controls, devising audit parameters for threat preparedness and **developing cyber-insurance products.**

4. **Digital payments:**

Mapping and modeling of devices and platform deployed, supply chain, transacting entities, payment flows, interfaces and data exchange, routine threat modeling exercises to disclose vulnerabilities, threat research and sharing of threat intelligence, timely disclosure of vulnerabilities.

5. **State-level cyber security:**

Developing state-level cybersecurity policies, allocation of dedicated funds, critical scrutiny of digitization plans, guidelines for security architecture, operations, and governance.

6. **Security of small and medium businesses:**

Policy intervention in cybersecurity granting incentives for higher level of cybersecurity preparedness, developing security standards, frameworks, and architectures for the **adoption of Internet of Things (IoT) and industrialization.**

What steps does the report suggest?

To implement cybersecurity in the above-listed focus areas, the report lists the following recommendations:

1.Budgetary provisions:

A minimum allocation of 0.25% of the annual budget, which can be raised up to 1% has been recommended to be set aside for cyber security.

In terms of separate ministries and agencies, 15-20% of the IT/technology expenditure should be earmarked for cybersecurity.

The report also suggests **setting up a Fund of Funds for cybersecurity** and provide Central funding to States to build capabilities in the same field.

While managing security of data, it is recommended to adhere to practices **based on discovery, visibility and risks of critical information.**

2.Research, innovation, skill-building and technology development:

The report suggests **investing in modernization and digitization** of **Integrated Circuits (ICT)**, set up a short and long term agenda for cyber security via outcome-based programs and provide **investments deep-tech cyber security innovation**.

In a bid to attract experts to work on cybersecurity, it is recommended to host hackathons, hands-on workshops, simulations on security on both national and state levels.

3.Crisis management:

For adequate preparation to handle crisis, **DSCI recommends holding cybersecurity drills** which include real-life scenarios with their ramifications.

In critical sectors, simulation exercises for cross-border scenarios must be held on an inter-country basis.

To identify possible weakness and exploitations in systems, DSCI recommend sharing of threat information between government departments.

4.Cyber insurance:

Cyber insurance being a yet to be researched field, must have an actuarial science **to address cybersecurity risks** in business and technology scenarios as well as calculate threat exposures.

DSCI recommends developing cyber insurance products for critical information infrastructure and quantify the risks involving them.

5.Cyber diplomacy:

Cyber diplomacy plays a huge role in shaping India's global relations.

Hence **cyber security preparedness** of key regional blocks like BIMSTEC and SCO must be ensured via programs, exchanges and industrial support.

To further better diplomacy, the government should **promote brand India** as a responsible player in cyber security and also **create 'Cyber envoys'** for the key countries/regions, suggests DSCI.

For a robust internet infrastructure, DSCI suggests **keeping critical infrastructure, root server of programs** controlling and governing India, inside India.

6.Cybercrime investigation:

With the increase in cybercrime across the world, the report recommends **unburdening the judicial system** by creating laws to resolve spamming and fake news.

It also suggests **charting a 5-year roadmap** factoring possible technology transformation, **setting up exclusive courts** to deal with cybercrimes and remove backlog of cybercrimes by increasing centres providing opinion related to digital evidence under **section 79A of IT act.**

Why does India need a cybersecurity strategy?

1. As per American cybersecurity firm **Palo Alto Networks' 2021 report**, **Maharashtra** was the **most targeted state** in India — facing **42% of all ransomware attacks.**
2. The report stated that India is among the more economically profitable regions for hacker groups and hence these hackers ask Indian firms to pay a ransom, usually using cryptocurrencies, in order to regain access to the data.
3. One in four Indian organisations suffered a ransomware attack in 2021 — higher the global average of 21%.
4. Software and services (26%), capital goods (14%) and the public sector (9%) were among the most targeted sectors.
5. **Increase in such attacks** has brought to light the **urgent need for strengthening India's cybersecurity.**

What is the progress in its implementation?

In the recent Budget session of Parliament, several MPs questioned the Ministry of Electronics & Information Technology (MEiTy) on when the Centre plans to introduce the policy.

In response, the Centre clarified that it has formulated **a draft National Cyber Security Strategy 2021** which holistically looks at addressing the issues of security of national cyberspace.

Without mentioning a deadline for its implementation, Centre added that it had no plans as of yet "to coordinate with other countries **to develop a global legal framework on cyber terrorism."**

Conclusion:

A **national framework** should be set in collaboration with institutions like **National Skill Development Corporation (NSDC) and ISEA (Information Security Education and Awareness)** to provide global professional certifications in security.

Moreover, DSCI suggests **advanced forensic training** for agencies to keep up in the age of AI/ML, Blockchain, IoT, Cloud, Automation.

Law enforcement and other agencies should partner with their counterparts abroad to seek information of service providers overseas. The report also suggests **creating a special cadre of Cybercrime investigators.**

DSCI further recommends **creating a 'cyber security services'** with cadres chosen from the Indian Engineering Services.