GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *47
TO BE ANSWERED ON: 26.7.2024

NEED FOR A NEW NATIONAL CYBERSECURITY POLICY

***47. SHRI S NIRANJAN REDDY:**

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether Government has recognized the need for a new National Cybersecurity Policy/Strategy due to emerging technologies and evolving threats;
(b) the steps being taken to formulate and implement a new National Cybersecurity Policy/Strategy addressing current and future cybersecurity challenges, including Artificial Intelligence (AI) and other critical technologies;
(c) whether Government has considered revising such policies periodically to keep pace with the fast-evolving nature of technology; and
(d) the timeline for introducing and implementing a new National Cybersecurity Policy/Strategy, and the key areas it will focus on to ensure a secure digital environment in the country?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI JITIN PRASADA)

(a) to (d): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN THE REPLY TO RAJYA SABHA STARRED QUESTION NO. *47 FOR 26.7.2024, REGARDING NEED FOR A NEW NATIONAL CYBERSECURITY POLICY

(a) to (d): Yes, the Government is committed to ensure that the Internet in India is Open, Safe, Trusted and Accountable for its users, specially in view of the role of emerging technologies and evolving threats. Government has taken several legal, technical, and administrative policy measures for addressing cyber security challenges in the country. The Government has also institutionalised a nationwide integrated and coordinated system to deal with cyber-attacks in the country which, inter alia, includes:

i. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) to ensure coordination amongst different agencies.
ii. Under the provisions of section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents.
iii. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.
iv. Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.
v. Ministry of Home Affairs (MHA) has created Indian Cybercrime Coordination Centre (I4C) to deal with cybercrimes in a coordinated and effective manner.
vi. Under the provisions of section 70A of the Information Technology (IT) Act, 2000, the Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.

MeitY addresses key concerns in cybersecurity including those related to emerging and critical technologies, particularly in the field of AI, through a continuous process of research, analysis, formulation and issue of necessary instructions and guidelines based on emerging needs and challenges. The primary focus is on the three pillars of Securing national cyberspace, Strengthening existing structures comprising of people, processes and capabilities and Synergise resources for their optimal utilization to protect the Digital Environment in the country and to ensure secure and resilient cyberspace for all citizens.

****

भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
राज्य सभा
तारांकित प्रश्न संख्या *47
जिसका उत्तर 26 जुलाई, 2024 को दिया जाना है।
4 श्रावण, 1946 (शक)

नई राष्ट्रीय साइबर सुरक्षा नीति की आवश्यकता

***47. श्री एस. निरंजन रेड्डी:**

क्या **इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री** यह बताने की कृपा करेंगे कि:

(क) क्या सरकार ने उभरती प्रौद्योगिकियों और बढ़ते खतरों को देखते हुए किसी नई राष्ट्रीय साइबर सुरक्षा नीति/रणनीति की आवश्यकता महसूस की है;

(ख) कृत्रिम बुद्धिमत्ता (एआई) और अन्य महत्वपूर्ण प्रौद्योगिकियों सहित वर्तमान और भविष्य की साइबर सुरक्षा चुनौतियों का सामना करने के लिए एक नई राष्ट्रीय साइबर सुरक्षा नीति/रणनीति तैयार करने और उसे लागू करने के लिए क्या कदम उठाए जा रहे हैं;

(ग) क्या सरकार ने तेजी से विकसित हो रही प्रौद्योगिकी के साथ तालमेल रखने के लिए समय-समय पर ऐसी नीतियों को संशोधित करने पर विचार किया है; और

(घ) एक नई राष्ट्रीय साइबर सुरक्षा नीति/रणनीति आरंभ करने और लागू करने के लिए समय-सीमा क्या है, और देश में एक सुरक्षित डिजिटल वातावरण सुनिश्चित करने के लिए इस नीति में किन प्रमुख क्षेत्रों पर ध्यान केंद्रित किया जाएगा?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय में राज्य मंत्री (श्री जितिन प्रसाद) :

(क) से (घ) : एक विवरण-पत्र सभा पटल पर रख दिया गया है।

*****

नई राष्ट्रीय साइबर सुरक्षा नीति की आवश्यकता के संबंध में दिनांक 26.07.2024 को राज्य सभा में पूछे गए तारांकित प्रश्न सं. *47 के उत्तर में उल्लिखित विवरण-पत्र

*****

(क) से (घ) : जी, हां । सरकार यह सुनिश्चित करने के लिए प्रतिबद्ध है कि भारत में इंटरनेट विशेष रूप से उभरती हुई प्रौद्योगिकियों और बढ़ते हुए खतरों की भूमिका को देखते हुए अपने उपयोगकर्ताओं के लिए खुला, सुरक्षित, विश्वसनीय और जवाबदेह है । सरकार ने देश में साइबर सुरक्षा चुनौतियों से निपटने के लिए कई कानूनी, तकनीकी और प्रशासनिक नीतिगत उपाय किए हैं। सरकार ने देश में साइबर हमलों से निपटने के लिए एक राष्ट्रव्यापी एकीकृत और समन्वित प्रणाली भी स्थापित की है, जिसमें अन्य बातों के साथ-साथ निम्नलिखित शामिल हैं:

i. विभिन्न एजेंसियों के बीच समन्वय सुनिश्चित करने के लिए राष्ट्रीय सुरक्षा परिषद सचिवालय (एनएससीएस) के तहत राष्ट्रीय साइबर सुरक्षा समन्वयक (एनसीएससी) ।

ii. सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख के प्रावधानों के तहत भारतीय कंप्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) को साइबर सुरक्षा घटनाओं का जवाब देने के लिए राष्ट्रीय एजेंसी के रूप में पदनामित किया गया है।

iii. सर्ट-इन द्वारा कार्यान्वित राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) देश में साइबरस्पेस को स्कैन करने और साइबर सुरक्षा खतरों का पता लगाने के लिए नियंत्रण कक्ष के रूप में कार्य करता है। एनसीसीसी साइबर सुरक्षा खतरों को कम करने के लिए कार्रवाई करने हेतु साइबर स्पेस से मेटाडेटा साझा करके विभिन्न एजेंसियों के बीच समन्वय की सुविधा प्रदान करता है।

iv. साइबर स्वच्छता केंद्र (सीएसके) सर्ट-इन द्वारा प्रदान की जाने वाली नागरिक-केंद्रित सेवा है, जो स्वच्छ भारत के दृष्टिकोण का साइबर स्पेस तक विस्तार करती है। साइबर स्वच्छता केंद्र बॉटनेट क्लीनिंग और मैलवेयर विश्लेषण केंद्र है और दुर्भावनापूर्ण प्रोग्रामों का पता लगाने में मदद करता है और उन्हें हटाने के लिए मुफ्त उपकरण प्रदान करता है, और नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियां और सर्वोत्तम पद्धतियां भी प्रदान करता है।

v. गृह मंत्रालय (एमएचए) ने समन्वित और प्रभावी तरीके से साइबर अपराधों से निपटने के लिए भारतीय साइबर अपराध समन्वय केंद्र (I4सी) बनाया है।

vi. सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 70क के प्रावधानों के तहत सरकार ने देश में महत्वपूर्ण सूचना अवसंरचना की सुरक्षा के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) की स्थापना की है।

एमईआईटीवाई साइबर सुरक्षा में उभरती हुई और महत्वपूर्ण प्रौद्योगिकियों, विशेष रूप से एआई के क्षेत्र में प्रमुख कठिनाइयों को अनुसंधान, विश्लेषण, निर्माण और उभरती हुई जरूरतों और चुनौतियों के आधार पर आवश्यक अनुदेशों और दिशा-निर्देशों को जारी करने की निरंतर प्रक्रिया के माध्यम से संबोधित करता है। प्राथमिक ध्यान राष्ट्रीय साइबर स्पेस को सुरक्षित करने, लोगों, प्रक्रियाओं और क्षमताओं से युक्त मौजूदा संरचनाओं को सुदृढ़ करने और देश में डिजिटल परिवेश की सुरक्षा के लिए उनके अनुकूलतम उपयोग के लिए संसाधनों को समन्वित करने और सभी नागरिकों के लिए सुरक्षित और लचीला साइबर स्पेस सुनिश्चित करने के तीन स्तंभों पर केंद्रित है।

*****

MR. CHAIRMAN: First Supplementary; Shri S Niranjan Reddy.

SHRI S NIRANJAN REDDY: Sir, my question to the Minister is that due to the ever increasing threat of cyber security-related issues, does the Ministry propose to have the National Cyber Security Co-ordinator (NCSC), NCCC and I4C closely co-ordinate with industry leading private sector stakeholders and strengthening the cyber security environment?

SHRI JITIN PRASADA: Sir, the Member has asked a very pertinent question and cyber security is a great concern and, especially, a top priority for this Government. I can assure, through you, to all the Members and, especially, the one who is asking that there is a complete co-ordination. As far as cyber security is concerned, the Government of India, with three Departments, the Ministry of Home Affairs, the NSA and the Ministry of IT & Electronics and this co-ordination have a series of measures, apart from the policy that is in place, that in the past ten years, the Government has come up with various initiatives to ensure that we are well-equipped as far as our cyber security is concerned. We have taken enough steps to protect the data for citizens and we are also, since it is a global challenge, completely aware of that and are in complete co-ordination with all our friendly countries. But, this cyber security is an issue which concern all of us and the nature of it is such that it is anonymous and it also transcends boundaries. We have taken steps with regard to having the main body that deals with cyber security, the CERT and under which we have this National Cyber Coordination Centre which has a budget outlay of Rs. 770 crores, which primarily tracks traffic and sees that wherever there is a threat perception, we go in for preventive measures and also, if there is an attack, post-that, how to course correct, all those measures are in place. Hence, all institutions that the Member has mentioned, they are working in complete co-ordination and I assure you that we are well-equipped to handle the situation.

MR. CHAIRMAN: Second Supplementary; Shri S Niranjan Reddy.

SHRI S NIRANJAN REDDY: Sir, my question to the Minister is that in relation to the victims of cyber security-related frauds or other issues, does the Government have any mitigation plan where it will compensate the victims by some kind of an umbrella trust arrangement that can be worked out because most of the times, the victims are poor people. So, I just wanted to ask the Minister that if there is a plan that is being thought of. Thank you, Sir.

SHRI JITIN PRASADA: Sir, the policy, like I said, is in place. But, the strategy is evolving. It is because this is such a sector that new issues keep coming up. As far as the protection of our citizens is concerned, it is a top priority and most of the times, in complete co-ordination with the Home Ministry and other institutions, we have been successful in ensuring that, especially, with regard to financial fraud that has been stopped and I can inform the House that a saving of around Rs. 2,400 crores because of cyber criminals have been there*...(Interruptions)...* and 7.6 lakh citizens.... *...(Interruptions)...*

MR. CHAIRMAN: No interruptions. *...(Interruptions)...* No; this is bad practice. Please. *...(Interruptions)...* No. *...(Interruptions)...*

SHRI JITIN PRASADA: Mr. Chairman, Sir,... *...(Interruptions)...*

MR. CHAIRMAN: Let the Minister reply. *...(Interruptions)...* Please. *...(Interruptions)...* Take your seat please. *...(Interruptions)...*

SHRI JITIN PRASADA: I would request, through you, that this is a very important question and issue and it concerns not only everybody in the House but also citizens across and it is an evolving process. I request everybody to understand the issue. This Government is committed to protect our citizens and we are working on various platforms as to how to stop the crime and ensure post-benefits to them.

MR. CHAIRMAN: Third Supplementary; Shri Raghav Chadha.

SHRI RAGHAV CHADHA: Sir, I along with several Members of this House, particularly, who sit on the Opposition Benches were victims of something called as the State-sponsored spyware attack whereby our mobile phones notified us that a State-sponsored cyber attack took place which was attempting to infiltrate our mobile phone devices. *...(Interruptions)...*

MR. CHAIRMAN: Your supplementary, Mr. Raghav.

SHRI RAGHAV CHADHA: Now, Members of not just this House, several people including journalists and eminent persons in public life are also victims.

MR. CHAIRMAN: Your supplementary, Mr. Raghav.

SHRI RAGHAV CHADHA: Therefore, I ask through you, Sir, to the hon. Minister whether the Government has taken cognizance of such attacks. Is there a list of the people who were attacked by such spyware attacks and, thirdly, what action has been taken? This is the second time I am raising this question in this House, Sir.

SHRI JITIN PRASADA: Sir, as far as what the Member has raised with regard to the issue of State-sponsored, I can categorically state that there is no such thing as State-sponsored hacking or tracking. What I am going to tell you is, as far as what the Member has mentioned...*(Interruptions)*...

MR. CHAIRMAN: Please listen. ...*(Interruptions)*... Priyanka*ji*, please. Please listen to the Minister...*(Interruptions)*...

SHRI JITIN PRASADA: Sir, I have not yet completed... ...*(Interruptions)*...

MR. CHAIRMAN: Randeep Surjewala*ji*, ...*(Interruptions)*... This is a very bad practice, Randeep*ji*. Do not rise. ...*(Interruptions)*... Listen to him. Yes, hon. Minister.

SHRI JITIN PRASADA: Sir, I have not yet completed, they are jumping the gun. ...*(Interruptions)*... As far as what this Member has said...

MR. CHAIRMAN: Hon. Minister, the point is, the Members would want a Half-an-Hour Discussion. If a request will come, we will do it. Go ahead, but hear him patiently.

SHRI JITIN PRASADA: Sir, there is no requirement for that. I am clarifying the issue. With due respect, those issues which were raised regarding Apple, our Computer Emergency Response Team, CERT India, this organisation is in touch with the Apple and we are in the process of getting information from Apple as where and how they have come to this conclusion. If they can share with us the data or the situation where they have got that information from, our agencies will act on that. Thank you.

MR. CHAIRMAN: Fourth supplementary; Shri Kunwar Ratanjeet Pratap Narayan Singh.

श्री कुँवर रतनजीत प्रताप नारायण सिंह: सभापति महोदय, धन्यवाद। माननीय मंत्री जी ने हमें बहुत विस्तृत जानकारी दी है कि साइबर क्राइम के लिए सरकार ने क्या कदम उठाए हैं। मैं आपके माध्यम से माननीय मंत्री जी से जानना चाहूंगा कि तमाम लोग आज भी आम आदमी और पढ़े-लिखे लोग भी बैंक डेटा से पैसे निकालते हैं। हाल ही में एक 80 साल की महिला के पूरे जीवन की जमा पूंजी, करीब 3 करोड़ रुपये का एक तरह का डिजिटल अरेस्ट हुआ है।

MR. CHAIRMAN: Ask your supplementary question.

श्री कुँवर रतनजीत प्रताप नारायण सिंहः इसी तरह तमाम लोग, गरीब आदमी, गाँव के लोग, जहां से मैं आता हूं वहां से लेकर पूरे देश में इस तरह से बैंक के खातों पर अटैक होता है।

MR. CHAIRMAN: Please ask your supplementary question.

श्री कुँवर रतनजीत प्रताप नारायण सिंहः इसके लिए सरकार, इनका मंत्रालय और गृह मंत्रालय कौन से ठोस कदम उठा रहे हैं?

श्री जितिन प्रसाद: माननीय सभापति महोदय, मैं आपके माध्यम से माननीय सदस्य को अवगत कराना चाहता हूं, क्योंकि उन्होंने बहुत ही महत्वपूर्ण विषय पर बहुत ही महत्वपूर्ण प्रश्न पूछा है, क्योंकि हमने देखा है कि हमारे बहुत से नागरिक जो इतनी जानकारी नहीं रखते हैं, वे बहुत से साइबर फ्रॉड और साइबर क्राइम के झांसे में आ जाते हैं और जिस वजह से बहुत लोगों को नुकसान हुआ है, उन्हें आर्थिक क्षति हुई है। मैं माननीय सदस्य को और इस सदन को आश्वस्त करना चाहता हूं कि सरकार के संज्ञान में यह विषय है। जैसा कि मैंने कहा है कि यह बड़ी evolving situation है। हमारा मंत्रालय, इलेक्ट्रॉनिक्स और आईटी की विभिन्न संस्थाएं और गृह मंत्रालय का Indian Cyber Crime Coordination Centre (I4C) जो नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल है, उसके आधीन ये शिकायतें दर्ज कराई जाती हैं। इसके अलावा एक हैल्पलाइन नम्बर 1930 भी जारी किया गया है। जितने तरीके के क्रेडिट कार्ड, डेबिट कार्ड, डिजिटल पेमेंट्स, यूपीआई प्लेटफॉर्म आदि तमाम जगह, जहां साइबर क्राइम हो रहे हैं, उन्हें रोकने के लिए इसके अधीन कार्य किया जा रहा है। हमारी जो CERT-in है, वह पूरी तरीके से इक्विप्ड है और प्रयास करते हैं कि अधिकतर ऐसे क्राइम्स को रोक दिया जाए। मैं माननीय सदस्य को आश्वस्त करता हूं कि आगे भी ऐसे क्राइम्स पूर्ण रूप से रोके जाएंगे।

MR. CHAIRMAN: Fifth supplementary question; Shri Jose K. Mani.

SHRI JOSE K. MANI: Sir, in my recent question, the Ministry of Home Affairs stated that the Narcotics Control Bureau has registered 92 cases related to the use of dark net in drug trafficking. What specific action is the Government taking to monitor and

to combat illegal activities on the dark net, such as the sale of illicit drugs, weapons and counterfeit currencies so far to ensure the dark net does not undermine national security efforts? How is the Government ensuring that cyber security agencies are equipped with the necessary tools and training to effectively investigate and dismantle dark net operations?

SHRI JITIN PRASADA: Sir, as I said earlier, there is complete coordination between three Departments, the Home Affairs, the NSA and the Electronics and IT Department. This question of the hon. Member pertains to the Home Ministry and I can assure him that I can get the full details with regard to the issue that he has raised from the Home Ministry and get back to him.

MR. CHAIRMAN: Now, Question No. 48.