Women's Indian Chamber of Commerce and Industry

Advocate Shruti Bist
National President, Cybersecurity Council

Smt. Nirmala Sitharaman 20/01/2021

Honorable Finance Minister

Ministry of Finance, Government of India

SUBJECT -SECTOR-SPECIFIC RECOMMENDATIONS TO THE MINISTRY OF FINANCE FOR THE UPCOMING BUDGET 2021

Respected Madam,

I am honored to introduce myself as the National President of the Cyber Security Council at the Women's Indian Chamber of Commerce and Industry. We collaborate for mutual benefit and shared goals with corporates, governments and other authorities to help develop sustainable value and supply chains as well as define an inclusive regulatory framework for the future. With increasing number of cyber crime in India especially on women and children , it is extremely crucial to improve legislations and implementation of cyber laws in India Cyber Laws in India . We look forward to collaborating with the government for better coordination of industry and government and netizens

With due respect and full allegiance, trust and faith on your Government that has been working for betterment of India in all respective direction, I humbly request to you for kindly considering my representation on issue of allocation of budget in various Ministry, departments and private organizations working on cyber laws reforms and security in India.

INTRODUCTION

Cyber-crime remains a persistent and borderless threat that continues to grow in size and scope, and with the pandemic ushering in, it has grown to an even greater extent as almost everything ranging from business and trade to entertainment sector now has a virtual reality, affecting both developing nations and those with higher levels of development. The widespread use of technology and the growing rates of internet connectivity around the globe coupled with the continued development of new technologies that allow for anonymity on the Internet have made cybercrime a low-risk, high-yield venture for a diverse range of state and non-state actors. As per a report by the Data Security Council of India (DSCI), India was the second-most affected country due to targeted cyberattacks between 2016 and 2018. Cyber security has thus become the need of the hour. Given the risks of cyberattacks it faces, India needs a separate budget for cyber security. The separate allocation would enable the country to finance its cyber security initiatives regularly, fostering innovation and to making the country a strong and robust digital economy.

One of the many sectors in which Women's Indian Chamber of Commerce and Industry (WICCI), which is the National Business Chamber to strengthen and encourage Women's participation in business and commerce across all sectors through engagement with government institutions and enabling fundamental changes in the laws and policies, strives to work is towards Cyber Security.

To accomplish this goal, it has established a robust Cyber Security Council at the national level which in collaboration with the various State and regional councils is working towards creating awareness about the growing cyber-crimes, facilitating research and participation in the field of cyber laws and enabling strategic policy changes in the cyber security laws and regulations. In furthering this purpose, the council is involved in conducting seminars/webinars and holding conferences on various emerging topics of cyber law, signing memorandum of understanding with a) national and central universities endeavoring to make the upcoming subjects of cyber laws a part of the curriculum, b) Information & technology ministries and c) cyber law organizations to ensure safety for women and netizens across the country.

IMPLEMENTABLE SUGGESTIONS/RECOMMENDATIONS

A. Establishment of a Task Force to conduct in depth study to identify the concerns which needs to be addressed- by engaging expert panel through NCCS: The Government and businesses need to work closely together in partnership to identify, monitor and manage risks, deal with the vulnerabilities, enforce domestic law, strengthen international law and norm and improve resilience.

This will demand collaboration to anticipate future threats through all source assessment, continuous scanning and early warning and feeding that into regional policy making through periodic risk assessments and reviews. To achieve practical progress to this end, an attempt should be made in the direction of setting up a regional cyber security action task force which will conduct research and study and help identify the cyber security concerns and thereafter provide the required solutions.

B. Solutions to fill the policy and legal gaps- legal and policy interventions:

a) Investing in cybersecurity training and also the rise of cyber education in schools and universities will begin to close the skills gap.

b) Building capability and technical expertise on the analysis of electronic evidence and its admissibility in a court of law.

c) Developing and enforcing domestic legislative cybercrime frameworks that comply with International Law and human rights standards, including necessary amendments to substantive and Criminal Procedure Law, and harmonizing them with applicable global conventions.

d) Developing and ensuring proper usage of investigative and attribution capabilities, including technology and promotion of new operating models with the private sector to ensure timely information sharing for attribution along with enhancing information sharing and cooperation between law enforcement, the private sector, and intelligence entities.

e) Building broad cybercrime expertise in law enforcement personnel and addressing cyber workforce shortages in key cybercrime institutions, keeping pace with technological innovations affecting cybercrime and the modus operandi of cybercriminals. This can be done by building cybercrime awareness and reporting processes among the public.

f) Developing an understanding of the differences between law enforcement's access to powers in different jurisdictions and the potential impact this may have on their ability to cooperate with similar bodies globally.

g) Fostering International cooperation: The cooperation of numerous law enforcement agencies each requiring the capacity and capability to contribute to a multi-agency, transnational investigation is the global cooperation needed to make progress in identifying and bringing to justice cybercriminals.

For instance, in March 2018, Europol, the European Union's agency for law enforcement cooperation, announced the arrest of the suspected leader of a cybercrime ring that targeted over 100 financial institutions in more than 40 countries, resulting in over 1 billion euros in losses. The leader of the group was arrested in Spain after an investigation lasting several years coordinated by Europol's Cybercrime Centre (EC3) and its Joint Cybercrime Action Taskforce (J-CAT). The arrest, conducted by the Spanish National Police, involved the support of the US Federal Bureau of Investigation, law enforcement agencies in Romania, Moldova, Belarus, Taiwan, and a number of private cybersecurity companies.

C. Ways to strengthen legal and institutional framework: Information technology has made the world a global village and has enhanced every sphere and sector of the society like economy, commerce, social and educational sectors. However, despite the advantages, the society is threatened by the growing trend of cybercrime. Information collected by India's Computer Emergency Response Team (CERT-in), 44,679, 49,455 and 50,362 cyber security incidents took place in India during the years 2014, 2015 and 2016, respectively. These incidents include phishing, website intrusions and defacements, virus and denial of service attacks amongst others.

As per the '2016 Cost of Data Breach Study: India' the average total cost of a data breach paid by Indian companies increased by 9.5 percent, while the per capita cost increased by 8.7 percent and the average size of a breach grew by 8.1 percent. Arguably, cyber-crime thrives because of lack of universal legal framework and jurisdictional challenges that make it difficult to bring cyber criminals to book. Some of the ways to strengthen the legal framework:

a) Lack of awareness of the cyber laws among the general public and the practical reality that most people are ignorant of the laws of cyberspace is a major issue. Educating the people about their rights and obligations in cyberspace and legal remedies in cyberspace law.

b) Our law enforcement officials lack proper training in cyber laws. Adequate training to law enforcement officials must be imparted to equip them with legal knowledge and required technical knowledge to enforce cyber laws, including the Judiciary and the Police officials to combat the Cybercrimes and to effectively enforce cyber laws. Because of the speed at which communications technologies and computers evolve, even experts must receive regular and frequent training in the investigation and prosecution of high-tech cases. At the judiciary level, the lawyers, judges and judicial officers both of civil court and criminal courts may also be involved in discussions on Cyber law and at the National Judicial Academy specialized workshops on cyber laws could be organized to develop better understanding of the law and to bring about speedy delivery of justice.

c) The reporting and access points in the police department require immediate attention. In domestic territory, every local police station should have a cybercrime cell that can effectively investigate cybercrime cases. Accessibility is one of the greatest impediments in delivery of speedy justice. Only 4 cybercrime crime cells in Metropolitan cities and a handful of police officers is highly inadequate in light of growing cyber-crimes in India.

d) Anonymity on the internet poses serious issues in tracking cybercriminals as tracing an IP can be complicated due to use of proxy servers and other spoofing tools. A major challenge in enforcement of cyber laws is posed by the fact that there are no territorial boundaries in the Cyberspace. It is recommended that adequate manpower and resources are dedicated to developing & promoting technologically sound applications to trace IPs and imparting forensic science education.

e) Lack of adequate legal provisions to maintain internet usage files and records makes combating cybercrimes a complex task. There is a need to enact stricter laws on maintaining logs and Registers for internet usage. Further under Section 79 of the IT Act, 2000, no guidelines exist for ISPs to mandatorily store and preserve logs for a reasonable period to assist in tracing IP addresses in Cybercrime cases. Adequate legal mechanisms will need to be developed to tackle these intricate issues.

f) Electronic data is sensitive and can be easily tampered or destroyed. Providing cyber forensic science education to law enforcement personnel will assist in protecting sensitive e-evidence admissible in court of law. Law enforcement officials must be cognizant of how to gather, preserve, and authenticate electronic evidence in an authentic manner that will be completely admissible in a court of law.

g) Law enforcement agencies often find it difficult to keep abreast of the dynamic technical knowhow & tools. Effective Public Private Partnership is recommended to circumvent this problem. Police and prosecution authorities often lack the technological experience and capacity to investigate and prosecute efficiently in a complex data-processing environment.

Therefore, criminal justice systems depend on the private sector – the civil society and the economy, in particular the information and communication technology industry and service providers of all kinds — for an efficient investigation and prosecution of cybercrimes. Without active participation of the private sector, it is hardly possible, for example, to detect the whole spectrum of child pornography in the internet and trace it to its distributors and, in the end producers.

h) Institutionalizing the contact points for reporting cybercrimes that affect National sovereignty and public good and safeguard. Critical Information Infrastructure absent or weak in the country. Computer Emergency Response team to be strengthened financially technically and by infrastructure to aptly serve as national agency for incident response. Establishing statutorily recognised accreditation agencies, creating certification policies, Office of Controller of Certifying authority, and other security measures will be indispensable in securing the online environment.

i) Heterogeneous laws and no one universal cyber law. Unification of Cyber Law through multilateral treaties and other international initiatives.

D. Development of training infrastructure of various government bodies and agencies who are responsible for implementation of laws: Our law enforcement officials lack proper training in cyber laws. Adequate training to law enforcement officials must be imparted to equip them with legal knowledge and required technical knowledge to enforce cyber laws.

There is an imperative need to impart the required legal and technical training to our law enforcement officials, including the Judiciary and the Police officials to combat the Cybercrimes and to effectively enforce cyber laws.

Because of the speed at which communications technologies and computers evolve, even experts must receive regular and frequent training in the investigation and prosecution of high-tech cases. In addition to domestic training, countries should participate in coordinated training with other countries, so transnational cases can be pursued quickly and seamlessly. Trained and well-equipped law enforcement personnel – at local, state, and global levels can ensure proper collection of evidence, proper investigation, mutual cooperation and prosecution of cyber cases. For instance, as part of its growing number of activities to tackle cybercrime, UNODC recently hosted a one-week training workshop for law enforcement officers on live data forensics, a subject area which looks at ways in which data can be seized from a suspect's computer while it is still running, thus avoiding the need to seize the computer and take it to a laboratory for analysis.

E. Modernization and up gradation of the technology used for cyber forensics: Law enforcement officials across India lack fundamental communication and transport infrastructure. 267 police stations had no telephones and 129 had no wireless communication devices as of January 2017, as per the latest available data from the Bureau of Police Research and Development. There were eight vehicles for every 100 police personnel for responding to distress calls, patrolling and maintaining law and order in their jurisdictions.

The number of police stations functioning without wireless communication devices across India increased by 231% from 39 in 2012 to 129 by the end of 2016. At the beginning of 2017, 273 police stations across the country did not possess a single transportation vehicle.

While security companies continue to develop tools to keep users safe, cybercriminals have adopted new technologies and attack methods to evade identification and perpetrate their crimes with relative ease.

As human dependence on technology intensifies, cyber laws in India and across the globe need constant up-gradation and refinements. Modernization includes the up gradation of weapons, communication systems including wireless devices and satellite networks and the developments of forensics infrastructure including labs and training of manpower. The pandemic has also pushed much of the workforce into a remote working module increasing the need for app security. Lawmakers have to go the extra mile to stay ahead of the impostors, in order to block them at their advent. Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users. Only the prudent efforts of these stakeholders, ensuring their confinement to the law of the cyber land - can bring about online safety and resilience.

F. Awareness programmes and events to facilitate knowledge sharing: The procedure in which knowledge (documented and undocumented) is transferred to others in an informative way that can be easily used is called knowledge sharing. In an organization, sharing knowledge not only increases productivity, but also empowers its employees to do their jobs effectively and efficiently.

Employees can work faster and smarter by getting easy access to insights, resources and expertise. There is a dire need in companies to mainstream the new items and services and keep updated about knowledge sharing to survive their businesses as according to a report from the Society for Human Resource Management, Fortune 500 companies lose just under $32 billion a year, simply by failing to share knowledge. So, to facilitate the culture of knowledge sharing, there has to be sufficient awareness about the same. Appropriate awareness programmes and events in which employees are provided explanations and comprehensive training by the right experts need to be taken up by the organizations.

G. Technical Courses on prevention, control and detection of cyber-crimes through development of courses: There is a pressing need to introduce advanced and technical levels of courses in the cyber law discipline which is quickly expanding its horizon. Not only is the discipline needs to be mainstreamed and be made a part of the mandatory curriculum of the universities, but also certain certificate and seminar courses need to be introduced to provide with some practical exposure as with just being taught the theoretical aspects of a law is doing no good in preparing and tackling one for the practical aspects of the crime. Knowledge of cyber laws would be a value addition, irrespective of one's professional qualifications and would certainly help the learner to move up on the knowledge value chain. The information technology act that is being taught, should be combined with the analysis of the criminal and civil liabilities to understand the framework along with the comparative analysis with other countries and judicial decisions on issues related to cyber law to understand the effectiveness of law. Learning about cyber laws is an opportunity to be in sync with the present-day world.

Many believe that cyberspace simply cannot be regulated and is beyond the government's reach. The anonymity and multi -jurisdictional city of cyberspace makes control by government in cyberspace impossible. This belief about cyberspace is wrong.

CONCLUSION

The impact of increasing globalization, greater connectivity via the internet and increasing access to internet via world wide web suggests that states should look at multilateral security cooperation with fresh eyes. With the states becoming increasingly vulnerable through their greater connectivity and dependence on cyberspace, it becomes imperative that governments, industry and individuals take action to mitigate these risks. The Government needs to have in place mature arrangements that ensure clarity of roles and responsibilities across their agencies in optimizing cyber security so that they can prioritize and allocate resources to mitigate the various cyber threats, generating sufficient political leadership to prioritize the cybercrime threat and invest sufficient resources in law enforcement and diplomacy to address it.

We strongly believe that India has to allocate separate funds for protection and preservation of its cyber sovereignty. This is so as India’s cyber sovereignty is constantly on the attack. Various challenges are likely to try affecting India’s cyber-sovereignty in the form of potential breaches of cybersecurity.

It becomes absolutely imperative to appreciate that there is an urgent need for allocation of specific direct funds, which can help fund programmes for protection and preservation of India's cyber sovereignty.

The areas which particularly need Fund allocation in the cyber security domain are:

a) Building an effective legal framework to handle cyber security cases: At present, there isn't any specific legislation in India that provides protection against cybercrimes. The Information Technology Rules, 2011, need to be revisited as the scale and the modus operandi of cybercrimes have evolved and will continue to do so.

b) Capacity building in the domain of cyber security: There is a dearth of adequately skilled cyber security professionals in India. This shortage, which is felt at both the government and the industry level, can affect India's fight against cybercrimes. The government should encourage research and education related to cyber security skills in the upcoming Budget.

c) Protecting critical infrastructure with deep monitoring and response capabilities: Critical Information Infrastructure (CII) involves assets, systems, or parts thereof, that are deemed to be critical for the normal functioning of a country. As new technologies like the Internet of things (IoT) are integrated into our national critical infrastructure, new cyber security threats emerge, which are required to be handled by specific security solutions.

d) Building and strengthening cyber defense and deterrence: State-sponsored cyber-attacks are growing by the day and becoming a covert method of warfare, allowing countries to deny accusations and blame citizens.

For the sake of sustainability and reliability in the digital age, the government needs to make India cyber-resilient by encouraging indigenous cybersecurity products and research and development (R&D).

e) Strengthening the weakest links by bringing sectoral agencies and regulators under one roof: Another important area that demands urgent attention is the necessity of a national-level agency for protection from cybercrimes. While India has several sector-specific regulators and agencies focusing on their respective areas, there is clearly a need for a central authority at the national level, given that cybercrimes have evolved to penetrate various sectors and regulatory regimes.

f) Public Awareness: The government should launch result-oriented cyber awareness campaigns to provide individuals one-to-one assistance and cyber security support. The awareness drives can include the formation of guidelines and provide people with government-recognized security applications, which can be installed to secure devices. There must be comprehensive drives to spread awareness about cybercrimes and how they can be prevented. Furthermore, the government could also consider making cyber security a part of school curriculums, so that students are aware of cyber threats and precautions they should take when using the internet and mobile phones.

g) Volunteering and Project Funding: The government should allocate funds towards volunteering and projects involved in the cyber law promotion. Also funds are needed by the various departments & private organizations working towards cyber law security and awareness.

Therefore, the Council request that the government needs to allocate reasonable funds to strengthen the country's cyber security framework and these funds need to be holistically distributed to strengthen the legal and policy framework. India can look at countries like the US, the UK, Germany and Australia and learn from the steps they have taken to ramp up their cyber security capabilities to address today's challenges.