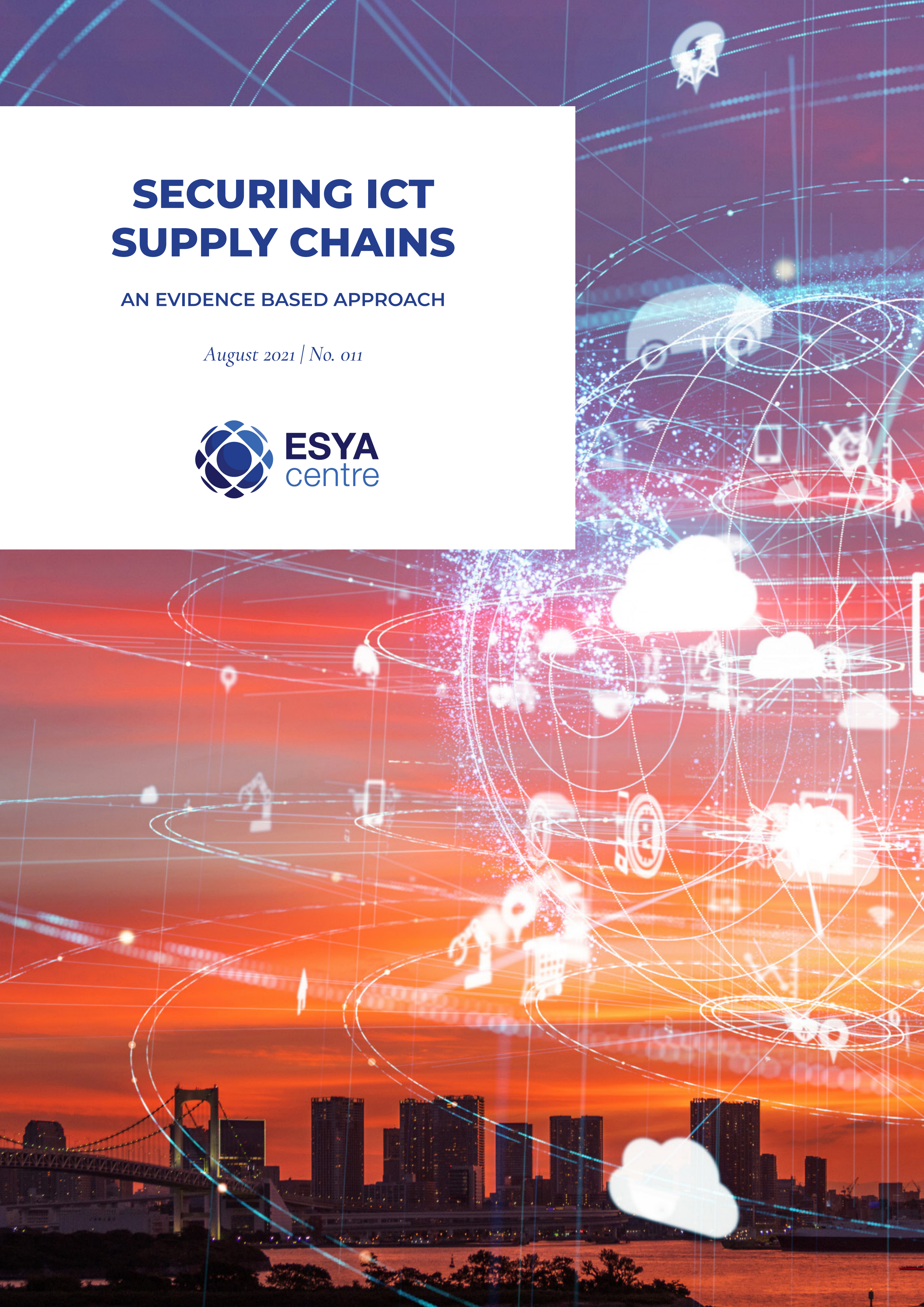
SECURING ICT SUPPLY CHAINS

AN EVIDENCE BASED APPROACH

August 2021 | No. 011

ESYA centre



ABOUT THE AUTHOR

Mohit Chawdhry is Junior Fellow at the Esya Centre.

ABOUT THE ESYA CENTRE

The Esya Centre is a New Delhi based technology policy think tank. The Centre's mission is to generate empirical research and inform thought leadership to catalyse new policy constructs for the future. It aims to build institutional capacities for generating ideas that will connect the triad of people, innovation, and value to help reimagine the public policy discourse in India. More details can be found at www.esyacentre.org.

Layout and design by Khalid Jaleel.

CONTENTS

INTRODUCTION 4

THE U.S. APPROACH TO SECURING ICT SUPPLY 5

1. Inter-agency consultation and coordination 5
2. Risk assessment 5
3. Due process and accountability 6
4. Public-private cooperation 6

SECURING ICT SUPPLY CHAINS IN INDIA 8

1. Inter-agency Consultation and Coordination 8
2. Risk assessment 9
3. Transparency and due process 10
4. Public-private cooperation 10

CONCLUSION 12

ENDNOTES 13

INTRODUCTION

Information and communication technologies are integral to the functioning of governments, businesses, and individuals. Contemporary ICT products and services include a range of software, hardware and other components produced and assembled by third parties transnationally. As a result, ICT supply chains (the systems of organisations, people, technology, and labour required to move a product from supplier to consumer) have become increasingly distributed and complex. This complexity carries greater security concerns, with the risks difficult to quantify or remedy.[1]

The repeated exploitation of ICT supply chain vulnerabilities (through hardware breaches, ransomware, and denial of service attacks) results in significant costs. Attacks last year on vulnerabilities in SolarWind's Orion software affected multiple departments of the US Government, including the Treasury and Commerce.[2] Studies suggest that such incidents will be more frequent in the coming decade.[3] With the growing frequency and impact of such attacks, securing ICT supply chains has become a key national security concern.

In 2013 an expert report of the UN Group of Governments identified critical risks to "secure and reliable ICT use and the ICT supply chain for products and services".[4] More recently, a series of actions by governments worldwide show the centrality of security concerns to regulating ICT supply chains. States have set up specialised agencies to deal with cybersecurity threats, particularly threats to the ICT supply chain. In 2016, the United Kingdom established a National Cyber Security Centre to improve its resilience and response mechanisms.[5] Similarly, in 2018 the United States set up CISA, the Cybersecurity and Infrastructure Security Agency to deal with threats to its ICT supply chains.[6]

Another example of security-oriented supply chain regulation is the exclusion of Chinese vendors such as Huawei and ZTE from 5G trials by various states, stemming from fears that they are part of a Chinese Military-Civilian fusion, and the components they supply may include backdoor vulnerabilities to compromise the cybersecurity of domestic organisations and citizens.[7]

Governments have also intervened in the ICT supply chain to ensure that domestic citizens' data is not collected, processed or shared by companies for malicious use. Both India and the United States banned certain Chinese apps from operating in their territory due to concerns that the data they collect would be shared with the Chinese government. In the US the ban was imposed in three executive orders issued by then-President Donald Trump, targeting eight Chinese apps. The orders were stayed by a US Court.[8] The Government of India has banned over 250 apps through orders issued under Section 69A of the Information Technology Act (IT Act) 2000.[9]

Implementing supply chain measures to improve national security may, however, impact the integrated nature of global ICT supply chains. Nations such as China have sought to secure their supply chains by favouring indigenous innovation, often at the cost of foreign investment. This threatens to splinter or balkanise existing supply chains. Moreover, ad-hoc and discretionary actions such as app bans hinder trust and certainty in the business environment, a crucial factor in ICT trade and investment.[10] States will need to adopt an approach that can balance the imperative of national security with business and investment concerns.

Indeed, some governments have sought to strike this balance, by adopting an evidence-based approach grounded in the principles of transparency, flexibility, and accountability.

An example of an evidence-based approach to securing ICT supply chains is the executive order (E.O.14034/2021) issued by US President Joe Biden, which revoked the ban on Chinese apps for its ad-hoc and discretionary nature. The order takes a balanced approach, establishing a system to determine the security risks posed by data collection activities of software apps owned or controlled by foreign adversaries, transparently and based on evidence.[11]

The order marks a reversion to an earlier system of continuously evaluating the threats to ICT supply chains, instituted by E.O.13873/2019 under Trump.[12] It further mandates an annual review of threats to supply chains in critical sectors and subsectors of the ICT industrial base.[13]

Taken together, the orders establish a predictable and deterministic approach to securing ICT supply chains without obstructing innovation or the consumer interest.

This brief analyses these executive orders, and the rules issued to implement them, identifying means to provide certainty, predictability, transparency, and accountability to the process of securing ICT supply chains. It concludes with an assessment of the extent to which the Indian cybersecurity framework currently incorporates these means.

THE U.S. APPROACH TO SECURING ICT SUPPLY

E.O.s 14017 and 14034 reflect the American commitment to securing its global supply chains, particularly in ICT. Unlike the orders banning TikTok, WeChat and other Chinese applications ad hoc, these reflect a measured and rules-based response to security concerns. They address the security concerns posed by ICTs, but in consonance with constitutional principles of due process. This helps engender trust, crucial to sustaining the global ICT value chains that are responsible for significant investment and innovation.[14] A study of the US approach may prove useful to policymakers and regulators seeking to introduce measures to help secure their ICT supply chains in a transparent manner reliant on evidence. This section provides a brief overview of four such characteristics.

A STUDY OF THE US APPROACH MAY PROVE USEFUL TO POLICYMAKERS AND REGULATORS SEEKING TO INTRODUCE MEASURES TO HELP SECURE THEIR ICT SUPPLY CHAINS IN A TRANSPARENT MANNER RELIANT ON EVIDENCE.

1. Inter-agency consultation and coordination

Identifying transactions that involve foreign adversaries and pose a security threat to the US is the prerogative of the Secretary of Commerce. In identifying such transactions, the Secretary of Commerce is required to consult the heads of various other departments, including the Trade Representative, Homeland Security, and the Treasury. Rules under E.O.13873 require the Secretary of Commerce to hold two rounds of consultation with a group of Secretaries: first in identifying transactions of concern, and again in recommending measures to address the concerns posed by any transaction.[15] Similarly, E.O.14017 requires the Secretaries of Commerce and Homeland Security to consult other functionaries in preparing their reports on vulnerabilities in ICT supply.[16]

This inter-agency approach accommodates diverse and differing considerations, such as those of finance and trade, while protecting national security. Inter-agency consultations at the decision-making stage may also lead to better enforcement of the measures adopted, which are finalised only after considering the capacities of each agency organisation.

2. Risk assessment

Credible and predictable policymaking requires an underlying base of information and evidence to guide it. The E.O.s require Government departments and agencies to issue periodic reports on various aspects of supply chain security, including threat assessments and vulnerability mapping (Table 1).

These reports are continuously updated and reviewed to help the Government determine which nations, corporations or transactions pose a threat to the cybersecurity of the United States. Security measures such as app bans or investment restrictions, when grounded in reports and assessments, give an intelligible character to agency determinations, reducing the scope for arbitrariness and discretion. The certainty this fosters will enable better decision-making in investment and trade.[17]

The rules under E.O.13873 also list the criteria and sources of information the Secretary of Commerce may rely on to determine the risks posed by an ICT transaction. This provides much needed clarity to businesses and investors, on the grounds on which an ICT transaction may be prohibited, letting them take preemptive measures to avoid a prohibition.

No.	Name / Scope of the Report	E.O. Numbers	Designated Fuctionary
1	Assessment of threats to the US and its people from ICTs developed, owned or controlled by foreign adversaries	13873	Director of National Intelligence
2	Assessment of entities, hardware, software and services that present vulnerabilities and pose consequence to US national security	13873	Secretary of Homeland Security
3	Sectoral Supply Chain Assessment of the ICT Industrial Base	14017	Secretary of Commerce and Secretary of Homeland Security
4	Report on recommendations to protect against harm from the access, sale or transfer of US citizens' data by software applications owned, controlled or developed by a foreign adversary	14034	Secretary of Commerce in consultation with heads of other sectoral agencies

Table 1: Responsibility for assessments of ICT supply chain security in the United States

3. Due process and accountability

Government actions that deny someone their life, liberty or property must meet the requirements of procedural due process. Those against whom such actions are contemplated must be given notice and be allowed to present their case.[18] The rules issued under E.O.13873 ensure procedural due process by requiring that the parties to an ICT transaction deemed to pose a security risk are notified upon initial determination. The parties are given 30 days to respond to the initial determination. The notice includes suggesting measures to help mitigate the security concerns raised in the initial determination.[19] Thus the E.O.s facilitate dialogue and conciliation between the Government and parties involved in ICT transactions, to arrive at measures that protect national security while minimising the impact on the functioning of ICT supply chains.

Publishing all orders and decisions is another element of procedural due process. Publication lets parties to the determination as well as others understand the rationale used by authorities to arrive at a certain decision. It helps ensure that decisions are based on relevant and bonafide considerations, as opposed to arbitrary and extraneous ones.[20] The ban on 8 Chinese apps was ostensibly based on extraneous considerations, as it did not demonstrate how a ban would help address the security concerns posed by the Chinese State. As a result, operation of the ban was stayed by a US Court.[21]

The E.O.s require publication of the Committee's final determination of each transaction in the Federal Register, in an unclassified manner, with no confidential information revealed. The determination order must explain the rationale behind the decision to prohibit or permit each transaction, and must also state the mitigation measures agreed to by the parties.[22] Businesses can refer to earlier published orders to help determine whether their ICT transactions are likely to provoke any national security concerns, and how these may be mitigated.

4. Public-private cooperation

As private corporations often provide critical information infrastructure, they are vulnerable to cyberattacks. The recent ransomware attack on the Colonial Pipeline highlights how cyberattacks on private entities can have considerable consequence for national security and the economy.[23] It is important therefore for governments to coordinate with the private sector in securing ICT supply chains.

The robust framework created by E.O.13636/2013 for public-private cooperation was bolstered by subsequent law, including the Cybersecurity Information Sharing Act of 2015.[24] The E.O. fosters cooperation in cybersecurity related information sharing, and the adoption of standards, measures and industry best-practices pertaining to cybersecurity.

THE E.O. FOSTERS COOPERATION IN CYBERSECURITY RELATED INFORMATION SHARING, AND THE ADOPTION OF STANDARDS, MEASURES AND INDUSTRY BEST-PRACTICES PERTAINING TO CYBERSECURITY.

On information sharing, the E.O. charges the Attorney-General, the Secretary of Homeland Security and the Director of National Intelligence with devising a strategy to disseminate unclassified cybersecurity information, in a rapid and timely manner, to the owners and operators of critical infrastructure. Such information sharing is required to incorporate privacy and civil liberty protections.[25]

The E.O. tasks the National Institute of Standards and Technology (NIST) with creating a baseline framework for reducing cyber risks to critical infrastructure. This includes identifying a set of standards and industry best practices to provide a flexible, repeatable and performance-based approach to cyber risk management.

The Cyber Infrastructure & Security Agency engages with subject experts, infrastructure owners and other key stakeholders through the Task Force on ICT Supply Chain Risk Management (SCRM). The Task Force works for cooperation in SCRM efforts such as bidirectional data sharing, criteria-based threat evaluation, and identifying trusted vendors and resellers.[26]

SECURING ICT SUPPLY CHAINS IN INDIA

For a decade and a half, creating a robust cybersecurity framework has been a key priority for the Indian Government. The IT Act and concomitant rules provide the statutory framework for India's cybersecurity architecture. The Act defines key terms like "critical infrastructure", and establishes agencies such as Cert-In, the nodal body for cyber incident response in India.[27] Reducing supply chain risks through standardisation, testing and awareness-building is also a key component of the National Cyber Security Policy 2013, which identifies the protection of critical information infrastructure (CII) as a priority.[28]

The National Critical Information Infrastructure Protection Centre (NCIIPC) established under the National Technical Research Organisation governed by the Prime Minister's Office is the central body for protecting CII.[29] Recently, Ministries have also set up dedicated wings or divisions to deal with emerging technologies and associated concerns. This includes the Ministry of External Affairs, whose New Emerging & Strategic Technologies division engages in technology diplomacy, and the foreign policy aspects of new technologies.[30]

Besides the institutional framework, there have been direct and targeted actions to reduce risks in the supply chain. Examples include the ban on 200 Chinese apps, and the restrictions imposed on FDI from nations sharing a land border with India, primarily China and Pakistan.[31]

ICT SUPPLY CHAIN REGULATION MUST FOSTER TRUST BY ADHERING TO ESTABLISHED PRINCIPLES OF TRANSPARENCY AND ACCOUNTABILITY.

ICT supply chain regulation must foster trust by adhering to established principles of transparency and accountability. The Prime Minister echoed this stance in his address to the G7, where he stressed that cyberspace should be used to protect and enhance democratic values.[32] The following paragraphs consider the extent to which India's approach to securing ICT supply chains measures up to these principles.

1. Inter-agency Consultation and Coordination

The Government has established a number of institutions and agencies to monitor cyber threats, collect intelligence, and undertake actions to improve cybersecurity (Table 2). Their work is complemented by Chief Information Security Officers in all Ministries and Departments, with CISOs in the Ministries of External Affairs, Home Affairs, and the Department of Telecom being particularly important.[33]

This framework is unsupported by mechanisms to facilitate cooperation and resolve overlap. A centralised framework of cooperation would promote coherence and collective enforcement actions.[34] The absence of such coordination mechanisms is consistently flagged as a key shortcoming of India's intelligence framework. For instance, the report of the Kargil Review Committee observed that "There is no institutionalized mechanism for coordination or objective-oriented interaction between agencies."[35] The Standing Committee on IT in its 52nd Report made similar observations, recommending the adoption of a central coordination mechanism to improve India's response to cyber threats.[36]

While the Government subsequently tasked the National Cyber Security Coordinator under the National Security Council Secretariat in the Prime Minister's Office with inter-agency cooperation, no rules or an action plan to facilitate such cooperation are yet in place.[37] Besides coordination at the Central level, there is a need to coordinate the actions of Central and State agencies, given the increased procurement and use of public-facing digital tools by State Governments.

The revised National Cyber Security Policy, expected to be released this year, must address these gaps in the coordination framework.

No.	Ministry	Agencies	Year of Formation
1.	Ministry of Home Affairs	NATGRID (National Intelligence Grid)	2008
		NCCC (National Cyber Co-ordination Centre)	2014
		DRDO NETRA (Network Traffic Analysis)	2014
2.	Ministry of Electronics and Information Technology	CERT-In (Computer Emergency Response Team)	2004
		CSK (Cyber Swacchata Kendra)	~2016
		TERM (Telecom Enforcement Resource and Monitoring)	2008
3.	Prime Minister's Office	NSC (National Security Council)	1998
		RAW (Research and Analysis Wing)	1968
		CCS (Cabinet Committee on Security)	n/a
		NTRO (National Technical Research Organisation)	2004
		NCIIPC (National Critical Information Infrastructure Protection Centre)	2014

Table 2: An overview of agencies mandated to deal with cybersecurity issues in India.

2. Risk assessment

The complexity of modern ICT supply chains poses a challenge to risk assessment. As ICT components are usually sourced from numerous countries, it is difficult to gauge the risk of possible backdoors or other malicious elements being present.[38] Faced with such complexity, some states chose to adopt simplistic policies from easily identifiable criteria. An example is India's ban on apps developed by Chinese companies. While the Chinese military-civil fusion does raise concerns about the safety of Indian citizens' data, it remains unclear whether all the 250-plus apps posed a similar threat level to national security and required the same treatment.[39]

Adopting a simplistic, targeted approach may not lead to improved national security. Such actions may address the concerns posed by the most significant adversaries, there is always a chance that residual risks escape the required level of scrutiny. A targeted approach also fails to consider that even domestically created and maintained ICT products can be tainted and require rigorous risk assessment.[40]

It is important to adopt a systematic approach that can continuously assess and identify threats to the ICT supply chain. This would involve identifying key assets, threat-modelling to assess supply chain risks, and a clear incident response procedure.[41] Not only would a risk-assessment framework improve security outcomes, it would also provide an evidentiary basis for Government actions, and help foster trust, certainty and confidence among enterprises and citizens.

The National Security Directive on Telecommunications signals the Government's intent to create a systematic risk assessment framework for crucial technologies. It establishes a National Security Committee on Telecommunication, responsible for evidence-based assessment and certification of telecom equipment manufacturers.[42] The Government must extend this approach, with a systematic and periodic risk assessment of larger vulnerabilities in the ICT supply chain, akin to the US procedure. It would include identifying countries, companies and applications that pose significant risk to India's strategic information infrastructure and to citizens' privacy. CERT-In or the National Cyber Coordination Centre could create these risk assessment reports, by collating information received from other agencies involved in cybersecurity.

3. Transparency and due process

It can be questioned whether India's cybersecurity framework and the measures adopted to secure the supply chain adhere to established principles of due process and transparency. Consider the Government's use of Section 69A of the IT Act to block access to content on national security grounds. 69A empowers the Central Government to block access to public information "in the interest of the sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States, public order, or for preventing incitement to the commission of any cognizable offence relating to the above". An RTI request filed by the Software Freedom Law Centre found the Government had used this provision to block over 14,000 websites in the period 2010–2018.[43]

While the Supreme Court upheld the constitutionality of 69A in the *Shreya Singhal* judgment, it observed that the reasons for a blocking order must be recorded in writing, and the originator and intermediary given the opportunity to be heard.[44] In practice, however, the blocking orders issued under 69A are kept confidential, as permitted by Rule 16 of the IT (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Blocking Rules). And no information is made available on the names of blocked websites or the reasons for blocking access to content.

There is also little evidence that the opportunity of a fair hearing is given to the originator or intermediary. Reports suggest that there is not a single recorded instance of a hearing being held prior to the issuance of blocking orders.[45] The opaque and discretionary manner in which blocking orders are issued by the Government has resulted in a fresh challenge to the constitutionality of 69A and the IT Blocking Rules.

Broadly, the Indian cybersecurity framework prioritises security considerations over the democratic rights of citizens. Government decisions to block or intercept content under the IT Act are not subject to review by the Judiciary or Parliament. This gives the Executive unrestrained power to intercept or block information, directly impacting the constitutionally recognised rights to privacy and free expression.[46]

BROADLY, THE INDIAN CYBERSECURITY FRAMEWORK PRIORITISES SECURITY CONSIDERATIONS OVER THE DEMOCRATIC RIGHTS OF CITIZENS.

A similar approach is evident in the Government's encryption policies. Rules under the Indian Telegraph Act require telecom service providers to use only 40-bit encryption in order to facilitate easy interception and access by the Government for national security or other purposes.[47] Similarly, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 require significant social media intermediaries to trace the originator of a message in India when asked to by the Government. There are fears that this will require communication applications such as Signal to abandon end-to-end encryption and provide backdoors for Government access.[48]

By prescribing weakened encryption standards, Government actions place the privacy of communication between citizens at risk. Strong encryption standards are crucial moreover to the digital economy, as many confidential and sensitive business and strategic transactions are conducted digitally.

Policymakers must look to recalibrate the cybersecurity framework in a manner that ensures the protection of civil liberties and democratic values. In particular, there is a need to assess whether the existing provisions for blocking, interception and encryption are in consonance with the various tests laid down by the Supreme Court to determine the legality of executive actions that infringe on fundamental rights, such as the rights to free speech and privacy.[49]

4. Public-private cooperation

Both CERT-In and the NCIIPC are required to interface with the private sector to enhance ecosystem resilience by facilitating the sharing of crucial and relevant information. The CERT-In Rules require it to assume a proactive role in enhancing resilience, by issuing advisories, vulnerability notes, and periodic guidelines and whitepapers.[50] Yet these publications are often outdated and unspecific to India.[51] Similarly, the NCIIPC interfaces with private business through partnerships meant to provide CII owners with information on potential threats and mitigation measures. But the absence of a transparent procedural framework clarifying how the data shared by companies will be used reduces the incentive for private companies to share relevant data with the Government.[52]

The Standardisation Testing and Quality Certification Directorate (under MeitY) and the Telecom Engineering Centre are the Government bodies largely responsible for standard-setting, testing and accrediting ICT products and services.[53] Unlike the US NIST, however, they do not engage in broad public and industry consultation to determine standards. Involving the private sector is important not only because of the growing level of risk it faces, but because collaboration to determine standards would make their implementation and adoption easier.

Evidence from countries including Canada, Japan and Australia suggests that promoting self-regulation and industry collaboration can help develop effective security standards.[54] The Joint Working Group on Engagement with Private Sector on Cybersecurity (JWG) further highlights the importance of involving industry and academia in setting standards. It suggests the creation of a permanent mechanism to institutionalise public-private cooperation in standard setting, testing, and capacity building.[55]

To create ecosystem-wide resilience to cyber threats, the Government must foster private sector participation in standard-setting and information sharing. It must consider ways to incentivise enterprises to share relevant information in a timely manner. Specifically, the Government could consider introducing legislation to mandate the reporting of cybersecurity incidents for operators of critical information infrastructure. This is already being considered in the United States, in the form of the Cyber Incident Notification Act, 2021 which aims to incentivise incident reporting within 24 hours by "covered entities" by providing various legal safeguards.[56]

TO CREATE ECOSYSTEM-WIDE RESILIENCE TO CYBER THREATS, THE GOVERNMENT MUST FOSTER PRIVATE SECTOR PARTICIPATION IN STANDARD-SETTING AND INFORMATION SHARING.

Further, the JWG recommendations should also be implemented, and a permanent public-private coordination mechanism, with representation from the Government, academia, and industry, must be set up to coordinate standardisation and testing.

CONCLUSION

With an increase in the importance of digital goods and services, it is inevitable that digitalization will come to occupy an important place in geo-strategic relations between nations. The security of ICT supply chains will form an important of these geo-strategic relations. However, in adopting reactionary and ad-hoc measures to secure supply chains, nations risk splintering the global framework of digital technologies that exists currently. Instead, nations ought to determine how best they can manage their national security interests in a manner that builds trust between other like-minded nations.

The recent executive order by the US administration illustrates a path that other nations can follow to secure their ICT supply chains in an evidence-based manner that fosters trust. Policy makers in India would do well to adopt best practices reflected in the orders. Specifically, the following recommendations may be incorporated into future measures aimed at securing the nation's supply chains:

- Create proper rules and processes to effectively implement the coordination mechanism between the various cyber-security agencies that have been created by the Government

- Institutionalise a framework of reports, to be prepared by Cert-IN or NCIIPC, that systematically analyse the various threats to the security of the Indian ICT supply chain.

- Re-evaluate the cybersecurity framework, including provisions on encryption, in light of recent technological developments as well as judicial decisions on privacy.

- Facilitate ecosystem wide resilience in the ICT supply chain by creating avenues for public-private cooperation in crucial aspects of cybersecurity including standardisation and testing.

ENDNOTES

[1] Oleg Demidov & Giacomo Paoli, *Supply Chain Security in the Cyber Age*, United Nations Institute for Disarmament Research, 2020 unidir.org/sites/default/files/2020-02/Supply%20Chain%20Security%20in%20the%20Cyber%20Age%20-%20UNIDIR%20Report.pdf

[2] Lucian Constantin, *SolarWinds attack explained: And why it was so hard to detect,* CSO Online, December 15, 2020 csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

[3] Cyber Security Market Report, 2020 bit.ly/3622g2f

[4] Group of Governmental Experts, *Developments in the Field of Information and Telecommunications in the Context of International Security*, UN General Assembly, June 24, 2013 unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf

[5] National Cyber Security Centre, ncsc.gov.uk

[6] United States Cybersecurity and Infrastructure Security Agency, cisa.gov/about-cisa

[7] Bojan Pancevski, *U.S. Officials Say Huawei Can Covertly Access Telecom Networks*, Wall Street Journal, February 12, 2020 wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256

[8] Ana Swanson, *U.S. Judge Temporarily Halts Trump's WeChat Ban*, New York Times, September 20, 2020 nytimes.com/2020/09/20/business/economy/court-wechat-ban.html

[9] MeiTY, *Government of India blocks 43 mobile apps from being accessed by users in India*, Press Information Bureau, November 24, 2020 pib.gov.in/PressReleasePage.aspx?PRID=1675335

[10] BSA, *Building a More Effective Strategy for ICT Supply Chain Security*, February 16, 2021 bsa.org/files/policy-filings/02162021supplychainsecurity.pdf

[11] Executive Order 14034, *Protecting Americans' Sensitive Data From Foreign Adversaries*, June 9, 2021 federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries

[12] Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*, May 15, 2019 federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain

[13] Executive Order 14017, *America's Supply Chains*, February 24, 2021 federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains

[14] Kendall Howell, *President Biden amends restrictions on connected software applications linked to Chinese companies*, Davis Polk, June 14, 2021 davispolk.com/insights/client-update/president-biden-amends-restrictions-connected-software-applications-linked

[15] Sections 7.104 and 7.108, 15 CFR Part 7 (Rules for the Implementation of E.O.13873) govinfo.gov/content/pkg/FR-2021-01-19/pdf/2021-01234.pdf

[16] Section 4(a)(iii), E.O.14017/2021

[17] National Institute for Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018 nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[18] Cornell Law School Legal Information Institute, *Procedural Due Process* law.cornell.edu/wex/procedural_due_process

19 Section 7.107, 15 CFR Part 7 (Rules for the Implementation of E.O.13873)

20 Cornell Law School, *Procedural Due Process*

21 Ana Swanson, *U.S. Judge Temporarily Halts Trump's WeChat Ban,* New York Times, September 20, 2020 nytimes.com/2020/09/20/business/economy/court-wechat-ban.html

22 Section 7.109, 15 CFR Part 7 (Rules for the Implementation of E.O.13873)

23 William Turton and Kartikay Malhotra, *Hackers Breached Colonial Pipeline Using Compromised Password,* Bloomberg, June 5, 2021 bloom.bg/3hkXnXd

24 E.O.13636/2013, *Improving Critical Information Cybersecurity,* February 12, 2013 govinfo.gov/content/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

25 Section 5, E.O.13636/2013

26 Cyber Infrastructure and Security Agency, *Fact Sheet on ICT Supply Chain Risk Management* cisa.gov/sites/default/files/publications/factsheet_ict-scrm_508.pdf

27 Section 70B, Information Technology Act, 2000 meity.gov.in/content/icert

28 MeiTY, *Draft National Cybersecurity Policy 2013* meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

29 Section 70A, Information Technology Act, 2000

30 Lok Sabha Debate, Unstarred Question No. 552, *New And Emerging Strategic Technologies Division* mea.gov.in/lok-sabha.htm?dtl/32359/QUESTION_NO552_NEW_AND_EMERGING_STRATEGIC_TECHNOLOGIES_DIVISION

31 Moneycontrol News, *New FDI rules bar automatic investments by neighbouring countries in policy targeted at China*, April 18, 2020 moneycontrol.com/news/business/economy/govt-amends-fdi-policy-bars-neighboring-countries-from-investing-with-nod-5162851.html

32 Geeta Mohan, *Cyberspace must advance democratic values, not subvert it: PM Modi at G7 Summit*, India Today, June 14, 2021 indiatoday.in/india/story/cyberspace-advance-democratic-values-not-subvert-it-pm-modi-g7-summit-1814396-2021-06-14

33 Gunjan Chawla, Sharngan Aravindakshan and Vagisha Srivastava, *Comments to the National Security Council Secretariat on the National Cyber Security Strategy 2020*, Centre for Communication Governance, January 10, 2020 drive.google.com/file/d/14XfyXu-5sAPgzAmEaKE78vphTTfH_Y5s/view

34 OECD, *Digital Security Risk Management for Economic and Social Prosperity*, 2015

35 Vinayak Dalmia, Vrinda Kapoor and Saikat Datta, *India's Enduring Challenge of Intelligence Reforms*, Observer Research Foundation, December 9, 2020 orfonline.org/research/indias-enduring-challenge-of-intelligence-reforms

36 Standing Committee on Information Technology, *Cybercrime, Cybersecurity, and Right to Privacy*, Fifty-Second Report, February 2014 eparlib.nic.in/bitstream/123456789/64330/1/15_Information_Technology_52.pdf

37 Union Ministry of Home Affairs, *Cyber Security,* Press Information Bureau, December 18, 2014 pib.gov.in/PressReleaseIframePage.aspx?PRID=1556474

38 Scott Charney and Erec Werner, *Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust*, Microsoft, July 26, 2011 query.prod.cms.rt.microsoft.com/cms/api/am/binary/REXXtT

39 Shubhangi Agarwalla and Siddharth Sonkar, *Examining the Legal and Policy Process Behind India's Ban on Chinese Apps*, The Wire, July 7, 2020 thewire.in/tech/india-ban-chinese-apps-tiktok-legal

[40] Scott Charney and Erec Werner, *Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust*, Microsoft, July 26, 2011 query.prod.cms.rt.microsoft.com/cms/api/am/binary/REXXtT

[41] Ariel Levite, *ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies*, Carnegie Endowment for International Peace, October 4, 2019 carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974

[42] Sujan Chinoy, *Boost for India's telecom security: New directive cuts reliance on foreign equipment, including from dubious sources*, Times of India, December 28, 2020 timesofindia.indiatimes.com/blogs/toi-edit-page/boost-for-indias-telecom-security-new-directive-cuts-reliance-on-foreign-equipment-including-from-dubious-sources

[43] Software Freedom Law Centre, *Right to Information on Websites blocked by MeitY*, July 1, 2019 sflc.in/over-14000-websites-blocked-meity

[44] Jyoti Panday, *The Supreme Court Judgment in Shreya Singhal and What It Does for Intermediary Liability in India?*, Centre for Internet & Society, April 11, 2015 cis-india.org/internet-governance/blog/sc-judgment-in-shreya-singhal-what-it-means-for-intermediary-liability

[45] Apar Gupta, *But what about s.69A?*, Indian Express, March 27, 2015 indianexpress.com/article/opinion/columns/but-what-about-section-69a

[46] Atmaja Tripathy, *India Takes a Dig at Chinese Apps - A Threat to Free Speech?*, Global Freedom of Expression, Columbia University, July 13, 2020 globalfreedomofexpression.columbia.edu/updates/2020/07/india-takes-a-dig-at-chinese-apps-a-threat-to-free-speech

[47] The Centre for Internet Studies, State of Cyber Security and Surveillance in India cis-india.org/internet-governance/blog/state-of-cyber-security-andsurveillance-in-india.pdf

[48] Prabhjote Gill, *Whatsapp, Signal and Telegram Face a Catch-22*, March 31, 2021 businessinsider.in/tech/apps/news/whatsapp-signal-and-telegram-face-a-catch-22-situation-as-indias-new-social-media-rules-threaten-encryption/articleshow/81221070.cms

[49] Courts in India have recognised time and again that any measure which infringes constitutional rights must comply with the following requirements:

a. Legality - it must be backed by law
b. Legitimacy - it must be geared toward achieving a legitimate objective
c. Rationality - a rational nexus between the measure and achieving the objective
d. Necessity - the least restrictive method of effectively achieving the objective
e. Proportionality - the impact on the rights holder must not be disproportionate

The test has been reiterated by the Supreme Court in numerous cases, most recently in *Justice K.S. Puttaswamy v. Union of India* and *Anuradha Bhasin v. Union of India*

[50] Sidharth Deb, *Towards a Cyber-Security Roadmap for Digital Payments: Best Practices and Recommendations*, Observer Research Foundation, 2019 orfonline.org/wp-content/uploads/2019/04/ORF_Report_Roadmap-Digital-Payments-.pdf

[51] Udbhav Tiwari, Cyber Security & the CERT-In: Report on the CERT-In's Proactive Mandate, the Centre for Internet and Society cis-india.org/internet-governance/files/cert-ins-proactive-mandate.pdf

[52] Sidharth Deb, *Towards a Cyber-Security Roadmap for Digital Payments: Best Practices and Recommendations*

[53] Utsav Mittal, *A New Framework for a Secure Digital India*, Observer Research Foundation, November 2020 orfonline.org/research/a-new-framework-for-a-secure-digital-india/#_edn5

[54] International Financial Consumer Protection Organisation, Online and mobile payments: Supervisory challenges to mitigate security risks, September 2016 finconet.org/FinCoNet_Report_Online_Mobile_Payments.pdf

[55] Confederation of Indian Industry, *Recommendations of Joint Working Group on Engagement with Private Sector on*

Cyber Security cii.in/WebCMS/Upload/JWG%20report.pdf

[56] Brad Williams, *Mandatory Cyber Reporting Within 24 Hours: Sen. Warner Bill*, Breaking Defense, June 21, 2021 breakingdefense.com/2021/06/mandatory-cyber-incident-reporting-within-24-hours-sen-warner-bill

ESYA centre

www.esyacentre.org