Volume 6, Issue 7, July 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Indian Perimeter Cyber Security: Cyber Security Policy and Implementation

Donthula Ravi Kumar*
University of Hyderabad,
Telangana, India

Abstract— Many nations are trying to protect their cyber space by applying cyber security policy and implementing diverse protection strategies and advanced technologies. This is very much required to India because of extreme dependence and usage of Internet and ICTs in Organizations, Critical sectors, economic and financial institutions, and in e-government functionalities. The boundary less cyber space also connected national Critical Infrastructures (CIs) and Critical Information Infrastructures (CIIs) for easy control, data transfer and central management activities. Now anti-national elements and inimical nations are using cyber as the media to harm other nations by penetrating into other country networks, sniffing sensitive data, social-media misuse, planting bots, espionage into defense systems, damaging or taking control of critical infrastructures etc. So the enemies don't need to do war against a nation to cripple down its CI/CIIs. They can easily do it through cyber route which is un-guarded. This paper provides national cyber perimeter security framework for controlling cyber-attacks and emerging cyber threats which are targeted at national cyber space.

Keywords— Critical information infrastructure protection, cyber security policy and implementation, cyber space, National cyber command and control, National cyber security.

I. INTRODUCTION

Cyber threats and cyber-attacks have increased tremendously world over at a fast pace. No country is completely safe from cyber threats and sophisticated cyber-attacks. Cyber space has become an easy and attractive target for terrorists. Terrorists are hiring hackers or learning hacking skills to target the nations. Foreign states are also using sophisticated capabilities to launch cyber-attacks against CI/CIIs to impair the security of the nation. Some are using cyber-attacks for "hacktivism" (Anonymous), destabilization (e.g. Estonia in 2007 using DOS and DDOS attacks), cyber-espionage (NSA), sabotage (e.g. in Iran using Stuxnet), political motivation and even military operations etc. [1]. For detecting and deter such kind of attacks the critical sectors should have multi layered cyber security mechanisms. The nation should have suitable security strategy to protect its CI/CIIs during cyber security emergencies. It has to understand the interdependencies and priority of CI/CIIs to protect at critical time.

The attacking patterns and the practice of cyber-attacks have been changing from time to time. As a result nations are trying to protect their cyber space by applying cyber laws, cyber policies and cyber security strategies. Some countries are even setting up cyber commands [2] and some are developing cyber military capabilities [3] to safeguard or threaten other countries.

In India many of the Internet Service Providers (ISPs) are under private control. For the government to control the cyber space through ISPs is very problematic and time consuming in emergency or critical situations. The implementation of control by the ISPs is also not similar due to non-technical feasibility or lack of skilled cyber experts [4]. So the government itself has to control and command the national cyber space as per the national cyber security policy.

India had initiated the National e-Governance Plan (NeGP) to make all government services available to the citizens of India via electronic media [5]. India has been facing many cyber threats and security challenges that are not easy to tackle. On the way to secure national cyber space India has drafted National Cyber Security Policy in the year 2013 [6]. Still there is a dire need to protect Indian CI/CIIs and cyber space from sophisticated cyber-attacks [7]. The problem is that most of the CI/CIIs are under private control so that public and private partnership and co-operation is required. In addition to this the government has to have a national level cyber-control and command mechanism to handle any cyber threat of any nature at any time in the digital cyber battle field.

II. INDIA AND ITS CYBER SECURITY POLICY

Insecurity in cyber space means economic insecurity. No Nation can afford economic insecurity. According to a report from Symantec, India ranked second among nations that were most targeted for cyber crimes through the social media in 2014, after the US [8]. There has been ever increasing threat of cyber terrorism over India [9].

So far India has not faced severe cyber-attacks like what happened in Estonia in 2007. India has faced most of the cyber-attacks originated from hostile nations. India's Government websites of defense, ministries and diplomatic

missions were hacked [10]. So India is among the nations that are most targeted for cyber-attacks. So India needs to act strategically and dynamically to detect, prevent, and stop cyber-attacks.

Due to nonexistence of globally acceptable international cyber security treaty, policy and policing [11], cyber threats are increasing day by day and endangering the e-sovereignty of the nation. The government of India introduced IT act 2000 [12] and framed cyber security policy in the year 2013 for protecting the national cyber space and CI/CIIs, and to avoid cyber misutilization.

It is not enough just to have a cyber security policy but also it is essential to have a cyber security framework, which will address all the related cyber problems over a long period of time [13]. The cyber security policy and framework should be in such a way that it should protect CI/CIIs, reduce vulnerabilities, block cyber-attacks and threats before impacting and ensure that disruptions to national cyber space are infrequent, of minimal duration, manageable, and cause the least public damage [14].

A major component of national cyber security policy is a nation's ability to detect, deter, investigate, and prosecute cyber-criminal activities. Weaknesses in any of these areas can compromise the cyber security of the nation [14].

To be secure, resilient and self-reliant in cyber security, India has to control its perimeter of cyber access, to control the threats from outer cyber world. The perimeter is the place where the nation's cyber infrastructure is connected to the International Internet Bandwidth. As part of the national cyber security strategy, the upstream and downstream cyber data of the nation has to be checked for harmful content at the national cyber boundary itself. This acts like a first layer of control to the national cyber. At the national cyber perimeter, it is very important to see that the national sensitive data should not be transmitted to other country through e-mail, or other file transfer mechanisms. It is also important to see that other countries should not use cyber media for defacing national web sites, violation of communal harmony, anti-social and anti-economic activities etc.

The government should also mandate that all national ISPs should be connected to the national firewall before connecting to the International Internet cloud. So that the government can effectively monitor and control the national cyber traffic and can handle the threats initiated from other nations. It also helps to combat logic bombs and cyber wars in future.

III. DESIGN

India at present has manageable number of International Internet Gateways and its quantity might increase in future. The national cyber boundary is the point at which the national Internet upstream and downstream traffic connected to the International Internet Bandwidth. This is the ideal place where the government can monitor and control the in/out Internet traffic and can check for cyber-attacks and cyber threats. Here multi layered and multi-functional boundary defenses like national firewalls, proxies, Network Intrusion Detection Systems, Intrusion Prevention Systems can be applied by using advanced technologies and processes.

Fig. 1 shows the establishing of Perimeter Cyber Control (PCC) Boxes for controlling the Internet traffic at the national cyber boundaries.

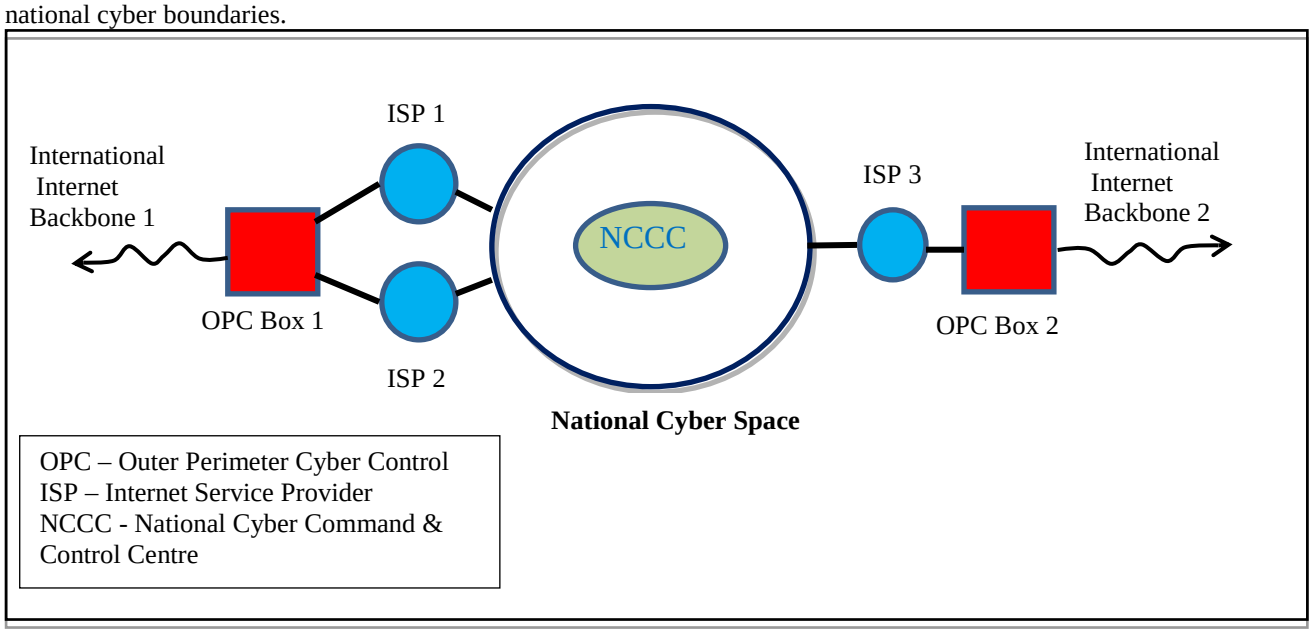

Fig. 1. National Perimeter Cyber Security through PCC Boxes

The PCC Boxes should be placed just before connecting to the International Internet Gateway. If more than one ISP is connected to same International Internet Gateway then single PCC Box is required to connect all these ISPs. It is also possible that a single PCC Box can be connected to more than one International Internet Gateways. If there is a provision, the PCC Box can be placed at the national submarine cable Landing Station itself. So that all national Internet upstream and downstream traffic travels through these PCC Boxes only; and these boxes act as the national cyber perimeter firewalls. A PCC Box includes many devices that can do the following activities:-

a) Switching features
b) Routing features
c) Firewall features (deep packet inspection and blacklisting IP-addresses etc.)
d) IDS and IPS features and
e) Network traffic Splitting and Merging features

All these PCC Boxes are connected to the centralized control and command station known as NCCC (National Cyber Command & Control Centre) where cyber experts monitor and control PCC Boxes. Highly secure, redundant, dedicated, and high speed data connection will be used between NCCC and the PCC Boxes. So the centralized control and command will be passed to all PCC Boxes at the same time, and the same control and cyber policy implementation will be possible.

The main features of the PCC Boxes are as follows:-

a) Controls Upstream and Downstream traffic as per the access rules applied.
b) Particular type of service like VOIP, Video calling etc., file types, and sizes can be blocked or continued nationally as per the NCCC directions. It is also possible to allow certain services only in critical situations. So that critical services can function in critical time also.
c) Obscene or objectionable web pages or web sites hosted in other countries can be blocked as per the national interest.
   It also cross checks that the government sensitive data cannot be passed or stored in private servers of other countries, as DIT (Department of Information Technology) instructed to all departments to host their websites only on servers located within India and as per CERT-IN guidelines Indian Government Websites must use .gov.in or .nic.in as domain names [15]. This is important because in the event of information leaked or hacked of server hosted abroad, there are difficulties in investigating the case, as Indian laws are difficult to be applied on those agencies [16].
d) In case of Indian government sensitive websites are accessed from other countries then the PCC Boxes monitor the sessions and secure those websites from hacking or other vulnerable activities.
e) As per the government regulations the ISPs should not allow national domestic traffic to be routed to International Internet gateways [17]. The PCC Boxes also restrict that the requests to government web sites (e.g. gov.in, org.in) should not pass to the International Internet gateways.
f) PCC Boxes scan whole cyber traffic passing through it, so the identified critical cyber vulnerabilities can be blocked at the national cyber perimeter itself. These boxes can also execute functions like IP blocking, deep packet filtering, URL filtering, VPN/SSH traffic recognition, VPN blocking etc.
g) The National CI/CIIs can be safe guarded from other nations by having a close watch on the connections established. National CI/CIIs and sensitive government organizations can be monitored effectively for DOS, DDOS cyber-attacks by assigning separate IP address ranges and deciding the depth of scrutiny.
h) Before actual war begins, the enemy country first attempts to cripple the CI/CIIs of the nation. At that time these PCC Boxes play a key role in protecting the national cyber space.
i) If in the worst case, International cyber space is facing problems then these PCC Boxes help to isolate the outer cyber space from the national cyber space. So that the national cyber can function without disruption and the national cyber space can be protected easily.
j) PCC Boxes help to apply policy as per the national interest and apply it similarly, instead of depending on ISP operators to apply. Some ISPs may not implement the policy due to lack of infrastructure or skilled man power.
k) At present, to implement cyber policy or block some IP addresses, the government has to share sensitive data with all ISPs. This process is insecure and if the data is leaked it may create annoyance to the government. NCCC avoids sharing of sensitive data with the ISPs.
l) Private domain implementation: - National private domains are the domains which are created and used within the nation only and these are not accessible from other nations. To implement private domains the domain names should be in the format as abc.private.in or abc.gov.private.in and the nation should have its own Domain Name System (DNS) Server. National Internet Exchange of India (NIXI) and Department of Telecommunications (DOT) have to play a major role in implementing the private domain system. PCC Boxes helps to block others to access these national private domains.
m) It provides the facility to satisfy the requirements of law and enforcement agencies as the total entry and exit of International Internet traffic flows through the PCC Boxes.
n) Botnet activities can be effectively controlled with the help of other research departments.
o) It also helps to study new cyber vulnerabilities and attack patterns.

IV. IMPLEMENTATION

In India many government departments are participating in protecting the national cyber space and CI/CIIs. Some are working for framing cyber policies, some are for domain control, some are for passing commands to the service providers and some are doing research on cyber threats and vulnerabilities. So there is a need to collaborate above departments to effectively monitor and control the national cyber space. Figure 2 shows the framework of NCCCs command and control center, and co-ordination with other departments.

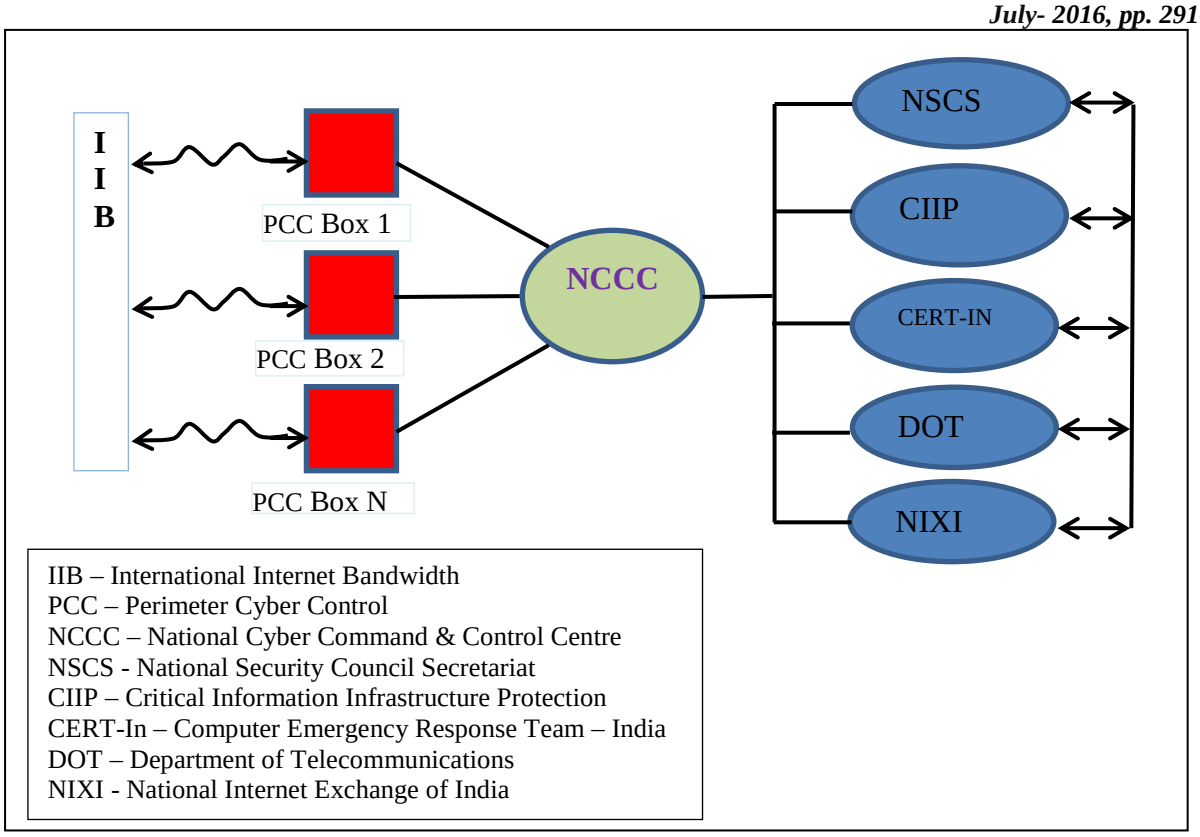

Fig. 2. National Perimeter Cyber Command and Control framework

A. National Cyber Command and Control Center (NCCC)

It consists of a "NCCC committee" and a team of executive "NCCC cyber experts". The NCCC committee will have members from NSCS, CIIP, CERT-IN, NIXI, and from DOT. The head of the "NCCC cyber experts" is also a member of the NCCC committee. The committee members will take decisions on what control policies to be implemented at the PCC Boxes, so that the National e-sovereignty, national cyber interests and the National CI/CIIs can be protected. This committee recommends adding, removing, modifying or reviewing the control policies at PCC Boxes.

The "NCCC cyber experts" team does the actual execution of placing control policies at PCC Boxes as recommended by the NCCC committee. They also monitor the performance of the PCC Boxes round-the-clock. This team also does tactical and strategic analysis of national level cyber threats, attacks and vulnerabilities to understand the potential consequences. It also associates with other research teams of India in assessing the potential cyber threats and vulnerabilities.

B. National Security Council Secretariat (NSCS)

NSCS [18] is the apex agency looking into the political, economic, energy and strategic security concerns of India and acts as the secretariat to the NIB (National Information Board).

C. Critical Information and Infrastructure Protection (CIIP)

India started focusing on protection of CI/CIIs to avoid cyber-attacks, cyber hazards, and general breakdown of critical services. It conducts research and risk assessment based on the analysis of vulnerabilities and the threats to the CI/CII, in order to protect economies and societies against the impacts of highest national concern. CIIP also establishes trusted public-private partnerships with a focus on risk management, incident response and minimizes damage and recovery time from cyber-attacks that do occur. CIIP would interact with other incident response organizations including CERTs, enabling such organizations to leverage the analytical capabilities for providing advanced information of potential threats.

D. Computer Emergency Response Team-India (CERT-IN)

CERT-In [19] monitors Indian cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among public and private cyber users and organizations in the country. It maintains 24x7 operations center and has working relations/collaborations and contacts with CERTs, all over the world; and Sectorial CERTs, public, private, academia, Internet Service Providers and vendors of Information Technology products in the country. Its stated mission is "to enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration".

E. Department of Telecommunications (DoT)

DoT [20] under the Ministry of Communications and Information Technology, Government of India, is responsible to coordinate with all ISPs and service providers with respect to cyber security incidents and response actions as deemed

necessary by CERT-In and other government agencies. DoT will provide guidelines regarding roles and responsibilities of Private Service Providers and ensure that these Service Providers are able to provide uninterrupted network services and have arrangements of alternate routing in case of physical attacks on these networks.

F. National Internet Exchange of India (NIXI)

NIXI [21] has been set up by DIT to ensure that Internet traffic, originating and destined for India is routed within India.

For effectively protecting the national cyber space and CI/CIIs multi-layer and multi levels of cyber security is required. The main important layer of security is the national perimeter cyber security, where the national Internet traffic exchanges with the International Internet Gateways. CERT-IN, NIXI, DIT, CIIP and NSCS acts as another layer of security as blocking objectionable content, domain control, cyber policies and laws creation and execution, cyber control, and cyber security research etc.

V. CONCLUSIONS

India is one of the biggest cyber user and its social and economic development is dependent on cyber applications like e-governing, e-banking, e-services, e-libraries, e-medical, e-education, e-trading, e-surveillance and "digital India" etc. Any damage or destruction on Indian cyber space or CI/CIIs can cause damage to the economic and social well-being of the nation. Every CI/CII has to protect its cyber perimeter by applying security controls as per its operational requirement and internal security policies. Each CI/CII should also follow the advisories of the CERT-IN and sectorial CERT-INs. In the same way each nation has to protect its national cyber security by detecting its cyber perimeter, developing defense-in-depth multiple layers of protection strategies and applying various levels of security controls and polices. All dynamic strategies applied at PCC Boxes should handle increased cyber risks, i.e. increased cyber threats, vulnerabilities and potential impact on the economy and the society of the nation. The PCC Boxes should also minimize damage & recovery time in case cyber-attacks do occur.

The suggested perimeter security help the nation to have full control on upstream and downstream of international Internet traffic and acts as the first defensive method. It can be tuned to implement national cyber security policies and can also be used for further research on new vulnerability trends etc.

The government should recognize cyber security as a growing challenge and has to play a leading role in building capacities at the larger level to handle national cyber traffic. In future India increasingly depends on cyberspace for its competitive advantage, public safety, and national defense. It has to streamline upstream and downstream cyber traffic to pass through the PCC boxes right from the beginning, so that it can easily handle cyber problems in future also.

International Cooperation: Cyber security is the global problem, so each country has to share cyber intelligence, research results, expertise, assistance and technology with other countries. They also have to participate in international laws, treaties and conventions which will help in securing the national cyber security. Every nation should have one NCCC center to protect its national cyber space, and the world should have one Inter-National Cyber Command and Control (INCCC) center for coordinating among all national NCCCs and for handling global cyber threats and related issues.

REFERENCES

[1] Detecon Deutsche Telekom Group, "Review report: e-commerce, cybercrime and cyber security –status, gaps and the road ahead", Final Version, pp. 260-262, 26 November, 2013.
[2] Bruce Schneier, "Pentagon staffs up U.S. cyber command", The Washington Post, February 1, 2013.
[3] Saudi Press Agency, "Army cyber command looks to build new HQ", Military.com, Dec 26, 2015.
[4] Tech2, "Government asks Internet service providers to block over 800 porn sites", 03 Aug 2015, [Online]. Available: http://tech.firstpost.com/news-analysis/government-asks-internet-service-providers-to-block-over-800-porn-sites-276368.html
[5] India.gov.in, national portal of India, https://india.gov.in/e-governance/national-e-governance-plan
[6] Ministry of Communication and Information Technology, Department of Electronics and Information Technology. (July, 2013). "National cyber security policy-2013", [Online]. Available: http://deity.gov.in/content/national-cyber-security-policy-2013-1
[7] National Computrade News, "Cyber Security: Major challenges in IT landscape", Dec 10th, 2014.
[8] Business Standard, "India ranked 2nd in cyber-attacks through social media in 2014", April 23, 2015.
[9] Firstpost, "72% of Indian companies faced cyber-attacks in 2015: KPMG", Nov 30, 2015.
[10] Syed Nazakat, New Delhi, "Why is India prone to cyber threat", the week, August 2012.
[11] Geeta dalal, "Indo US Cyber Security Relationship Needs Improvements", International ICT Policies and Strategies, April 26, 2012, [Online]. Available: http://ictps.blogspot.in/2012_04_01_archive.html
[12] Ministry of Law, Justice and Company Affairs (Legislative Department), New Delhi, "The Information Technology Act, 2000" Part II, Section 1, 2000, [Online]. Available: http://www.dot.gov.in/act-rules/information-technology-act-2000
[13] Neha Alawadhi, "Cyber security policy must be practical: Experts", the economic times, Oct 22, 2014.
[14] World federation of Scientists, Permanent monitoring panel on information security "Toward a universal order of cyberspace: Managing threats from cybercrime to cyber war, Report & recommendations", World summit on the information society, Geneva, pp. 45 & 51, 2003.

[15] National Informatics Centre, Department of Information Technology, GOI, "Guidelines for Indian government websites", January 2009, [Online]. Available: http://darpg.gov.in/documents/rulesmanuals/ Guidelines_for_Government_websites.pdf

[16] Conflict of laws in cyberspace, Internet and computer era, "Advisory by Maharashtra government to use official E-Mails, Indian cloud based services, Routing traffic through NIXI and section 43 A compliance check", Monthly Archives: November 2013.

[17] Telecom Regulatory Authority of India, "Recommendations on improvement in the effectiveness of national Internet exchange of India (NIXI)", April 20, 2007.

[18] Vivek Gurung, "The national cyber security policy-2013 of India", Cyber Kendra, Latest hacking news and tech news, Jul, 2013.

[19] Indian Computer Emergency Response Team, Department of Electronics & Information Technology, Ministry of Communications & Information Technology, http://www.cert-in.org.in

[20] Department of Telecommunications (DoT), Ministry of Communications & Information Technology, http://www.dot.gov.in

[21] National Internet Exchange of India (NIXI), http://nixi.in

