॥न्यायस्तत्र प्रमाणं स्यात्॥

NATIONAL LAW UNIVERSITY DELHI

Prof. (Dr.) Ranbir Singh
Vice-Chancellor

January 10, 2020

Lt. Gen. Rajesh Pant, PVSM, AVSM, VSM (Retd.)
National Cyber Security Coordinator
National Security Council Secretariat
Sardar Patel Bhawan,
Sansad Marg, New Delhi - 110001

Subject: Submission of Comments for the National Cyber Security Strategy 2020 (NCSS 2020)

Dear Lt Gen. Pant

The National Law University Delhi is a publicly funded university established by the government of the National Capital Territory of Delhi on the initiative of the High Court of Delhi, via Act No.1 of 2008 of National Capital Territory of Delhi. The Chief Justice of India is a Visitor to the University and the Chair of the Governing Council. The Chief Justice of High Court of Delhi is the Chancellor of the University.

The Centre for Communication Governance (CCG) was established by the University in 2013 to ensure that Indian legal education establishments engage more meaningfully with information law and policy, and contribute to improved governance and policymaking. CCG is the only academic research Centre dedicated to working on information law and policy in India. The Technology and National Security team at CCG looks at the role of international and domestic law in India's national security matters from a legal and policy perspective, with a particular focus on cybersecurity, cyber conflict, and other emerging technologies. It aims to build a better understanding of national security issues in a manner that identifies legal and policy solutions that balance the legitimate security interests and national security choices with the rule of law.

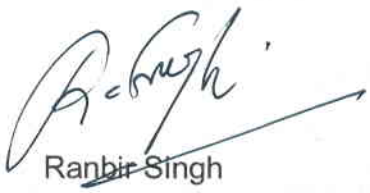
We welcome the opportunity to provide comments for the NCSS 2020 and commend your leadership for adopting a public and consultative approach to the whole process.

As part of our work, and given how critical it is to provide policymakers with useful material, we have drafted comments for the National Cyber Security Strategy 2020 (NCSS 2020), which are enclosed herewith.

We hope that the comments are of assistance to the task force in formulating the NCSS 2020, and we will be happy to find any additional material and provide any assistance for the process.

I also request you to provide an opportunity to my colleagues Ms. Gunjan Chawla (gunjan.chawla@nludelhi.ac.in), Programme Manager, Technology and National Security, CCG and Mr. Sarvjeet Singh (sarvjeet.singh@nludelhi.ac.in), Executive Director, CCG to present our work before the task force.

With warm regards,
Yours sincerely,



Ranbir Singh

(A University of Law Established in 2008 by Act No. 1 of 2008 of Delhi)
Sector-14, Dwarka, New Delhi - 110 078 ☎ :+91 11 2803 4253 🖷:+91 11 2803 4256
: ranbirsingh2107@gmail.com, vc@nludelhi.ac.in website: www.nludelhi.ac.in

CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

COMMENTS TO THE NATIONAL SECURITY COUNCIL SECRETARIAT ON THE NATIONAL CYBER SECURITY STRATEGY 2020 (NCSS 2020)

AUTHORED BY

Gunjan Chawla, Programme Manager, Technology and National Security, Centre for Communication Governance at National Law University Delhi

Sharngan Aravindakshan, Programme Officer, Technology and National Security, Centre for Communication Governance at National Law University Delhi

and

Vagisha Srivastava, Research Assistant, Centre for Communication Governance at National Law University Delhi

REVIEW AND EDITING ASSISTANCE

Sarvjeet Singh, Executive Director, Centre for Communication Governance at National Law University Delhi

Table of Contents

Volume II
Annexures

प्रस्तावना/ **Preface**

शक्ति और क्षमा/ Strength and Mercy*

क्षमा, दया, तप, त्याग, मनोबल
सबका लिया सहारा
पर नर व्याघ्र सुयोधन तुमसे
कहो, कहाँ, कब हारा?

Mercy, resolve, tact, tolerance
You've tried everything and some
But o' my King of men
When did Suyodhan succumb?

क्षमाशील हो रिपु-समक्ष
तुम हृये विनत जितना ही
दुष्ट कौरवों ने तुमको
कायर समझा उतना ही।

The more forgiving you were
In your humane compassion
The more these rogue Kauravas
Pegged you as cowardly ashen.

अत्याचार सहन करने का
कुफल यही होता है
पौरुष का आतंक मनुज
कोमल होकर खोता है।

This is the consequence of
tolerating atrocities
The awe of machismo is lost
When one is gentle and kindly

क्षमा शोभती उस भुजंग को
जिसके पास गरल हो
उसको क्या जो दंतहीन
विषरहित, विनीत, सरल हो।

Forgiveness is becoming of
The serpent that's got venom
None cares for the toothless,
Poison-less, kind, gentle one

तीन दिवस तक पंथ मांगते
रघुपति सिन्धु किनारे,
बैठे पढ़ते रहे छन्द
अनुनय के प्यारे-प्यारे।

For three days Lord Ram kept
Asking the ocean for a passage
Sitting there he petitioned
Using the sweetest words to
engage

उत्तर में जब एक नाद भी
उठा नहीं सागर से
उठी अधीर धधक पौरुष की
आग राम के शर से।

When in response there was
Not a whisper from the sea
A raging fire of endeavor rose
from Ram's body

सिन्धु देह धर त्राहि-त्राहि

The ocean took human-form
And supplicated to Ram
Touched his feet, was

करता आ गिरा शरण में
चरण पूज दासता ग्रहण की
बँधा मूढ़ बन्धन में।

सच पूछो, तो शर में ही
बसती है दीप्ति विनय की
सन्धि–वचन संपूज्य उसी का
जिसमें शक्ति विजय की।

सहनशीलता, क्षमा, दया को
तभी पूजता जग है
बल का दर्प चमकता उसके
पीछे जब जगमग है।

- **रामधारी सिंह "दिनकर"**

subservient
A slave he had become

Truth be told, it's in the quiver
That lies the gleam of modesty
Only his peace-talk is reputable
Who is capable of victory

Tolerance, forgiveness and
clemency
Are respected by the world
Only when the glow of strength
From behind them is unfurled

- Ramdhari Singh "Dinkar"

TERMS OF REFERENCE: CALL FOR COMMENTS ON THE NATIONAL CYBER SECURITY STRATEGY 2020

The Government of India (GoI) under the leadership of the National Security Council Secretariat ('NSCS' or 'the Secretariat') through a well-represented task force is in the process of formulating the National Cyber Security Strategy 2020 (NCSS 2020) to cater for a time horizon of five years (i.e., 2020-2025). Accordingly, a call for comments was issued on 01.12.2019, inviting views on various aspects of the NCSS.[1]

The NSCS has envisioned that a strategy so formulated should ensure a safe, secure, trusted, resilient and vibrant cyber space for the nation's prosperity. In light of the rapidly changing landscape of technologies, platforms, threats, services and aspirations since the formulation of the National Cyber Security Policy of 2013 (NCSP 2013), there is a felt need for a new direction in policy, that is guided by deeper commitment of protecting India's strategic interests at home and abroad.

The Centre for Communication Governance at National Law University Delhi is an academic research centre that seeks to embed good governance within communication law and policy through rigorous academic research and capacity building. We are dedicated to working on information law and policy in India, with a focus on issues that arise at the intersection of national security law and policy, and existing and emerging technologies.

We thank the members of the National Security Council Secretariat for inviting comments on the formulation of the NCSS 2020. Through the submission of these comments , we hope to meaningfully contribute to the existing law and policy making efforts of the NSCS in an open and transparent manner. Accordingly, in the course of this submission, we also highlight certain relevant areas in law and policy that require further research support from the Secretariat from a legal and policy standpoint.

[1] National Cyber Security Strategy 2020: Call for Comments, https://ncss2020.nic.in/.

EXECUTIVE SUMMARY

Cyberspace is a complex environment consisting of interactions between people, software and services supported by worldwide distribution of information and communication technology (ICT) devices and networks.[2] Accordingly, cybersecurity too, is a complex challenge that encompasses multiple governance, policy, operational, technical and legal aspects.[3]

Cybersecurity can also be viewed as one component of the broader activity of internet governance. The Ministry of Electronics and Information Technology (MeitY) considers (cyber)security as one of four layers of internet governance; the other three being governance of the (1) physical layer of the internet (e.g. routers, modem, fibre optic cables, and other ICT equipment and hardware), (2) the logical layer of the internet (e.g. TCP/IP protocol etc.) and (3) the content layer (eg. websites, posts on social media, etc.).[4]

However, the recognition of the ICT sector, including cybersecurity, as a strategic sector implies that the governance of activities within its realm has a significant impact on the national security choices available to the country. This means that security concerns that originate in cyberspace have impacts that permeate far beyond just the IT/ITES sector. It is a very important catalyst for the nation's economic growth and development, and neglect of its security could result in the negation of any economic benefits derived from its smooth functioning and healthy development. At the same time, strategic thinking demands that we bear in mind internal and external constraints operating to restrict our security choices, and make efforts to economize and encourage the judicious use of available resources and

[2] National Cybersecurity Policy 2013, para. 1, https://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.

[3] International Telecommunication Union, *Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity*, 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

[4] Ministry of Electronics & Information Technology, *Internet Governance and Proliferation*, https://meity.gov.in/content/internet-proliferation-governance.

actively guard against cybersecurity becoming a bottomless pit for public funds and resources[5] being used inefficiently to produce uncertain outcomes.

RESEARCH METHODOLOGY

These comments are the product of rigorous legal academic research. We place reliance on primary sources of doctrinal legal research, applicable domestic and international law and precedents as well as secondary sources such as news reports, statistics on cybercrime and malicious cyber activity compiled and released by various Government departments and agencies as well reports by international organizations, comments and research papers by international scholars and experts in the domain of cyber security.

Other significant primary sources include strategy and policy statements issued by various countries and their analyses by scholars and practitioners. The present comments have been complied after an in-depth comparative study of the cyber security strategies and policy documents of 16 countries, namely, Australia, Brazil, Canada, China, France, Germany, Israel, Jamaica, Japan, New Zealand, Russian Federation, Singapore, South Africa, Sri Lanka, the United Kingdom and the United States.

We examine each of these strategy and/or policy documents on a set of 25 parameters that outline the core issues, conceptual elements and institutional design to create a secure ecosystem in cyberspace.[6] In doing so, we were able to compare

[5] Tony Bradley, *The Standard Cybersecurity Model is Fundamentally Broken*, FORBES, 7 October 2019, https://www.forbes.com/sites/tonybradley/2019/10/07/the-standard-cybersecurity-model-is-fundamentally-broken/#4fc350ef1189.

[6] These parameters are (1) **Declared Objectives of the Strategy/Policy Document** (2) **Basic Pillars** (3) **Approach specified (if any)** (4) **Definitions of key concepts** (5) **Period of validity** (6) **Allocated Budgetary Resources (if any)** (7) **First responders in Cyber Incident Management and Response** (8) **Institutions (Civilian)** (9) **Institutions (Military)** (10) **Role of intelligence agencies** (11) **Offensive Cyber Capabilities** (12) **Declared stance on international norms for responsible State behaviour in cyberspace** (13) **Declared stance on free and open nature of the internet** (14) **Declared stance on public attribution of cyber-attacks** (15) **International Cooperation and Information Sharing Mechanisms** (16) **Relationship between the public and private sector** (17) **Preventive measures for cybercrime** (18) **Investigation of and punitive**

and contrast different approaches to similar issues in different jurisdictions, in light of their declared strategic and policy goals. A compilation of the summaries of these strategy and policy documents is appended as **Annexure 'A**' to this submission.

Our research is also enriched by consultations and interactions with various stakeholders and interactions with leading experts at various conferences and seminars organized by industry bodies such as NASSCOM, FICCI, CII as well as other civil society organizations working on issues in technology policy and digital rights.

Additionally, we have also taken into consideration the *Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity*[7] developed by the International Telecommunications Union and Microsoft's Whitepaper on *Developing a National Cybersecurity Strategy: Foundations for Security, Growth and Innovation*[8] for structural guidance.

SCOPE AND STRUCTURE

We have drafted these comments in view of the current geopolitical climate, rapid technological developments at home and abroad, fully cognizant of India's adversaries and allies in the realm of conventional security. Without presuming predictability, we also bear in mind the implications of declared objectives and

---

measures for cybercrime (19) **Status of Data Protection Laws** (20) **Skilling and Capacity Building for Cybersecurity Personnel** (21) **Economic Growth of the ICT sector generally** (22) **Approach to foreign investment** (23) **Supply chain risk management** (24) **Government initiatives, campaigns and programmes for cyber space** (25) **Other relevant strategies or policy documents**.

[7] International Telecommunication Union, *Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity*, 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

[8] Cristin Flynn Goodwin and J. Paul Nicolas, *Developing a National Cybersecurity Strategy: Foundations for Security, Growth and Innovation*, Microsoft, October 2013, https://www.microsoft.com/en-us/cybersecurity/content-hub/developing-national-strategy-for-cybersecurity.

programmes for the latest iterations[9] of India's foreign policy. We have tailored our research in accordance with the terms of reference outlined in the NSCS' Call for Comments on the National Cyber Security Strategy 2020 - 2025. The research is presented in six parts.

Part I presents details of our research methodology and a brief introduction to the need for a cybersecurity strategy as distinct from but connected to policy and theoretical frameworks in strategic thought that have guided the formulation of suggestions made in this paper.

Part II examines the scope and sources of existing and emerging threats to cybersecurity in India. We present and analyse statistics on malicious cyber activity tracked by CERT-In as well as data on incidence and reporting of cybercrimes under the Information Technology Act, 2000 as well as ICT enabled commission of crimes punishable under the Indian Penal Code, 1860. Based on the analysis of this data, we present the contours of the cybersecurity threat landscape in India and possible approaches to prioritizing cybersecurity threats and risks that need to be managed, tackled or eliminated.

The next three parts of this paper, in accordance with the three Pillars of Strategy envisioned and enumerated in the Call for Comments, analyzes a wide-ranging set of issues in cybersecurity under the following themes:

1. Secure (The National Cyberspace)
2. Strengthen (Structures, People, Process, Capabilities) and
3. Synergise (Resources including cooperation and collaboration)

Part III unpacks the contents and constraints of the first pillar, namely, "Secure". Here we outline the relevant provisions of international and domestic law that must be taken into consideration in defining and demarcating the 'national cyberspace', or

[9] Shri S. Jaishankar, Speech at the 4th Ramnath Goenka Lecture, 14 November 2019, https://mea.gov.in/Speeches-Statements.htm?dtl/32038/External+Affairs+Ministers+speech+at+the+4th+Ramnath+Goenka+Lecture+2019; *see also* Special Correspondent, *PM Affirms India's 'strategic autonomy'*, The Hindu, 1 June 2018, https://www.thehindu.com/news/national/pm-affirms-indias-strategic-autonomy/article24061287.ece.

a ‘sovereign (protected) cyberspace’. We also attempt to identify discrete components and entities that would comprise such a realm, the protection of which would be the primary responsibility of the Government. In accordance with India’s international legal obligations and domestic needs and priorities, we present the principle of peaceful uses of cyberspace for the consideration of and adoption by the Secretariat in its formulation of the NCSS 2020. In this regard, we also submit for consideration and adoption the principle of ‘common but differentiated responsibility’ for assigning roles and responsibilities to public and private in the protection of cyberspace. The comments and suggestions contained herein deal with the *horizontal dimension* of our cybersecurity strategy which deals primarily with the dialectic between allies and adversaries in cyberspace.

Part IV expounds on the second pillar, namely, “Strengthen”. In this we deal with the *vertical dimension* of strategy, namely the tangible and intangible links within the institutional architecture for cybersecurity that need to be strengthened for enhanced protection from malicious activities in cyberspace. We classify our analysis and suggestions under three main categories: processes, institutions and skills/awareness.

Part V deals with the third pillar, namely, “Synergise”, where we examine how the *horizontal* and *vertical dimensions* of the strategy can be integrated in order to optimize levels of inherent *friction* that could hinder the achievement of strategic and policy goals. We outline three levels at which synergies need to be identified and/or created. First, at the inter-ministerial level, among government departments and agencies. Second, at the national level, for enhanced cooperation and strategic partnerships between the public and private sectors. Third, at the international level for enhanced cooperation and strategic partnerships with like-minded nations towards building stronger defences in cyberspace.

Finally, the last part concludes the major findings, suggestions and recommendations of this submission.

LIMITATIONS

The scope of this paper is as outlined above. However, it is pertinent to highlight that the present submission does not deal with cyber security strategy for the nation's armed forces, except to the extent of examination required to highlight opportunities to create synergies between the military establishment and civilian agencies performing similar functions. We believe that the cyber security strategy for the defence forces needs to be articulated separately, bearing in mind their unique requirements. Namely, the complementary need for confidentiality to retain the element of surprise in sensitive military operations, as well the need to ensure an agile force that that plays a highly specialized role in the broader landscape of creating a cyber-secure nation. In this regard, the formulation of the Joint Training Doctrine of the Armed Forces in 2017, is a step in the right direction, but needs to be strengthened and aligned with the broader framework of National Cyber Security Strategy 2020 after it is formalized.

Additionally, since our Right to Information (RTI) request for a copy of the COMCASA and LEMOA Agreement signed in 2016 between the United States and India was denied on the grounds under Section 8 of the RTI, 2005, we are at this stage, unable to provide a comprehensive analysis of strategic cooperation in defence and military communications.[10]

[10] RTI Applications no. MODEF/R/2019/53566 dated 30.10.2019, MODEF/R/2019/81386 dated 05.11.2019 (COMCASA); RTI Applications No. MODEF/R/2019/53584 dated 31.10.2019 and MODEF/R/2019/81387 dated 05.11.2019 and MODEF/R/2019/81392 dated 06.11.2019. Response received via letter addressed to Ms. Vagisha dated 25.11.2019, MOD ID No. 45(1)/2018-D(IC-II). (On file with the authors)

I. INTRODUCTION: WHY WE NEED TO ARTICULATE A NATIONAL CYBER SECURITY STRATEGY

The National Cyber Security Policy of 2013 was introduced by the Government of India with the aim of protecting information as well as to build a secure and resilient cyberspace for businesses, citizens and government.[11] The 2013 Policy highlighted the need to protect cyber infrastructure, reduce vulnerabilities, build capabilities to prevent and respond to cyber threats. It also sought to minimize damage from cyber incidents through a combination of institutional structures, stakeholder participation, process, technology and cooperation.[12]

One of the most significant contributions of the 2013 policy statement was the recognition of the strategic importance of the IT/ITES sector. However, mere recognition of the strategic importance of the sector does not necessarily result in a strategic approach to policy. The policy provided an overview of what it takes to effectively protect information, information systems and networks and also gave an insight into the Government's approach and strategy for the protection of cyberspace in the country.[13] However, under the rubric of 'strategy', the document outlined and highlighted certain *policy* goals and objectives.

We submit that the current strategy and the strategic goals in it should articulate aspirations and principles that build on the previous policy/strategy and extend beyond policy objectives. We believe that the strategy must drive policy goals, and not *vice versa*. In addition to the human, institutional and political units that form part of the strategic enterprise, we must at the very outset, recognize that the material elements, which are the object of regulation and governance through policy, i.e. cyber security products and services are inherently dual-use items that must remain available for utilization by civilians as well as military and state organs in accordance with the 'whole-of-nation' approach emphasized in the call for comments.

---

[11] National Cyber Security Policy 2013 at p.5, accessible at https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf.

[12] Ibid.

[13] Ibid at page 2 para 7.

The crucial role of the IT sector in general and cybersecurity sector in particular, in creating new economic opportunities and in preserving and promoting the economic growth trajectory of the nation must be retained at the heart of our cybersecurity strategy. MeitY estimates that India can create upto 1 trillion dollars of economic value from the digital economy by 2025, with half of the opportunity originating in new digital ecosystems.[14] **However, this does not imply an adoption of the American approach, which is designed around the belief that "economic security is national security".[15] Over-securitization of a strategic sector may risk stifling the sector's economic growth and innovation in the Indian context, where the cybersecurity industry is still in its infancy stage.** Thus, the formulation of strategy must first and foremost, focus on creating an ecosystem that is conducive to the creation of a robust industrial base for cybersecurity upon which the security infrastructure of the nation can effectively rely.

A. THE THEORETICAL UNDERPINNINGS OF STRATEGY AND ITS DIMENSIONS

"War is the continuation of politics by other means," wrote Carl von Clausewitz, the Prussian General and military theorist.[16] He viewed strategy as being "the art of the General". However, with the advent of 'cyber warfare' and a broader, global proliferation of tendencies towards the weaponisation of ICT technologies, the physical, social, economic and cognitive impacts of such 'cyber wars' extend far beyond the military domain. Accordingly, strategy too, must be designed bearing in mind the role and contributions of civilian institutions and stakeholders.

Writing nearly a century after Clausewitz in 1965, General Andre Beaufre, finding the Clausewitzian definition to be restrictive, asserted[17] that strategy cannot be a single defined doctrine. It is a method of thought, the object of which is to codify events, set them out in order of priority and then choose the most effective course of action. In

[14] Ministry of Electronics and Information Technology, Government of India, *India's Trillion Dollar Digital Opportunity,* https://meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

[15] National Security Strategy of the United States of America, The White House, November 2017, at p.17, accessible at https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[16] Carl von Clausewitz, *On War* (1832) at p.1.

[17] Andre Beaufre, *An Introduction to Strategy* (1965).

his view, the essence of strategy can be distilled, and it is the art of the dialectic of force, or, more precisely, the art of the dialectic of two opposing wills using force to resolve their dispute. In the view of Edward Luttwak,[18] the sphere of strategy applies to the domain of human relations that… "*are conditioned by armed conflict actual or possible*"[19]. In his book *The Logic of Strategy*[20]*,* dubbed as one of the finest works of Clausewitzian revival, he asserts that the paradoxical logic of strategy applies to adversarial relations in such situations of actual or possible armed conflict (eg. if you want peace, prepare for war).

The entire realm of strategy is pervaded by a paradoxical logic of its own, standing against the ordinary linear logic by which we live in all other spheres of life, it often violates ordinary linear logic by inducing the coming together and even the reversal of opposites. [21]

This is in contradistinction to all other spheres of life, such as trade, commerce, culture, and consensual governance where conflict is merely incidental to the carrying out of activities in daily life, where ordinary linear logic rules supreme [if you want A, strive for A]. The element of consent in social and political intercourse is of crucial importance for the applicability of linear logic, and he identifies regressive and dictatorial regimes as an exception to this general rule. Absent such agreement, consent or submission to legitimate authority, arises the conflict of opposing wills, each trying to force itself on its opponent. This absence of consent between adversaries necessitates the use of the paradoxical logic which pervades the entire realm of strategy [if you want A, strive for B/ if you want to sail your ship safely, strive to sink your enemy's ship], as an exception to ordinary linear logic in consensual governance, or administration. This dynamic between real and potential adversaries relates to the *horizontal dimension* of strategy, i.e. the dynamic between two

[18] Thomas Meany, *The Machiavelli of Maryland,* The Guardian, 9 December 2015, accessible at https://www.theguardian.com/world/2015/dec/09/edward-luttwak-machiavelli-of-maryland, last accessed on 2 January 2020.

[19] Edward Luttwak (1987), *The Logic of Strategy,* p. 5

[20] Ibid.

[21] Harry G Summers Jr., *When is a bad road good?,* The New York Times, 30 August 1987, accessible at https://www.nytimes.com/1987/08/30/books/when-is-a-bad-road-good.html.

adversaries who seek to "*oppose, deflect, and reverse each other's moves*". And so, war becomes an "*an act of force to compel our enemy to do our will*".[22]

However, we must also examine and delve into the *vertical dimension* of strategy, i.e. the interplay of technological, tactical, operational and higher, or grand strategy levels, among which natural harmony is always lacking.[23] Luttwak, like Clausewitz, recognized *friction* as an all-pervasive feature in war which prevents such harmonisation and the realisation of strategic goals. He acknowledges the centrality of strategy in the conduct of warfare at all these levels, but its role is unimportant, or even irrelevant in administrative aspects, or the governance and logistics of war, where the ordinary linear logic of economic efficiencies must apply. The subject of such an endeavour is identified to be inanimate objects, or entities that do not or cannot oppose the will of the principal actor.

The principal distinguishing feature of strategic action is that while pursuing strategic objectives, effectiveness (result-oriented action) trumps efficiency (resource-oriented action), whereas in administrative action, the economization of resources and greater efficiency are accorded higher priority. However, this does not imply that strategic action entirely excludes administrative action from its ambit. For example, technological advancement of the means of warfare available to a state may still be constrained by its financial resources and thus, would require that the state economize its resources in the pursuit of technological advantage for a strategic objective. In *The Logic of Strategy*, Luttwak also identifies situations wherein strategy's paradoxical logic may be displaced by economic priorities, and recognizes it as perfectly valid, but only in peacetime.

Accordingly, we analyse India's strategic options in cyberspace with a view to identifying points of tension and synergy across the horizontal and vertical dimensions of the dialectic between multiple stakeholders in cyberspace, each seeking to protect and advance their interests.

[22] Carl von Clausewitz (1832), *On War* Book 1, Chapter 1, p. 1

[23] Edward Luttwalk (2001), *Strategy: The Logic of War and Peace*, p. xii.

II. EXISTING AND EMERGENT CYBER THREATS: LANDSCAPE FOR INDIA

The cyber-attacks on the Kudankulam Nuclear Power Plant (KKNP) and the Indian Space Research Organisation (ISRO) in September 2019 highlighted the urgent need to prioritize the cybersecurity of *inter alia* our critical information infrastructure and sovereign assets.[24] Similarly, the cyber-attack on Cosmos Bank in Pune, in August 2018 resulted in the siphoning off a massive sum of Rs. 94 crore in merely two days.[25]

While both these incidents are extremely serious and alarming for the state of cybersecurity in India, the formulation of a strategy to deal with attacks of these kinds must take the broader landscape of existing and emergent threats into account. Most successful national strategies are based on a risk-management approach, wherein the Governments and private sector partners agree on the risks that must be managed, mitigated or even accepted.[26] The KKNP/ISRO as well as the Cosmos Bank cyber-attacks are salient examples of the *risks* posed to the overall security of the nation due to malicious actors in cyberspace, that need to be managed and mitigated.

According to the Data Security Council of India (DSCI), India was the second most affected country due to targeted cyber-attacks between 2016 and 2018.[27] Cyber-attacks have evolved and increased in volume over the years. Attacks have also become sophisticated in nature and types of attacks such as APT, Zero Day,

---

[24] Gulshan Rai, *Why Cybersecurity Should be India's Foremost Priority,* THE ECONOMIC TIMES, 31 October 2019, accessible at https://economictimes.indiatimes.com/tech/internet/why-cybersecurity-should-be-indias-foremost-priority/articleshow/71843562.cms.

[25] Cosmos Bank's server hacked, Rs. 94 crore siphoned off in 2 days, THE ECONOMIC TIMES, 14 August 2018, accessible at https://economictimes.indiatimes.com/industry/banking/finance/banking/cosmos-banks-server-hacked-rs-94-crore-siphoned-off-in-2-days/articleshow/65399477.cms.

[26] Microsoft Policy Papers, *National Cyber Security Strategy, accessible at* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW5Aly

[27] NASSCOM-Data Security Council of India, *Report on Cyber Insurance in India: Mitigating Risks Amid Changing Regulations and Uncertainties*, 26 April 2019, accessible at https://www.dsci.in/content/cyber-insurance-in-india.

malwares, multi-vector attacks have become common, targeting core infrastructure such as ATM switches, payment interfaces.[28]

For want of technical expertise, we refrain from making detailed qualitative comments on the technical characteristics or sophistication of cyber-attacks directed against India. Instead, we offer a quantitative analysis of the incidence and reporting of such cyber-attacks, cyber incidents, and cybercrimes, relying on information released by two main Government agencies, namely, the data compiled by CERT-In[29] and the National Criminal Records Bureau[30] to describe the nature of malicious cyber activity India is faced with, and is aware of.

Based on the analysis of this data, we are able to make evidence-based recommendations on the nature of threats to cyber security that need to be accorded the highest priority in the formulation of the National Cyber Security Strategy 2020.

A. Trends in Malicious Cyber Activity in India (2013-19)

Annual Reports of the Indian Computer Emergency Response Team (CERT-In) describe various types of malicious cyber activity including phishing, network scanning/probing, virus/malicious code, spam, website intrusion and malware propagation, website defacement and others. We have compiled data from 2013 through 2018. At the time of writing, the CERT-In's Annual Report for 2019 has not yet been released by the Government.

The graphical representation in Figure 1 shows a dramatic increase in network scanning / probing between the years 2013 to 2018. From 9359 incidents of network scanning and probing in 2017, we saw 127481 such incidents in 2018, more than a

[28] NASSCOM-Data Security Council of India and Price Waterhouse Cooper, *Report on Cyber Security Market in India: What Lies Beneath*, 4 December 1029, accessible at https://www.dsci.in/sites/default/files/documents/resource_centre/Cyber%20Security%20India%20Market.pdf.

[29] Accessed from Annual Reports (2013-2018) published by CERT-In, available at https://www.cert-in.org.in, last accessed on 5 January 2020.

[30] Accessed from Crime in India Reports (2013-2018) published by NCRB, available at http://ncrb.gov.in, last accessed on 5 January 2020.

ten-fold increase. This is a worrying trend, given that network scanning and probing constitutes a major means of carrying out cyber espionage. Admittedly, not all network scanning and probing activities in cyberspace would constitute espionage. However, the magnitude of risk posed by these frequent scanning and probing activity to the overall security of information networks within the 'national cyberspace' cannot be taken lightly. The incidence of viruses or malicious code has seen a five-fold increase in the same time period.

Another dangerous trend evident from Figure 1 is the prevalence of spam, or unsolicited communication, which highlights data protection issues in our cyber ecosystem. High levels of spam, or unsolicited emails and other communications are symptomatic of low levels of protection to privacy of personal information such as contact details. Increase in spam also leads to vulnerability to phishing attacks. This cannot be taken lightly, given that the KKNP cyber attackers reportedly gained entry by way of a phishing email to one of the senior employees.[31]

For this reason, it is worrying that the CERT-In has discontinued reporting on the incidence of spam since 2017. It is important that the government track and monitor this as not only a potential point of entry into protected systems by attackers, but also as an indicator of the successes of the legal framework for personal data protection, which is currently being considered and deliberated upon by a Joint Parliamentary Committee of the Parliament.

[31] *Suspected North Korea Hackers targeted Indian space agency,* FINANCIAL TIMES, 7 November 2019, https://www.ft.com/content/ac6a8782-ffad-11e9-b7bc-f3fa4e77dd47.

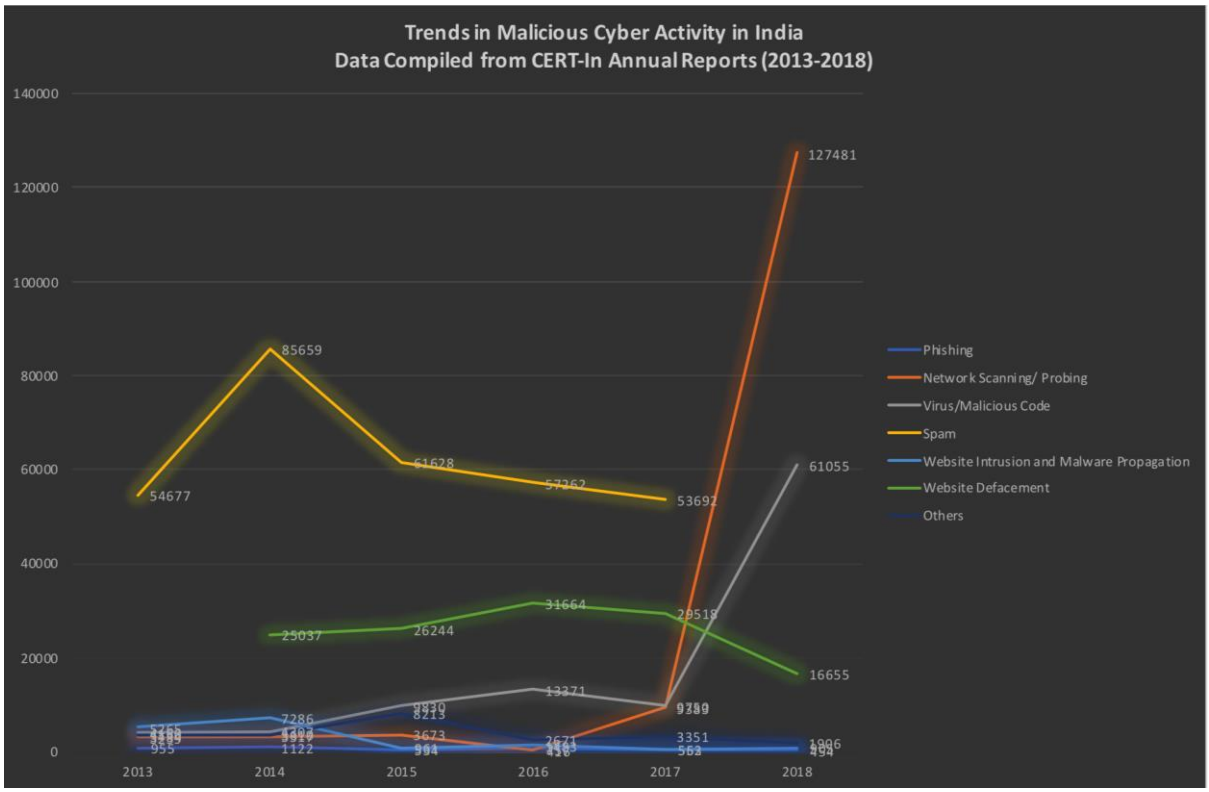


Figure 1: Trends in Malicious Cyber Activity in India (2013-19)

We remove the three most frequent malicious activities (spam, virus/malicious code and network scanning/probing activities) from Figure 1 for clarity on other kinds of malicious cyber activity in Figure 2. We can consistently see a much higher incidence of defacement of websites than any other malicious activity. Another point to improve reporting of cyber incidents by CERT-In is to encourage clarity on what activities constitute “Others”, a term which remains unexplained in its Annual Reports.

In the next section, we examine trends in reported incidence of cybercrimes in India since the formulation of the National Cyber Security Policy 2013.

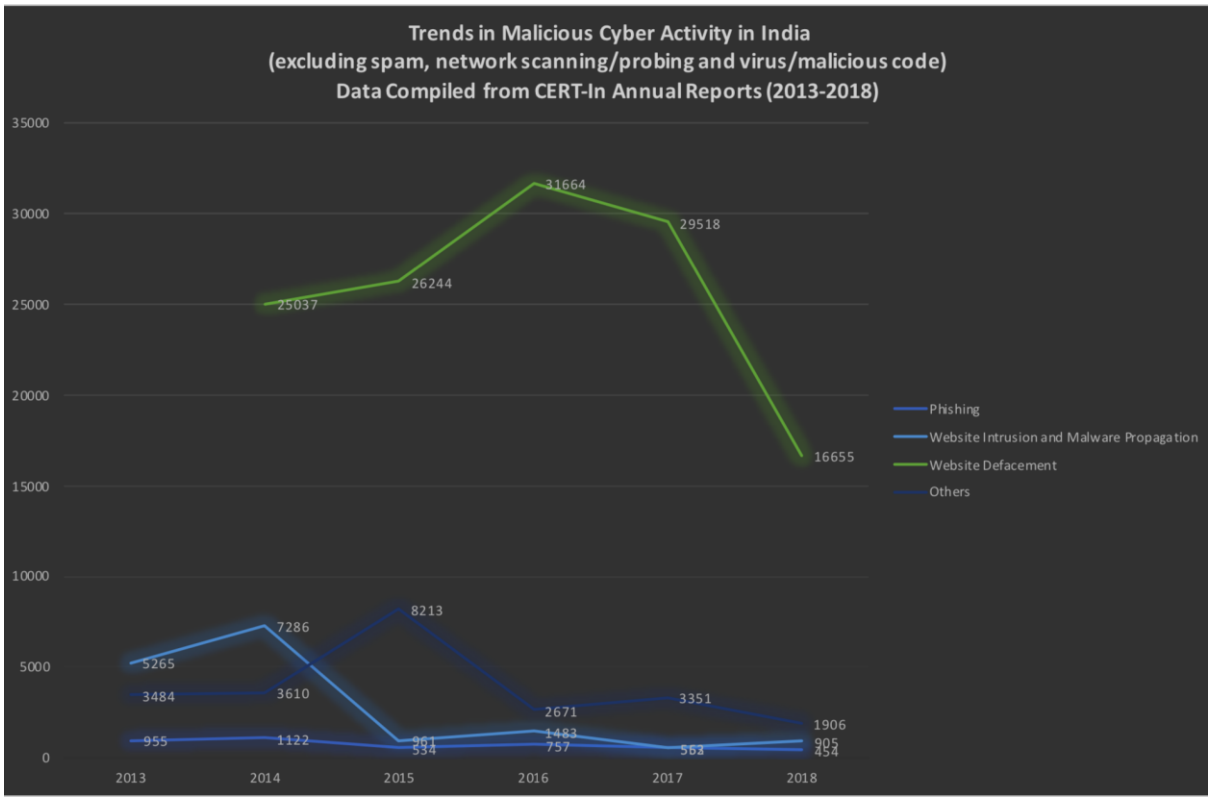


Figure 2: Trends in Malicious Cyber Activity in India excluding spam, virus/malicious code and network scanning/probing activities (2013-19)

B. Incidence and Investigation of Cyber Crime in India

Fighting cybercrime was one of the key objectives of the National Cyber Security Policy 2013.[32] However, the number of cyber-crimes almost doubled in 2017.[33] Data released by the National Crime Records Bureau indicates that India recorded 9622, 11592 and 12317 cases of cybercrimes in 2014, 2015 and 2016 respectively.[34]

It is difficult to strictly view cybercrimes only as a law and order issue like other crimes. This is because, due to the inherent nature of ICT and cyberspace, a cybercrime can be committed both by domestic criminals as well as actors such as international terrorists or even State sponsored attacks, which pose a larger threat to

[32] National Cyber Security Policy 2013, Page 6, paras 10 & 11.

[33] Utpal Bhaskar, Cyber-crime cases in India almost doubled in 2017, Livemint, dated 22 October 2019, accessible at https://www.livemint.com/companies/news/cyber-crime-cases-in-india-almost-doubled-in-2017-11571735243602.html, last accessed on 26 December 2019.

[34] Ibid.

national security. Hence, cybercrimes having a clear and substantial international element may be investigated from a national security perspective as well.

However, this may play out differently in actual practice, due to the use of various concealment and disguising tools easily available to malicious cyber actors. Cybersecurity firm Symantec notes that it is also possible for actors to insert false flags, including carry out purposeful misdirection, obfuscation, and fake clues designed to mask their identities.[35] We deal with these challenges in the investigation and prosecution of cyber crimes in Part IV, with a view to strengthening technological capacity of investigative agencies.

With the exception of cyber terrorism, defined under Section 66F of the Information Technology Act, 2000, the responsibility to investigate all other cybercrimes is entrusted to local law enforcement agencies. In accordance with Schedule I of the National Investigation Agency (NIA) Act, 2008, as amended in 2019, the investigations relating to incidents of cyber terrorism is entrusted to the National Investigation Agency. While investigating domestic cybercrime in itself is an uphill task for most cybercrime cells[36], when state sponsored cybercrimes are thrown in the mix, it becomes nearly impossible to conclusively attribute responsibility even on the technical level, let alone legal.[37] Lack of consequences due to difficulties in attribution has led to a steady rise in state sponsored cybercrimes.[38]

---

[35] The Cyber Security Whodunnit: Challenges in Attribution of Targeted Attacks, Symantec Corp, dated 3 October 2018, accessible at https://www.symantec.com/blogs/expert-perspectives/cyber-security-whodunnit-challenges-attribution-targeted-attacks, last accessed on 5 January 2020.

[36] Arunab Saikhia, Why most cybercrimes in India don't end in conviction, Livemint, 29 July 2016, https://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html.

[37] International law cannot keep up with cyber-criminals, World Economic Forum, 25 February 2019, https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/.

[38] State-Sponsored Cyberattacks Are On The Rise, Nasdaq, 21 February 2019, accessible at https://www.nasdaq.com/articles/state-sponsored-cyberattacks-are-rise-2019-02-21.

The negative monetary effects of malicious cyber activity cannot be underestimated. According to a report by the Office of the President of the United States, malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.[39] Similarly, a study by the Data Security Council of India shows that the average cost for a data breach in India has gone up to INR 11.9 Cr (USD 1.7 Mn), an increase of 7.9% from 2017 with the average cost per record being INR 4,552 (USD 64).[40] The study also found India as the second most affected country due to targeted cyber-attacks.[41] Denial of Service (DoS) attacks can cause huge losses to service providers, while the IP theft of a small enterprise relying on one product can cause it to shut down entirely. Given India's aims of reaching a $5 trillion dollar economy by 2025, serious attention will need to be shown to secure our cyberspace from the threats that manifest as cyber-crime and cyber attacks.

1. Trends in Cyber Crimes under the Information Technology Act, 2000 (2013-17)

Figure 3 is a graphical representation of the reported incidents of crimes under the IT Act, 2000.

There are certain issues with the reporting of incidence of these crimes by the NCRB. Firstly, it is not clear why offences between Sections 66 to 66E are reported in a consolidated manner. Each of these offences are distinct and have different consequences for the victims of such crimes. For example, the offence of hacking (Section 66), identify theft (Section 66C), and offences relating to publishing images of private areas (Section 66E) can indeed, be viewed through the common lens of being violations of under privacy. Yet, depending on the identity of the intended victim (whether it is a protected system, whether it is owned by a private individual, corporation, or Government agency, etc.) these crimes may have vastly different and

[39] The Council of Economic Advisors, Office of the President of the United States of America, *The Cost of Malicious Cyber Activity to the U.S. Economy*, February 2018, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[40] Data Security Council of India, *Cyber Insurance in India- Mitigating risks amid changing regulations & uncertainties*, (2019), p. 18, https://www.dsci.in/resource/centre/studies-%26-reports/cyber-security.

[41] Ibid.

in some cases, even negligible consequences or implications for the maintenance of law and order. Hence, clubbing and reporting them together may not present the right picture.

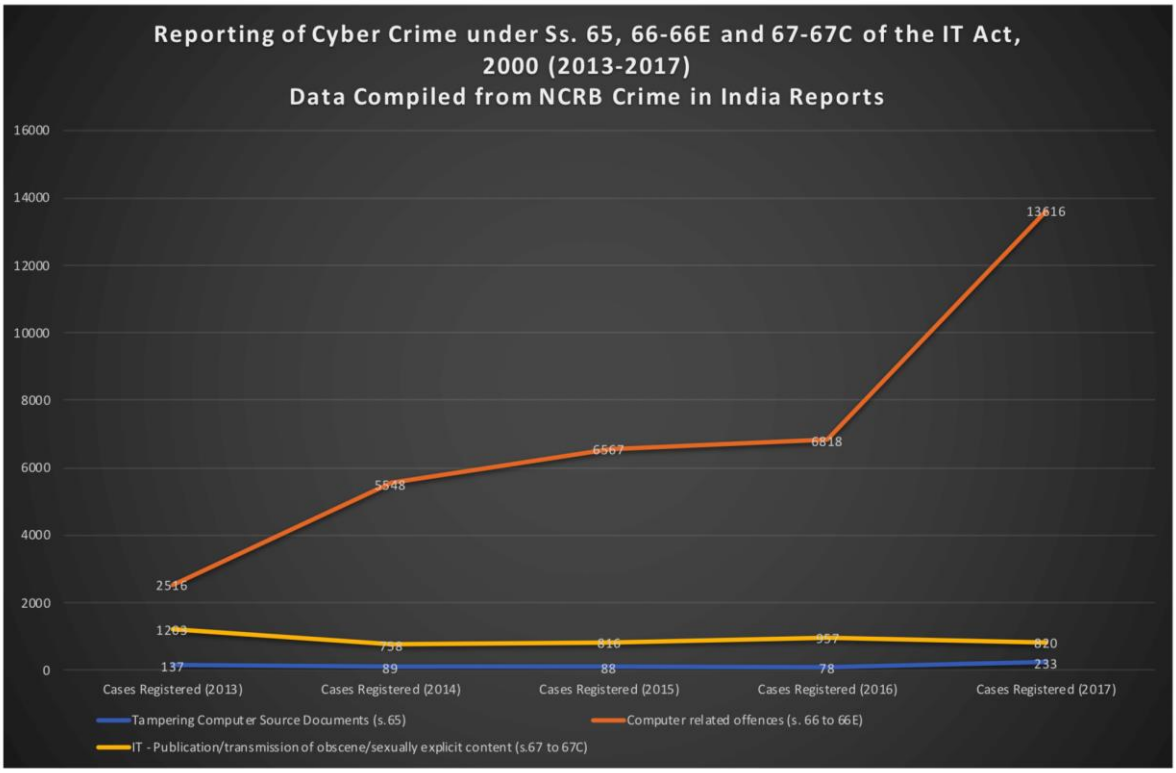


Figure 3: Reporting of Cyber Crime under Sections 65, 66-66E and 67-67C of the IT Act, 2000 (2013-17)

Secondly, the clubbed reporting of these offences has continued even after 2015, i.e., when the Supreme Court struck down Section 66A as unconstitutional.[42] This raises issues of clarity since it has come to light that offences under Section 66A were continued to be registered,[43] and it is not clear whether this reporting includes such cases. This presents a distorted and potentially even exaggerated picture of the incidence of each of these crimes, and needs clarification from the NCRB for reliable

[42] *Shreya Singhal Vs Union of India*, (2013) 12 SCC 73.

[43] Abhinav Sekhri and Apar Gupta, *Section 66A and Other Legal Zombies (October 31, 2018)*, IFF Working Paper No. 2/2018 (Nov. 26, 2018), https://ssrn.com/abstract=3275893; SC to Centre: Why the continued use of the dead Section 66A of the IT Act?, Medianama, https://www.medianama.com/2019/01/223-sc-centre-section66a-still-in-use-it-act/..

data which can form the basis for evidence-based policy making for the enforcement of law and order in cyberspace.

In any case, it is evident from Figure 3 that there is a steady rise in offences under Sections 66 to 66E of the Information Technology Act, 2000, with 2516 cases registered in 2013, 5548 cases registered in 2014, 6567 cases registered in 2015, 6818 cases registered in 2016. This number sharply increased to 13616 cases registered in 2017. However, we are unable to comment on the share of each of these offences (under Sections 66 to 66E) in the total reported numbers or draw any further inferences therefrom.

Offences in tampering with computer source documents have also risen from 78 in 2016 to 213 in 2017. This is a cause for concern as it adversely impacts the integrity of data available to the intended victim. If the intended attack surface is a protected system under the control of the Government or contains classified data of any of its departments or agencies, prompt and strict action must be initiated without delay. Obscenity related offences have maintained their presence and numbers with 957 cases registered in 2016 and 820 cases registered in 2017.

2. Cyber Terrorism and Other Offences under the IT Act, 2000

Figure 4 shows a marked increase in cyber terrorism from 0 reported cases in 2013 to 13 registered cases in 2017. Given that the 2013 Policy identified cyber terrorism as a significant threat[44] and also aimed at ensuring cyber resilience, the rising trend in cyber terrorism is a possible indicator of its ineffectiveness, highlighted by the recent cyber-attack on the nuclear facility in Kudankulam. It is worth emphasizing that the NIA has the exclusive jurisdiction to investigate such incidents of cyber terrorism.

With serious privacy and data protection implications, there is also a rise in offences relating to breach of confidentiality and disclosure of information. It is worrying that the NCRB has omitted reporting data on these offences after 2016.

[44] National Cyber Security Policy, 2013, at page 4, para 5.

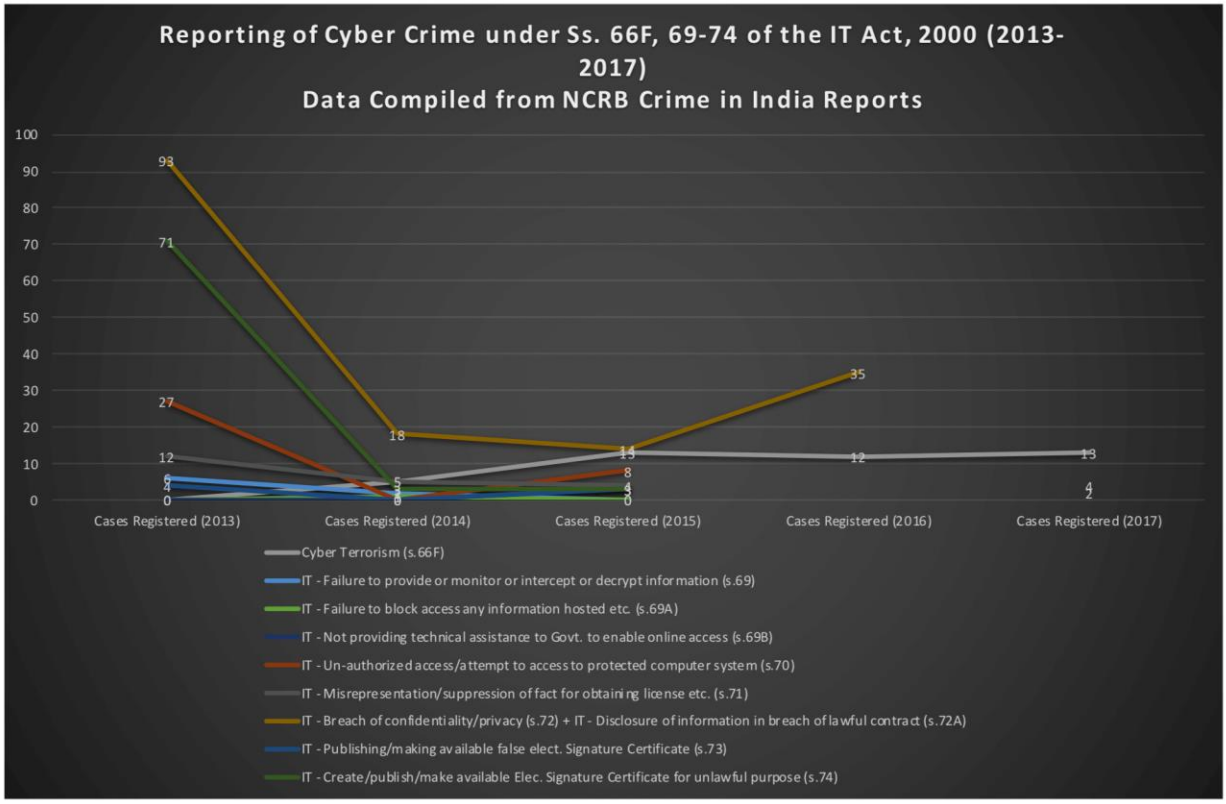


Figure 4: Reporting of Cyber Crime under Sections 66F, 69-74 of the IT Act, 2000 (2013-17)

It is equally worrying that there is no reporting post 2015 of certain offences such as those relating to unauthorized access to computer systems (Section 70).

In this regard, we submit that data on the incidence of cyber-crimes should be made available publicly, and disseminated widely, in order that individuals may be made aware of the kinds of cyber-crime and cyber malicious activity that are most prevalent in India's cyber space. This would enable at the very least, those persons having the required technical skills and training, or even basic levels of cyber security awareness, to take appropriate measures within their means to protect themselves from cyber-crimes, intrusions and attacks.

3. Trends in ICT-enabled crimes under the Indian Penal Code, 1860 (2013-17)

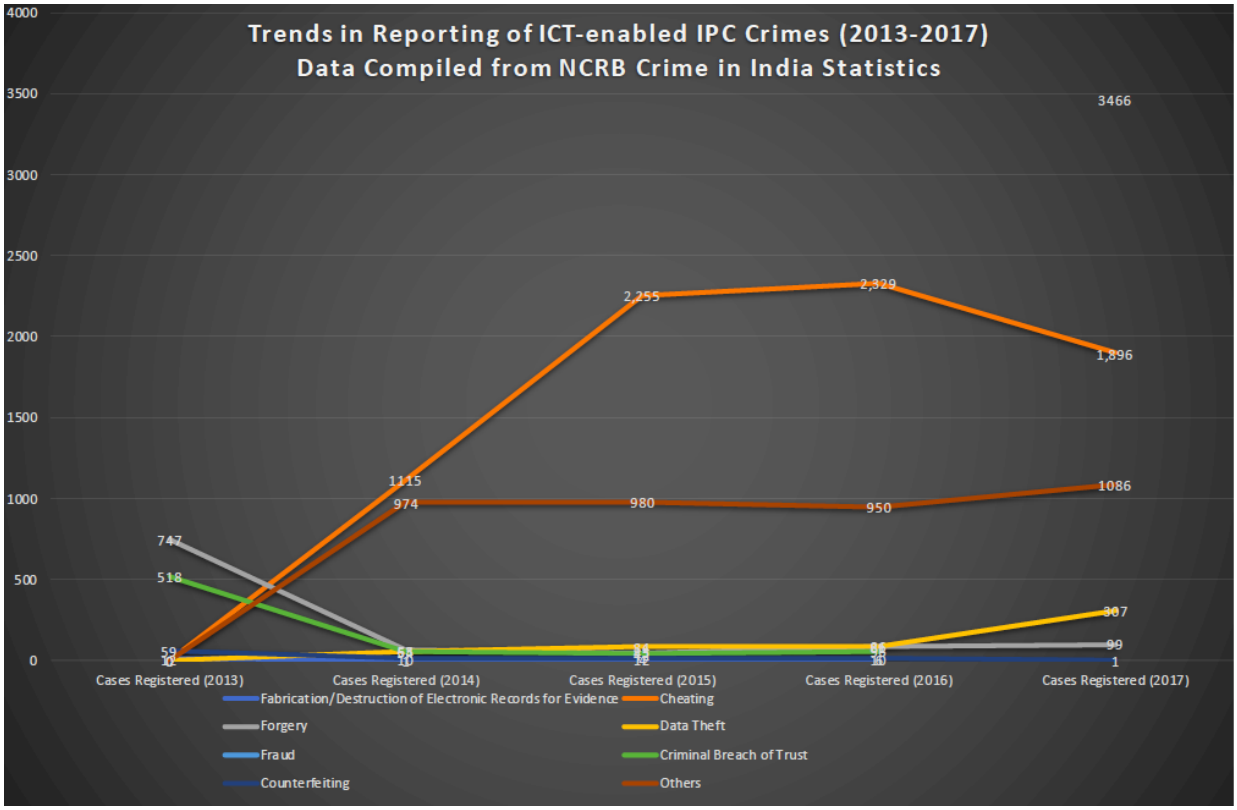


Figure 5: Trends in reporting of ICT-enabled IPC crimes (2013-17)

Figure 5 charts the incidence of major crimes under the Indian Penal Code, 1860 (IPC) that are enabled by the use of information and communication technologies (ICT). The solitary number 3466 at the top right corner of this chart represents the incidence of ICT-enabled fraud. This data has been included for the first time by the NCRB in compiling its statistics on Crime in India. In fact, other than being the *crime* with the highest incidence compared, fraud is also an important *motive* for cyber criminals. The 2017 Report highlights that fraud is the single most prevalent motive for more than half of cyber-crime reported in India, followed by sexual exploitation and causing disrepute.[45] It is therefore not surprising that the offence of cheating (u/s 420 of the IPC) is consistently among the highest reported crimes.

For clarity on trends in crimes having a relatively lower incidence and reporting levels, we omit 'cheating' 'fraud' and 'other' offences in Figure 6.

[45] *Fraud and sexual exploitation prime motives of cyber crimes in country: NCRB Data*, The Print, 22 October 2019, https://theprint.in/india/fraud-and-sexual-exploitation-top-cyber-crimes-in-country-shows-ncrb-data/309799/.

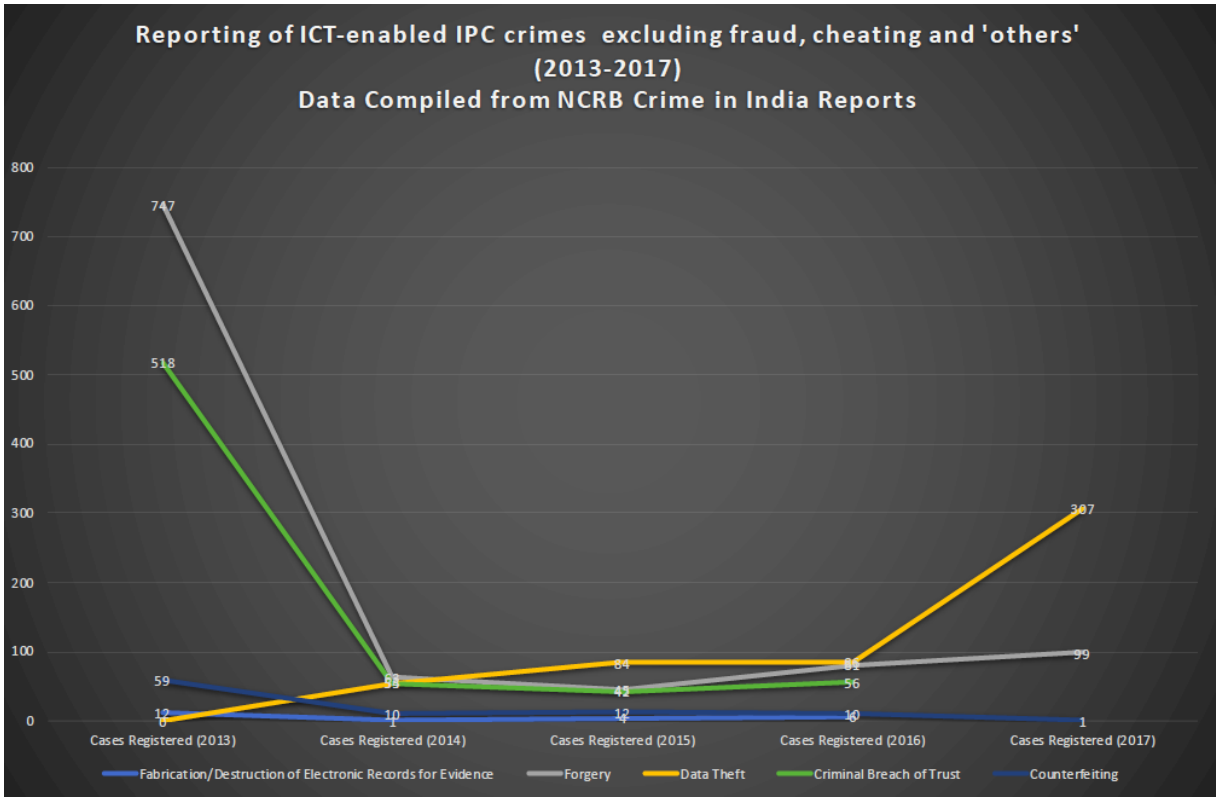


Figure 6: Reporting of ICT-enabled IPC crimes excluding fraud, cheating and others (2013-17)

Figure 6 shows a steep decline in ICT enabled forgery and criminal breach of trust cases which could possibly be an immediate consequence of the mechanisms installed by the National Cybersecurity Policy of 2013, although both show a slow but steady rise thereafter. We can also see that data theft and forgery are steadily on the rise, both of which have significant implications for financial losses as a direct consequence of economically-motivated cyber-crime.

Again indicating reporting issues, the incidence of the crime of fabrication of electronic records and criminal breach of trust are not indicated after 2016 without assigning any reasons for this omission.

The NCRB's Crime in India 2017 report includes statistics on the incidence of certain other cyber-crimes that were not included in earlier reports. Data with respect to these offences is as indicated in Figure 7:

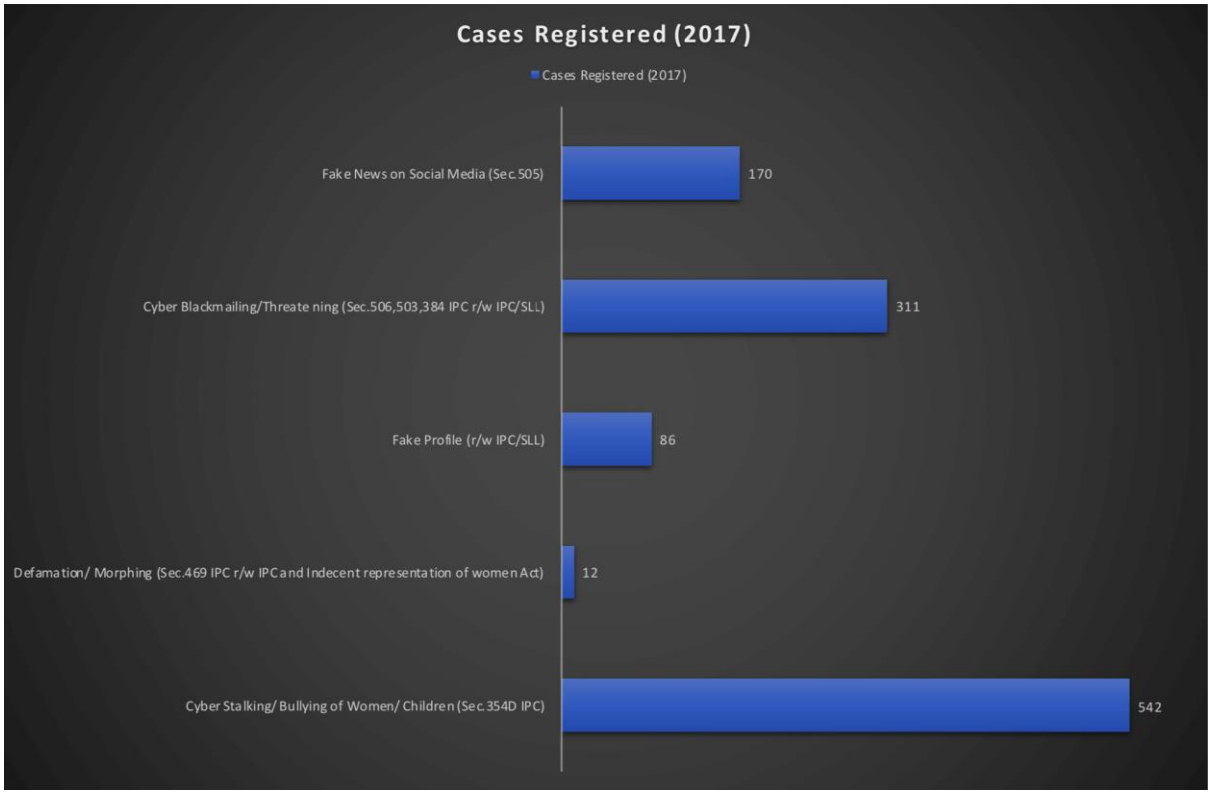


Figure 7: Incidence of Certain Cyber Crimes in 2017

C. Conclusion

Based on the data presented in this part, we can draw three definite conclusions

1. The threat of cyber espionage is the most prevalent, and a serious threat to national security emanating in cyber space.

2. The economic motive behind activities of cyber criminals demands attention from law enforcement agencies, as it has serious implications for the financial stability and economic growth.

3. The Government needs to formulate clear directions to the CERT-In and NCRB to emphasize the need for accurate, consistent and reliable data on the incidence of cyber-crimes and other malicious cyber activity which can form the basis for evidence-based policy making for

    a. the enforcement of law and order in cyberspace and

b. raise the general levels of cybersecurity awareness by widely disseminating information on the incidence of cyber-crimes to encourage reporting and self-help.

III. THE FIRST PILLAR: "SECURE" (THE NATIONAL CYBERSPACE)

In our understanding, the first pillar of the envisioned strategy, 'secure' would involve, first and foremost, to define the perimeter of actors and activities in cyberspace that need to be brought within the protection of the State. In this section, we rely on recent pronouncements and iterations of the "data sovereignty" policy by the Government as a representative indicator of strategic goals sought to be achieved through economic policies in data governance. We then attempt to map these goals in the background of applicable and relevant international legal rules and norms to examine whether certain principles can be crystallized to identify the contours of the "national cyberspace".

A. Data Sovereignty versus Cyber Sovereignty

In drafting and consultation process of the Data Protection Bill, 2018, the Government of India has stressed the need for strategic autonomy in carving out its vision for "data sovereignty". Certain policy instruments such as data localisation have been announced to translate this vision into reality. The objective of this policy is to effectively guard against the perceived "data imperialism" of foreign players in advanced technologies.[46] However, we must be cognizant of the exponential increase in attack surface area within our territorial jurisdiction that will be an inevitable consequence of data localisation if adequate measures to ensure its security are not implemented.[47]

Unarguably, irrespective of its legal classification as a public good or an individual resource owned by individual juridical persons, data resides in cyberspace, interspersed across multiple jurisdictions and international borders. Conceptually, and in reality, data sovereignty is a technologically complex, even unrealistic goal without *de jure* and *de facto* sovereignty in cyber space. This raises the issue of

[46] Vinit Goenka, Lt. Gen VM Patil, Lt. Gen Dr. DB Shekatkar, Lt. Gen Vinod Khandare, Lt. Gen Vinod Bhatia, Jayadeva Ranade and Bharat Panchal, *Data Sovereignty: The Pursuit of Supremacy* (2019), pp. xi-xx.

[47] Arindrajit Basu, Elonnai Hickok, and Aditya Singh Chawla, *The Localisation Gambit; Unpacking Policy Measures for Sovereign Control of Data in India*, Centre for Internet and Society, dated 19 March 2019, at p. 6, https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf.

whether the domain of cyberspace is amenable to the exercise of the State's sovereignty under international law? In other words, we examine whether an unsolicited intrusion into 'India's cyberspace' by foreign actors can be treated in international law, at par with violations of our sovereign territory, airspace or territorial waters?

Given the strong link between (cyber) sovereignty and the protection of the national information sphere, sovereignty, as well as its boundaries in cyberspace [is] a highly contentious issue[48] in international law. Cyber sovereignty entails that national governments have exclusive power of jurisdiction over their own national cyberspace at the level of both infrastructure and content.[49] However, one cannot merely see this as a point of international law leading to particular legal rights and entitlements *de jure*. A proclamation of *de jure* sovereignty over cyberspace would lack credibility in the absence of industrial and security capacity to ensure sovereignty *de facto.* We deal with the *de facto* aspects of industrial and security capacity as integral parts of sovereignty in cyberspace in Part III.

As countries ready themselves for conducting operations in cyberspace (including those possibly harmful), India needs to ensure a deep familiarity and constant engagement with the evolving contours of the international legal regime which continues to restrain our national security choices. This requires a nuanced understanding of existing and emergent norms under the international legal regime governing State actions during peacetime as well as in times of armed conflict. Accordingly, the following section is devoted to examining the applicable international legal rules, principles and norms that guide and restrain the scope and limitations of *de jure* state sovereignty and consequently, the spectrum of lawful State actions in cyberspace as well as available remedies when hostile or unlawful acts in cyberspace are directed at India's 'national cyberspace' by State and Non-State Actors.

---

[48] Dennis Broeders, Liisi Adamson and Rogier Creemers, *A coalition of the unwilling? Chinese and Russian Perspectives on Cyberspace*, Policy Brief 2019, The Hague Program for Cyber Norms, at p. 3, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3493600.

[49] Ibid at p. 3.

B. The International Law on Cyber Sovereignty

The international legal regime applicable to cyber operations is an amalgamation of black-letter rules of India's existing treaty obligations, basic principles enshrined in the UN Charter (Charter) and the rules and norms of customary international law (CIL). These include the principles of sovereign equality[50], the principle of non-intervention in another nation's internal affairs[51], prohibition on the use of force[52] as well as armed attacks and the inherent right of self-defence.

Over time, each of these principles has been interpreted by sovereign nations in line with their own security interests in cyberspace. There appears to be an evolving consensus among a group of states that the UN Charter in its entirety applies to cyber operations.[53] The United Kingdom[54], the United States,[55] the Netherlands[56]

[50] Article 2(1), Charter of the United Nations, 1945.

[51] Article 2(4), Charter of the United Nations, 1945.

[52] Article 2(4), Charter of the United Nations, 1945

[53] UN GGE Report (2013), https://undocs.org/A/68/98, para 19 at p.8; UN GGE Report (2015), para 24 at p.12, https://dig.watch/sites/default/files/UN%20GGE%20Report%202015%20%28A-70-174%29.pdf.

[54] Script of Attorney General Jeremy Wright QC MP's Speech at Chatham House Royal Institute for International Affairs, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

[55] Script of Brian Egan's Speech (Legal Advisor to Secretary of State, February 2016- January 2017) at Berkeley Law School, California, 10 November 2016, https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf.

[56] Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace dated 5 July 2019 with an appendix that discusses the main issues relating to international law, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

and Australia[57] have each separately declared their acceptance of these prohibitions under international law.

Certain pronouncements and interpretations of the law by international courts and tribunals, especially the International Court of Justice (ICJ) shed light on the content of these principles. We are of the opinion that these are binding on India only insofar as they relate to norms or rules of CIL. In accordance with the Statute of the International Court of Justice, decisions rendered by the Court have a binding effect only for the States that are party to the dispute.[58]

The most notable and relevant example of such an obligation, is the inherent right of self-defence of sovereign States. This principle is enshrined in Article 51 of the UN Charter and is also recognized as a norm of CIL. However, this right can be invoked only in the event of an "armed attack" directed at the State. With respect to the right to self-defence, Australia,[59] the Netherlands,[60] the United States,[61] and the United Kingdom[62], have all declared that the right can be invoked by states that are victims of cyber-operations that rise to the level of an armed-attack. But there is widespread

[57] Annex A: Australia's Position on How International Law Applies to State Conduct in Cyberspace, 2019 International Law Supplement, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/annexes.html#Annex-A.

[58] Article 59, Statute of the International Court of Justice, 1945.

[59] Annex A: Australia's Position on How International Law Applies to State Conduct in Cyberspace, 2019 International Law Supplement, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/annexes.html#Annex-A, Para 1.

[60] Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace dated 5 July 2019 with an appendix that discusses the main issues relating to international law, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, Page 8.

[61] Script of Brian Egan's Speech (Legal Advisor to Secretary of State, February 2016- January 2017) at Berkeley Law School, California, 10 November 2016, https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf.

[62] Script of Attorney General Jeremy Wright QC MP's Speech at Chatham House Royal Institute for International Affairs, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

disagreement among scholars as well as practitioners on the question of whether, in the absence of any physical damage or destruction of life or property, a cyber attack could be treated as an "armed attack" within the meaning of Article 51 of the UN Charter and under customary international law. The occurrence of such 'below-the-threshold'[63] attacks in cyberspace is not a new phenomenon, but one that India has been grappling with for over a decade now. According to the ICJ in *Certain Military and Paramilitary Activities (Nicaragua v. the United States),* whether an attack rises to the level of an "armed attack" or not is determined by its scale and effects.[64] While this judgment did not relate to cyber operations, nonetheless, it has had a significant impact on the development of the applicable law and it interpretations expressed in both editions of the Tallinn Manual.[65] We would recommend that the Secretariat take up this issue by commissioning an in-depth study of the implications of such interpretations of Article 51 of the UN Charter, as it has a significant impact on the range of legal remedies available to India in cases of State-sponsored cyber espionage.

[63] This refers to the threshold of what constitutes an 'armed attack' within the contemporary understanding and interpretation of Article 51 of the Charter of the United Nations which recognizes the inherent right of self-defence of nation-states. For a more detailed discussion, *see* Gunjan Chawla, *Respond to the Cyber Intrusion, Within Law,* THE HINDUSTAN TIMES, 14 November 2019, accessible at https://www.hindustantimes.com/analysis/respond-to-the-cyber-intrusion-within-law-opinion/story-TkUs7CAwKFEXwmWmMHkT8K.html.

[64] *Case Concerning Military And Paramilitary Activities In And Against Nicaragua (Nicaragua v. United States of America),* International Court of Justice (ICJ), 27 June 1986, Para. 195.

[65] The Tallinn Manuals are an independent, non-binding study on the applicability of existing international law to state and non-state action in cyberspace (including cyber conflicts and cyber warfare). It is the product of a group called the International Group of Experts (IGE) composed of legal scholars and practitioners with experience in cyber issues. While the Tallinn 1.0 deals with actions in cyberspace rising to the level of use of force and armed-attacks or reaching the threshold of armed conflict under international humanitarian law, Tallinn 2.0 elaborates upon the rules relating to actions in cyberspace for below-the-threshold actions in cyberspace *See* Schmitt, Michael N (Gen. ed.) (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York, United States of America: Cambridge University Press. *See also* Tallinn Manual 2.0 on The International Law Applicable to Cyber operations, 2nd edition, Michael N Schmitt (Gen. Ed.), (CUP, 2017).

Cyber operations crossing the threshold into armed conflict would be governed by international humanitarian law. There is agreement among most states that the basic principles of humanity, necessity, proportionality and distinction apply to state action in cyberspace.[66] On this question, the International Committee of the Red Cross ("ICRC") in a recent position paper has articulated its view that the international humanitarian law limits cyber operations during armed conflicts, and (military) cyber capabilities that qualify as weapons, just as it limits the use of any other weapon, means and methods of warfare in an armed conflict, whether new or old.[67]

It is also relevant to track the development of creative interpretations of the law of armed conflict currently underway in the United States, which stands in opposition to the interpretation of the law by the ICRC. In a recent paper, Michael N Schmitt, one of the principal authors of the Tallinn Manual 1.0 and Tallinn Manual 2.0, in a reconsideration of his opinion expressed in these Manuals, has argued that cyber capabilities cannot meet the definition of a weapon or means of warfare, but that cyber operations may qualify as methods of warfare.[68] Such an interpretation permits 'cyber weapons' to circumvent at least three obligations under IHL, including the requirement for legal review of weapons under Article 36 of the Geneva Conventions and taking precautions in attack.[69] Most importantly, the argument that cyber weapons cannot be classified as munitions has the consequence of depriving neutral

[66] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, United Nations General Assembly, Res. A/68/98, dated 24 June 2013, Para 28(d), https://dig.watch/sites/default/files/UN%20GGE%20Report%202015%20%28A-70-174%29.pdf.

[67] ICRC Position Paper, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

[68] Jeffrey T Biller and Michael N Schmitt, *Classification of Cyber Capabilities and Operations as Weapons, Means or Methods of Warfare,* 95 INT'L L. STUD. 179 (2019) at p. 219, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2462&context=ils.

[69] Ibid.

States of their sovereign right to refuse permission of their transportation (or in this case, transmission of weaponised cyber capabilities) through their territory.[70]

If the law presumes, in line with American interpretations, that cyber capabilities are neither weapons nor munition, it may be difficult to classify instances of cyber attacks, including cyber espionage, as "armed attacks". Thus, it is also useful to examine them through the lens of prohibitions articulated in Article 2 of the UN Charter, which offers guidance on the realm of State sovereignty. International law protects State sovereignty by the rule on prohibition of the use of force, the principle of non-intervention and the principle of sovereign equality. However, there is disagreement among states with respect to the extent of protection offered to State sovereignty under international law.

For instance, the Netherlands has stated that it endorses the "sovereignty as a rule" approach, i.e., the principle of sovereignty as an obligation by itself, separate from and complementary to the principles of prohibition on non-intervention and use of force.[71] In the Netherlands' view, a State's sovereignty may be violated by a cyber attack if the effects of the operation in question manifest on the territory of the state concerned (eg. physical damage is caused to the cyber infrastructure or any other property) or the operation interferes with or usurps its inherently governmental functions.

In contrast, the United Kingdom has refuted the "sovereignty as a rule" approach and has instead declared that there is no such rule as a matter of current international law in cyberspace.[72] They take the view that sovereignty is a *principle*, not an enforceable rule under international law. The United States has expressed similar

[70] Ibid.

[71] Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace dated 5 July 2019 with an appendix that discusses the main issues relating to international law, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, Page 2.

[72] Script of Brian Egan's Speech (Legal Advisor to Secretary of State, February 2016- January 2017) at Berkeley Law School, California, 10 November 2016, https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf.

doubts to the applicability of the "sovereignty as a rule" approach to cyberspace.[73] This divergence gains particular significance in the context of cyber-espionage, which involves malicious cyber activity stealing or gaining access to classified or sensitive data in order to obtain a tactical or commercial advantage. However, it is relevant to emphasize that espionage is not *per se* illegal under international law.

By its very nature, cyber-espionage will involve an unauthorized intrusion into the cyberspace of another nation. According to the Netherlands, a malicious cyber activity will have to constitute something more than mere intrusion into a state's cyberspace (such as causing damage, or taking over inherent state functions) in order to constitute a violation of sovereignty.[74]

Interpretations of the same rule by Russia and China stand in stark contrast to the Western interpretations outlined above, and place a much heavier emphasis on sovereignty in cyberspace. However, in doing so, Russia recognises the applicability of 'generally recognised principles of international law, international treaty obligations, as well as domestic legislations'[75]. Whereas, China emphasized 'respect for maintaining cyberspace sovereignty' as one of four basic principles articulated in its cybersecurity strategy, along with the principle of 'peaceful uses of cyberspace', 'governing cyberspace according to law' and 'coordinating network security and development'.[76] China also envisions playing a leading role in supporting the United Nations to promote the development of universally accepted international rules on cyber space, cyberspace international counter-terrorism conventions, etc. as one of

[73] Gary P. Corn and Robert Taylor, *Sovereignty in the Age of Cyber*, American Society of International Law, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/02314DFCFE00BC901C95FA6036F8CC70/S2398772317000575a.pdf/sovereignty_in_the_age_of_cyber.pdf.

[74] Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace dated 5 July 2019 with an appendix that discusses the main issues relating to international law, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, Page 2.

[75] Information Security Doctrine of the Russian Federation.

[76]Cyber Security Strategy 2017, Cyberspace Administration of China.

nine strategic tasks.[77]

Currently, several parallel processes are underway, within and outside the aegis of the United Nations for building consensus on universal norms that may guide or govern responsible State behaviour in cyberspace. We recommend that India should actively monitor developments in these ongoing processes, and be prepared to take an active part in their formation and formulation. This would enable us to protect our strategic interests in cyber space from external pressures, and prevent the legitimizing of imperialist interventions in international law. In doing so, we must also vigilantly guard our interests by ensuring representation and active participation in multilateral and multi-stakeholder fora at the international level.

Even beyond UN led efforts, States are also clarifying their own approaches to *how* international law is applicable in cyberspace. We recommend that the Secretariat should consider the benefits of similarly articulating its own position on international legal principles in cyberspace. Silence from states on these issues "could lead to unpredictability in the cyber realm, where States may be left guessing about each other's views on the applicable legal framework" and this "uncertainty could give rise to misperceptions and miscalculations by States, potentially leading to escalation and, in the worst case, conflict."[78]

In articulating its stance on how international law applies in cyberspace, we would also recommend for the consideration of the Secretariat, espousing the principle of peaceful uses of cyberspace. It is most consistent with protecting our national interests in cyber space as well as India's international legal obligations, including the principle of peaceful uses of outer space contained in the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies, 1967 ('the Outer Space Treaty'). However, it is relevant to point out that the framework of the Outer Space Treaty is based on the principle that outer space is not subject to national appropriation by

[77] Ibid.

[78] Script of Brian Egan's Speech (Legal Advisor to Secretary of State, February 2016- January 2017) at Berkeley Law School, California, 10 November 2016, https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf.

claim of sovereignty, by means of use or occupation, or by any other means, but recognizes that outer space shall be free for exploration and use by all States.[79] Further research and study in this domain would also be advisable.

C. Review of Major Ongoing Norm-Building Efforts for Responsible State Behaviour in Cyberspace

1. Multilateral Processes

i. **United Nations Group of Governmental Experts (UNGGE):** The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) is a UN-mandated working group in the field of information security. Six working groups have been established so far under its aegis and the Group consists of states selected on the basis of equitable geographical distribution. India has been a nominated member of five GGEs, barring the one in 2015. The UN GGE's 2015 report was adopted by the UN General Assembly in Resolution 70/237.[80] The UN GGE can be credited with two major achievements – (1) outlining the global agenda for cyberspace and (2) introducing the principle that international law applies to the digital space.[81] The UN GGE is currently undergoing its sixth session (2019) and India is one of the member states.[82]

---

[79] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, United Nations Office of Outer Space Affairs, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html.

[80] Resolution adopted by the General Assembly on 23 December 2015, United Nations General Assembly, A/RES/70/237, https://undocs.org/A/RES/70/237.

[81] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, United Nations General Assembly, Res. A/68/98, dated 24 June 2013, https://undocs.org/A/68/98.

[82] United Nations Office for Disarmament Affairs, Group of Governmental Experts, https://www.un.org/disarmament/group-of-governmental-experts/.

ii. **Open Ended Working Group (OEWG)**: The OEWG is also a UN-mandated working group established by UNGA resolution 73/27.[83] According to the resolution, the substantive issues for discussion are (1) existing and potential threats, (2) international law, (3) rules, norms and principles, (4) regular institutional dialogue, (5) confidence building measures and (6) capacity building. The OEWG started its work in 3-4 June 2019 with representation from more than 100 states. It recently held an inter-sessional consultative session from 2 - 4 December 2019. It should report to the UNGA in its 75th Session from 15-30 September 2020. India also voted in favour of the resolution establishing the OEWG.[84]

2. Multi-Stakeholder Efforts

i. **Global Commission on Stability of Cyberspace (GCSC):** The GCSC was established as a result of the Global Conference on Cyberspace held in The Netherlands in 2015.[85] The main partners of the GCSC are the Government of the Netherlands, Microsoft Corporation, the Government of Singapore and the Hague Centre for Strategic Studies, among others.[86] The GCSC recently released its final report containing eight norms designed to ensure the stability of cyberspace.[87] Significantly, one of the norms identified by the GCSC was that states

[83] Resolution adopted by the General Assembly on 5 December 2018, United Nations General Assembly A/RES/73/27, https://undocs.org/A/RES/73/27.

[84] Official Records, United Nations General Assembly, A/70/PV.82, p. 12, https://undocs.org/en/A/70/PV.82.

[85] GIP Digital Watch Observatory, *Global Commission on the Stability of Cyberspace*, https://dig.watch/actors/global-commission-stability-cyberspace.

[86] Ibid.

[87] Global Commission on Stability of Cyberspace, *Advancing Cyberstability Final Report*, (November 2019), https://cyberstability.org/wp-content/uploads/2019/11/Digital-GCSC-Final-Report-Nov-2019_LowRes.pdf.

and non-state actors should not knowingly damage the "public core of the internet".[88] There was no formal representation from states.

ii. **Paris Call for Trust and Security in Cyberspace**: Led by the French Government, the Paris Call is a non-binding consensus statement issued on November 12, 2018, on the growing concerns relating to cyber-threats.[89] With more than 400 signatories (currently)[90], among which 64 are nation-states, the Paris Call reflected consensus on the importance of a peaceful cyberspace, the relevance of international law and responsible behaviour by governments, and the threat posed by malicious cyber activities.[91] The statement also contained an agreement on key principles such as the need to strengthen international capacity and to prevent and recover from malicious activities. Several major corporations including Microsoft and Siemens, along with non-governmental organizations / civil society such as Chatham House, the Carnegie Endowment for International Peace and the Internet Society have also supported the Paris Call.[92]

3. Private Sector Initiatives

i. **Tech Accords**: Led by Microsoft, the Cybersecurity Tech Accords is a public commitment among more than 80 global companies which oversee important aspects of the world's communication and information infrastructure, to protect and empower civilians online and

[88] Ibid, p. 21.

[89] GIP Digital Watch Observatory, *Paris Call for Trust and Security in Cyberspace*, https://dig.watch/instruments/cybersecurity-paris-call-12-november-2018-trust-and-security-cyberspace.

[90] The Supporters, Paris Call, https://pariscall.international/en/supporters.

[91] Paris Call, https://pariscall.international/en/call.

[92] The Supporters, Paris Call, https://pariscall.international/en/supporters.

to improve the security, stability and resilience of cyberspace.[93] The four key pillars identified in the Tech Accords are (1) Stronger Defence, (2) No Offense, (3) Capacity Building and (4) Collective Action.[94]

ii. **Digital Geneva Convention**: Again led by Microsoft, and recognizing the importance played by major technology companies in cyberspace, in April 2018, more than 30 companies signed the Digital Geneva Convention committing to never take part in cyber-attacks against individuals and businesses.[95] Facebook, Microsoft, Arm and Trend Micro were some of the companies that took the pledge, while Google, Amazon and Apple are not signatories.[96]

iii. **Charter of Trust**: In 2018, Siemens and eight partners launched the Charter of Trust at the Munich Security Conference which provides a set of common principles designed to reduce cyber-risk broadly.[97] Significantly, the Charter of Trust places emphasis on the security of digital supply chains.[98]

---

[93] Brad Smith, *34 companies stand for cybersecurity with a tech accord*, Microsoft On the Issues, https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/,; also see Tech Accord, https://cybertechaccord.org/about/.

[94] Tech Accord, https://cybertechaccord.org/accord/,.

[95] Alex Hern, *Facebook among tech firms to sign 'Digital Geneva Convention'*, The Guardian, d,ated 18 April 2018 https://www.theguardian.com/technology/2018/apr/18/tech-firms-including-facebook-sign-up-to-digital-geneva-convention.

[96] Alex Hern, *Facebook among tech firms to sign 'Digital Geneva Convention'*, The Guardian, dated 18 April 2018, https://www.theguardian.com/technology/2018/apr/18/tech-firms-including-facebook-sign-up-to-digital-geneva-convention.

[97] Joe Kaeser, How Siemens' Charter of Trust Aims to Improve Industrial Security, IoT World, dated 16 February 2018, https://www.iotworldtoday.com/2018/02/16/how-siemens-charter-trust-aims-improve-industrial-security/

[98] Ibid.

D. The Domestic Law and Policy on Cyber Sovereignty

Apart from articulating its own stand on international legal issues, India must navigate the global norm-making processes in a manner that aligns with its own domestic law and policy. We are mindful of India's recent proposed data protection law which seeks to promote a free and fair digital economy[99] while at the same time reflects a data-sovereignty approach,[100] with certain data localisation requirements to address issues of law enforcement access to data.[101]

This approach puts India squarely in the middle of a global divide on the approach to data management and protection. The G7 and EU countries, led by the United States, advocate a global internet and data model which is free-flowing and is controlled largely by market forces, whereas countries such as Russia, Iran and China advocate a restricted, data-sovereignty approach to enable themselves to reduce and control cyber-crime, take advantage of their digital economies, etc.[102] India can take this opportunity to find a middle ground and bridge two seemingly divergent approaches in the norm-making process, while at the same time protecting and promoting its interests of ensuring maximisation of the benefits of its burgeoning digital economy, as well as protecting the constitutional rights of its citizens online.

For the purposes of contemplating whether a coordinated State response (beyond the normal procedures of the domestic criminal justice system to prosecute cyber crimes) to any malicious cyber activity is warranted and permissible, we must be

---

[99] Preamble, Data Data Protection Bill 2019, accessible at https://www.medianama.com/wp-content/uploads/Personal-Data-Protection-Bill-2019.pdf, last accessed on 27 December 2019.

[100] Country's Data Sovereignty Cannot Be Compromised: Ravi Shankar Prasad on Data Localisation, Kritti Bhalla, Inc42, dated 23 September 2019, accessible at https://inc42.com/buzz/countrys-data-sovereignty-cannot-be-compromised-ravi-shankar-prasad-on-data-localisation/, last accessed on 27 December 2019.

[101] Clause 34, Data Protection Bill 2019, accessible at https://www.medianama.com/wp-content/uploads/Personal-Data-Protection-Bill-2019.pdf, last accessed on 27 December 2019.

[102] Breaking Down the Vote on Russia's New Cybercrime Resolution at the UN, Justin Sherman and Robert Morgus, dated 19 November 2018, accessible at https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/breaking-down-vote-russias-new-cybercrime-resolution-un/, last accessed on 27 December 2019.

aware of the constraints operational under international law, and recognize that cyber espionage remains the biggest threat to the country's information security.

It is relevant to highlight that even though (cyber) espionage, is not *per se* illegal under international law, there are several provisions under domestic law to protect the confidentiality and integrity of sensitive Government data. For instance, penal provisions under the IT Act, 2000 prohibit unauthorised access to protected computer systems.[103] Similarly, espionage, or spying remains a crime punishable under the Official Secrets Act, 1923, but may need to be amended to re-focus on the technological challenges in ensuring network security and protecting classified and sensitive information.

In this regard, we submit that the Secretariat should consider demarcating the contours of "the sovereign cyberspace", as a narrower subset of the broader realm of "the national cyberspace", which remains and is most likely to remain as layer permeable to foreign/external actors in the networked economy.

However, any intrusion into or attack via cyberspace on this narrowly defined realm of 'the sovereign cyberspace' from a foreign source could be legitimately treated as a violation of the State's sovereignty or the international legal principle of non-intervention with utmost urgency and seriousness. This perimeter should include (1) defence communications and operational networks, (2) security of the intra-government communication networks (3) security of classified and privileged information within government ministries, departments and/or agencies that form part of the cybersecurity architecture, including critical data which may be notified under Section 33(2) of the Personal Data Protection Bill, 2019.

Since the promulgation and notification of the Information Technology (Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2014, CII falls within the purview of the National Critical Information Infrastructure Protection Commission (NCIIPC). However, Rule 3(4) excludes systems notified by the Ministry of Defence (MoD) as critical information infrastructure**.** To enable this legally, (1), (2) and (3) as mentioned above ought to be notified by the Ministry of Defence as such, and explicitly entrusted to the newly-

[103] Section 70, Information Technology Act, 2000.

constituted Defence Cyber Agency (DCyA) for appropriate action and protective measures with appropriate directions.[104] Along with defining the contours of cyberspace the protection of which the Government's conventional security apparatus ought to concern itself, this would also allow for a clearer demarcation of responsibilities between first responders within the military (DCyA) and civilian sectors (NCIIPC and CERT-In). We delve deeper into institutional frameworks and how they can be strengthened in Part IV.

This narrow realm of the 'sovereign cyberspace' would be notionally surrounded and supported by a larger perimeter of a 'sovereign-protected cyberspace' (see Figure 7) of which, critical information infrastructure (CII) is the main component. This domain is distinct from, but interlinked with "the sovereign cyberspace", as well as the national cyberspace at large, as it is largely run and controlled by private sector corporations.

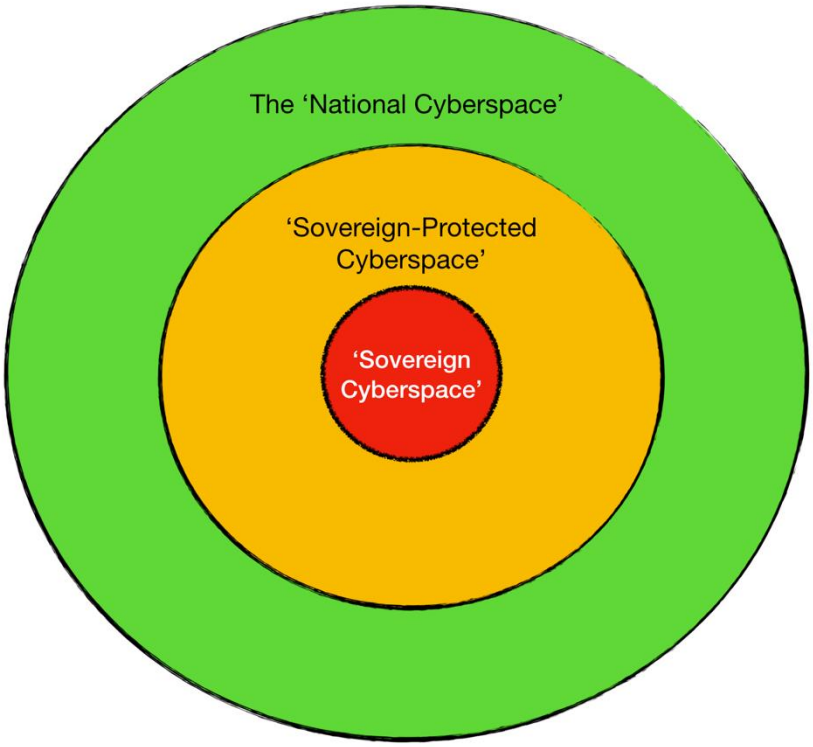


Figure 7: A Visualization of the 'National Cyberspace'

[104] Gunjan Chawla, *Defence Cyber Agency-II: Balancing Constitutional Constraints and covert Ops*, MEDIANAMA, 4 October 2019, https://www.medianama.com/2019/10/223-india-defence-cyber-agency-part-2/.

Our conceptualisation of the sovereign cyberspace, the sovereign-protected cyberspace and the national cyberspace can be visualised as a set of concentric circles, with increasing levels of integration with the global network as one approaches the periphery, or what the GCSC calls the 'public core of the internet'.

However, this narrow view of the 'sovereign cyberspace' does not imply that the cybersecurity of the rest of the nation, or the broader 'national cyberspace' that is interlinked and even integrated with the global economy, would be left entirely to the individual. Indeed, there is a pressing need to engage in rapid and effective measures to make the population at large "cyber-aware". However, until we can achieve universal digital/cybersecurity literacy, we may place reliance on the Government's conceptualisation of data as a "public good". We submit that irrespective of its classification as a public or private good, the *security* of this data, and cyberspace at large, is a public good. Accordingly, we submit for consideration by the Secretariat, endorsement of the principle of Common but Differentiated Responsibility (CBDR) to govern the apportionment of roles and responsibilities in responding to cyber security incidents. We elaborate on this principle in the following section, and further in Part V of this paper.

E. The Cybersecurity Implications of Data as a Public Good in the National Cyberspace

In 2019, two iterations of the draft national e-commerce policy (second one christened with the theme "India's Data for India's Development") were put out by the Department for Promotion of Industry and Internal Trade (DPIIT) under the Ministry of Commerce.[105] These endorsed certain concepts such as "community data"[106] – data is viewed as a "societal commons" or a "national resource", where the undefined "community has rights to access the data but the Government has

[105] Amber Sinha and Arindrajit Basu, *The Politics of India's Data Protection Ecosystem,* Economic and Political Weekly, 2 January 2019, https://www.epw.in/engage/article/politics-indias-data-protection-ecosystem.

[106] Draft National E-Commerce Policy 2019 "India's Data for India's Development", 23 February 2019, at pp. 6, 17, https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf.

overriding control to utilize the data for welfare purposes.[107] Notwithstanding the apparent ambiguity in these concepts, they resonate in and are amplified by Chapter 4 of the Economic Survey released by the Ministry of Finance in July 2019, which also conceptualised data as a "public good".

Drawing inspiration from the principles enshrined in the Rio Declaration of 1992 to govern "global commons" such as the high seas, Antarctica etc. **we are of the view that a notion of data, or cyberspace as "national commons" should include within it, the principle of Common But Differentiated Responsibility (CBDR) between multiple stakeholders for tackling malicious actors and threats in cyber space.** Admittedly, the principle originated in international environmental law, but we believe that in the interest of (1) bridging the digital divide and integrating the next half billion of the population into the networked economy and (2) identifying equitable principles to underpin the governance of cyberspace in India, **CBDR is useful to ensure that the most cyber-capable stakeholders are also the ones held most responsible for ensuring peace, stability and security in cyberspace**. Indeed, the importance of cybersecurity in ensuring that levels of economic development achieved by economies like India remain sustainable cannot be over emphasized.

The concept of CBDR was enshrined as Principle 7 of the Rio Declaration at the first Rio Earth Summit in 1992.[108] The declaration states:

> "In view of the different contributions to [to environmental degradation], States have common but differentiated responsibilities. The developed countries acknowledge the responsibility that they bear in the international pursuit of sustainable development in view of the pressures their societies place on the global environment and of the technologies and financial resources they command."

---

[107] Arindrajit Basu, *India's Role in Global cyber Policy Formulation*, The Lawfare Blog, 7 November 2019, https://www.lawfareblog.com/indias-role-global-cyber-policy-formulation.

[108] Rio Declaration on Environment and Development, 1992, https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_CONF.151_26_Vol.I_Declaration.pdf

Similar language exists in the UN Framework Convention on Climate Change (UNFCCC), which states that parties should act to protect the climate system "on the basis of equality and in accordance with their common but differentiated responsibilities and respective capabilities."[109] The principle of CBDR could also potentially be used to ground public private partnerships, technology, knowledge and information sharing, as well as the pooling of financial resources in the face of hard budget constraints, which we examine in Part V. Such an approach would also remind us to be cognizant of the Digital Divide, and encourage us to work towards closing this yawning gap, in order that we may work towards common, shared responsibilities for all stakeholders. We delve deeper into the dynamic in Part V of this submission.

[109] Article 3(1), United Nations Framework Convention on Climate Change, 1992.

IV. THE SECOND PILLAR: "STRENGTHEN" (STRUCTURES, PEOPLE, PROCESSES AND CAPABILITIES)

The scale, effects and sophistication of cyber threats are rapidly evolving and malicious actors in cyberspace are constantly upgrading their cyber capabilities through innovation even as experts struggle to develop new ways to neutralize their effects. In this constantly evolving threat landscape, where a Digital India aspires for the adoption and integration of new, cutting-edge and emerging technologies, building cyber defences and strengthening cybersecurity must be a continuous process. It should be geared towards achieving universal levels of not merely digital literacy, but cybersecurity literacy and awareness. This goal can only be adequately and consistently achieved by strengthening existing Government institutions engaged in cyber security.

A. Institutions and Initiatives

1. The Architecture of Cybersecurity Institutions

Based on publicly available data on Ministry websites and the allocation of Government business among various Ministries and Departments, we have compiled an infographic to outline the architecture of institutions that play a direct role in national efforts to ensure cybersecurity (see Figure 8).

Specific departments under MeitY have not been highlighted, except CERT-In, since the Ministry as a whole plays a crucial role in laying down procedures, standards and guidelines for internet governance at large. Detailed organograms displaying the structure of Ministerial Departments that contribute to the overall cybersecurity efforts of the Government have been appended as **Annexure 'B**' to this submission, wherein the Departments that are most relevant to cybersecurity have been identified.

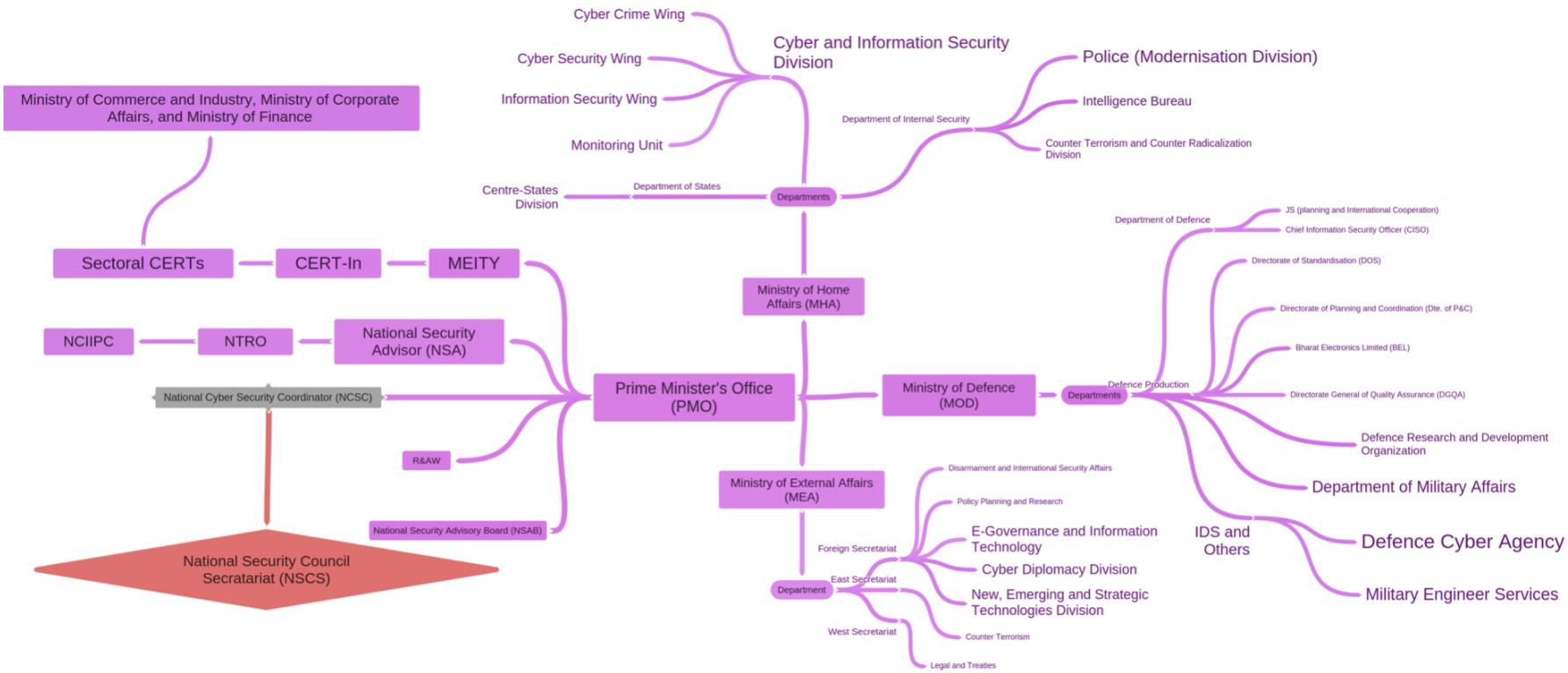


Figure 8: The Architecture of Cyber Security Institutions and Agencies in India

We submit that the Chief Information Security Officers (CISOs) of all Ministries should be brought in direct contact with and submit periodic reports on the state of information security in their respective Ministries to the office of the National Cyber Security Coordinator (NCSC). However, the role and authority of the NCSC in relation to the National Security Advisor (NSA) requires some clarification.

The CISOs of the Ministry of Defence, Ministry of External Affairs, Ministry of Home Affairs, MeitY, as well as the Department of Telecom (DoT) under the Ministry of Communications play an especially important role in conceptualization of India's 'sovereign cyberspace' (see Figure 7). The CISOs of these Departments should be the first line of defence against cyber espionage and foreign surveillance of the State's core activities and inherently governmental functions, and any disruptions that may arise therefrom. They would also be expected to play an important role in laying down standards and guidelines as well as the formulation of cyber and information security policies for various Ministries.

1. Protection of Critical Information Infrastructure

Critical Information Infrastructure (CII) is the most important component within our conceptualization of the realm of the 'sovereign-protected cyberspace' (see Figure7). CII is defined under Section 70 of the Information Technology Act, 2000, as "*the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety*". This provision also permits the appropriate Government to declare any computer system which affects the facility of CII to be a protected system by notification in the Official Gazette. Pursuant to its powers under Section 70A of the IT Act, 2000, the National Critical Information Infrastructure Protection Centre (NCIIPC) was established by a Gazette Notification on 16 January 2014.[110]

Since its establishment, the NCIIPC has issued certain guidelines, including Guidelines for the Protection of CII[111] as well as roles and responsibilities of

[110] Government of India, National Critical Information Infrastructure Protection Centre (A Unit of National Technical Research Organization), https://nciipc.gov.in/.

[111] Guidelines for the Protection of Critical Information Infrastructure, National Critical Information Infrastructure Protection Centre, Government of India, https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf.

CISOs[112] in 2015. In 2017, the NCIIPC also formulated certain Standard Operating Procedures (SOPs) for (1) auditing of CIIs/protected systems by private/government organisation[113] (2) incident response and (3) identification of Public Private Partnership entities for partnership with NCIIPC[114], which also contains a formulation of training requirements along with guidelines for conducting training. In 2018, it also notified Rules for Information Security Practices and Procedures for Protected Systems. Most recently in 2019, the NCIIPC issued Guidelines for Identification of Critical Information Infrastructure.[115]

The NCIIPC functions as a unit of the National Technical Research Organisation (NTRO), which functions directly under the authority of the Prime Minister's Office (PMO). While the NTRO plays an extremely important role in the network of intelligence agencies in India, it is also important to recognize that a substantial portion of the systems protected under the mandate of the NCIIPC falls under civilian infrastructure in the transport, communications, power and banking sectors. All of these sectors primarily perform civilian functions, or have a much larger presence of private players. The CII of Defence and Strategic Enterprises undoubtedly demands a higher degree of inputs from intelligence agencies, and can be retained within this hierarchy.

However, for **those sectors that have a bigger presence of the private sector or perform primarily civilian functions, in view of their centrality to sustaining and promoting India's economic growth and development should be brought within the ambit of the Cyber and Information Security Division under the Ministry of Home Affairs to allow for more open and transparent public-private**

[112] Suggested Roles and Responsibilities of CISO (2015), National Critical Information Infrastructure Protection Centre, Government of India, https://nciipc.gov.in/documents/Roles_Responsibilities-CISO.pdf

[113] Standard Operating Procedure, Auditing of CIIs/Protected Systems by Private/Government Organisation (2017), National Critical Information Infrastructure Protection Centre, Government of India, https://nciipc.gov.in/documents/SOP-CII_Audit.pdf.

[114] Standard Operating Procedure, Identification of PPP (Public-Private-Partnership) entities for partnership with NCIIPC and formulation of training requirements along-with guidelines for conducting training, National Critical Information Infrastructure Protection Centre, Government of India, https://nciipc.gov.in/documents/SOP-PPP.pdf

[115] Standard Operating Procedure, Identification of PPP (Public-Private-Partnership) entities for partnership with NCIIPC and formulation of training requirements along-with guidelines for conducting training, National Critical Information Infrastructure Protection Centre, Government of India, https://nciipc.gov.in/documents/Guidelines_for_Identification_of_CII.pdf

partnerships. The current status of the CII for these sectors falling under the NCIIPC creates transparency issues, given that the NCIIPC is under the ambit of an intelligence agency, i.e., the NTRO. In the alternative, they could also be integrated with sectoral CERTs being set up through CERT-In under MeitY.

2. The Digital India Initiative

The Digital India programme is a flagship programme of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy.[116] Launched in 2015, it is centred on three key areas - (a) Digital Infrastructure as a core utility to every citizen, (b) governance and services on demand and (c) digital empowerment of citizens.[117] The Digital India programme was initiated on the back of the National e-Governance Plan 2006, which intended to bring all government services to citizens through electronic means[118], and supplement the National e-Governance Plan.[119]

The Digital India initiative has led to the creation of certain other initiatives such as the Cyber Swacchta Kendra (Botnet Cleaning and Malware Analysis Centre) run by CERT-In to enhance the cyber security of Digital India's IT infrastructure by providing information on botnet/malware threats and suggesting remedial measures,[120] as well as the Cyber Surakshit Bharat which is aimed at spreading awareness, building capacity as well as enabling government departments on steps that need to be taken to create a cyber resilient IT setup.[121]

Other major efforts undertaken by the Government to achieve these goals include formulating Cyber Crisis Management Plans for countering cyber threats and cyber

[116] Government of India, Ministry of Electronics & Information Technology, Digital India, Introduction, https://digitalindia.gov.in/content/introduction.

[117] Government of India, Ministry of Electronics & Information Technology, Digital India, Vision and Vision Areas, https://digitalindia.gov.in/content/vision-and-vision-areas.

[118] Government of India, Ministry of Electronics & Information Technology, National e-Governance Plan, https://meity.gov.in/divisions/national-e-governance-plan.

[119] Government of India, Ministry of Electronics & Information Technology, Digital India, Introduction, https://digitalindia.gov.in/content/introduction.

[120] Government of India, Ministry of Electronics & Information Technology, CERT-In, About Us, https://www.cyberswachhtakendra.gov.in/about.html.

[121] Government of India, Ministry of Electronics & Information Technology, Cyber Surakshit Bharat, https://meity.gov.in/writereaddata/files/Cyber_Surakshit_Bharat_Programme.pdf.

terrorism[122], setting up of the National Cyber Coordination Centre (NCCC), the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Defence Cyber Agency (DCyA).

3. Public Private Partnerships

Public-Private Partnership (PPP) models for cybersecurity already exist in countries such as the USA, UK, Australia, Sweden, Switzerland, Germany, France, Estonia.[123] Our analysis of the cybersecurity strategies of 16 countries indicates that all of them have charted out goals and objectives for developing and integrating the cybersecurity of their private sector with the national cyber security.[124]

The Digital India and Make in India programmes have already jump-started several efforts in this regard. Digital India's Cyber Surakshit Bharat, a collaboration between MeitY and a consortium including Microsoft, Intel, WIPRO, Redhat and Dimension Data is an attempt to leverage the IT industry's expertise in cybersecurity.[125] Under MeitY's Information Security and Awareness program, Microsoft together with the Data Security Council of India (DSCI) has launched Project Cyber Shikshaa (2018) for skilling women engineering graduates in the niche field of Cyber Security.[126]

The Ministry of Home Affairs has also announced the setting up of a Joint Working Group (JWG) for Public Private Partnership on cyber security at the National Security Council Secretariat working on the following areas:

- Setting up of Information Sharing and Analysis Centres (ISACs) in critical sectors like Banking, Telecommunications and Power.
- Establishment of Centres of Excellence (CoEs) on Policy Research, Standards, Audit.

---

[122] Press Release dated 20 March 2018, Ministry of Home Affairs, Government of India, https://pib.gov.in/newsite/PrintRelease.aspx?relid=177722.

[123] ENISA, Cooperative Models for Effective Public Private Partnerships Desktop Research Report, 2011, https://www.enisa.europa.eu/publications/copy_of_desktop-reserach-on-public-private-partnerships/at_download/fullReport.

[124] See Annexure A to the Dossier.

[125] Cyber Surakshit Bharat, Microsoft, https://www.microsoft.com/en-in/about/cybersecurity-surakshit-bharat.aspx.

[126] Cyber Shikshaa, Digital India, https://www.dsci.in/cyber-shikshaa/.

- Capacity building for law enforcement agencies and cyber forensics.
- Establishment testing labs for telecom and IT equipment under PPP model.[127]

India has a strong network of industry bodies and associations which must be tapped into by the government to lead cybersecurity skilling. Existing bodies such as FICCI, ASSOCHAM, CII, IAMAI etc. with their extensive outreach are capable of galvanizing different parts of the private sector to contribute to and benefit from cybersecurity skilling. This in essence involves the repetition and proliferation of the successes of projects like Cyber Shikshaa and Cyber Surakshit Bharat on a more frequent and larger scale.

B. Processes

1. Cyber Incident Response and Crisis Management

The NCIIPC Standard Operating Procedure (SOP) on Incident Response details the protocols to be followed by stakeholders in case of a cyber incident involving protected systems in CII. As we pointed out in parts III and IV, while several sectors including power, energy and transportation have been identified as critical information infrastructure,[128] responsibility for sectors such as defence and intelligence agencies lies with the MoD/DRDO, and not the NCIIPC. The NCIIPC should also be sharing threat and post-incident response information with the DRDO since the same threats to other CII can be relevant for these sectors as well, and prompt further research in developing cutting edge technologies for India's cyber defences. While the SOP mentions sharing information with CERT-In,[129] it is silent on this aspect.

In their present form, the SOP mandates reporting of any incident across the country to the NCIIPC Incident Response (IR) team, which then, depending on whether the

[127] Press Release dated 20 March 2018, Ministry of Home Affairs, Government of India, https://pib.gov.in/newsite/PrintRelease.aspx?relid=177722.

[128] Government of India, National Critical Information Infrastructure Protection Centre (A Unit of National Technical Research Organization), https://nciipc.gov.in/.

[129] Para 7.3, Standard Operating Procedure, Incident Response, National Critical Information Infrastructure Protection Centre, Government of India, https://nciipc.gov.in/documents/SOP-Incident_Response.pdf.

reporting organization is Delhi-based or not, will provide local assistance.[130] Given the frequency and magnitude of cyber incidents in India on a daily basis, this is not logistically sustainable. We submit for the consideration of the Secretariat, the establishment of State level IR Teams under the authority of State Governments, but who will be bound to report incident response and mitigation measure to the national level IR team at the NCIIPC. This will enable prompt and efficient access to remedies for cyber incidents involving CII victims, as well as widen the NCIIPC's net for incident response and / or assistance.

At the national level, CERT-In has also formulated a 'Cyber Crisis Management Plan'[131] (CCMP) for countering cyber attacks and cyber terrorism. The CCMP creates a four-tiered classification of cyber incidents, depending on the scale, effects and intended victim of the cyber incident. These are

i. Level 1 (Guarded) threats that affect only individual organisations;

ii. Level 2 (Elevated) threats that affect multiple organisations;

iii. Level 3 (Heightened) threats that affect an entire State or multiple States as attacks on infrastructure of a critical sector; and

iv. Level 4 (Serious) threats that affect the entire nation by cyber attacks on infrastructure of critical sector and Government across the nation.

Affected organizations are expected to notify CERT-In, NTRO/MoD, and the Integrated Defence Staff's Defence Information Assurance Research Agency (DIARA) for Level 1 and Level 2 threats. The reporting and recovery procedures are indicated separately for each category. In the case of Level 3 and Level 4 cyber threats, the affected organizations and Ministerial Departments are expected to report to the National Crisis Management Committee (NCMC), in addition to CERT-In, NTRO/MoD and IDS (DIARA). It also envisions that all Ministries and Departments of the Union and state governments and Union territories to draw up

[130] Para 6, Standard Operating Procedure, Incident Response, National Critical Information Infrastructure Protection Centre, Government of India, https://nciipc.gov.in/documents/SOP-Incident_Response.pdf.

[131] Government of India, Ministry of Electronics & Information Technology, CERT-In, Cyber Crisis Management Plan, https://www.cert-in.org.in/.

their own CCMP. Progress on this front ought to be regularly monitored and reported to the office of the NCSC.

2. Vulnerabilities Discovery and Disclosure

CERT-In defines a "vulnerability" as a "feature or bug in a system or program which enables an attacker to bypass security measures".[132] In other words, vulnerabilities are weaknesses that can be exploited by malicious actors to perform unauthorized actions within a computer system. Reported vulnerabilities enable the developer to fix the vulnerability by way of a "patch" or an update which betters security.

In India, the only government entities that vulnerabilities can be reported to are CERT-In, NCIIPC, NIC-CERT and the Kerala Police Cyberdome.[133] Budget documents indicate that budgetary allocations were earmarked for a CERT under the Department of Telecom (T-CERT) in 2017-18[134], and news reports[135] are the only form of publicly available data on this. We suggest that information on its functioning and activities be released in the public domain by the DoT.

Each CERT has a separate form for notifying a vulnerability with separate requirements.[136] This system has also been criticized for a lack of accessibility and transparency with no incentives such as recognition or reward.[137] Additionally,

---

[132] Government of India, Ministry of Electronics & Information Technology, CERT-In, Vulnerability Reporting, https://www.cert-in.org.in/VulnerIncident.jsp.

[133] The Centre for Internet & Society, *Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India*, 23 January 2019, https://cis-india.org/internet-governance/resources/Improving%20the%20Processes%20for%20Disclosing%20Security%20Vulnerabilities%20to%20Government%20Entities%20in%20India.pdf.

[134] Government of India, Ministry of Communications, Department of Telecom, Notes on Demands for Grants 2017-18, Demand No. 14, https://www.indiabudget.gov.in/budget2017-2018/ub2017-18/eb/sbe14.pdf; See Also Union Budget Notes on Demands for Grants 2018-19, Demand No. 14, https://www.indiabudget.gov.in/budget2018-2019/ub2018-19/eb/sbe14.pdf; and Union Budget Notes on Demands for Grants 2019-20, Demand No. 13, https://www.indiabudget.gov.in/doc/eb/sbe13.pdf.

[135] Rishi Ranjan Kala, *Cybersecurity: Telecom Sector To Have Own Emergency Response Team*, Financial Express, dated 30 March 2018, https://www.financialexpress.com/industry/technology/cyber-security-telecom-sector-set-to-have-own-emergency-response-team/1115627/.

[136] The Centre for Internet & Society, *Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India*, 23 January 2019, https://cis-india.org/internet-governance/resources/Improving%20the%20Processes%20for%20Disclosing%20Security%20Vulnerabilities%20to%20Government%20Entities%20in%20India.pdf.

[137] The Centre for Internet & Society, *Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India*, 23 January 2019, https://cis-india.org/internet-

research indicates that certain provisions and definitions of offences under the IT Act, 2000 pose a hinderance to cyber security researchers and white-hat hackers acting in good faith.[138] Accordingly, we recommend that the Secretariat should engage in further study of these provisions, with a view to introducing amendments that may encourage and incentivise independent cyber security researchers to responsibly discover and report vulnerabilities and supplement the efforts of Government agencies.

Researching vulnerabilities forms a large part of tech companies' focus. For instance, Google's Project Zero, consisting of a team of security analyst employees, is tasked with finding zero-day vulnerabilities.[139] Recognizing their importance, countries are hastening to establish vulnerability disclosure regimes. China, for instance, has proposed rules that will require reporting a vulnerability first to the government before the vendor.[140] This has been criticized as potentially delaying vendor-notification, which in turn delays fixing the vulnerability, rendering it open for exploitation.[141]

3. Reporting and Investigation of Cyber Crimes

According to a press release issued by the Ministry of Home Affairs in July 2019, the Government has indicated that it has taken or is in the process of taking several steps to address the issue of cybercrimes in India.[142] These include chiefly, among other measures, launching an online cybercrime portal, (www.cybercrime.gov.in) to enable complainants to report crimes against women and children as well as the

---

governance/resources/Improving%20the%20Processes%20for%20Disclosing%20Security%20Vulnerabilities%20to%20Government%20Entities%20in%20India.pdf.

[138] The Centre for Internet & Society, *Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India*, 23 January 2019, https://cis-india.org/internet-governance/resources/Improving%20the%20Processes%20for%20Disclosing%20Security%20Vulnerabilities%20to%20Government%20Entities%20in%20India.pdf.

[139] Andy Greenberg, *Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers*, Wired, dated 15 July 2014, https://www.wired.com/2014/07/google-project-zero/.

[140] Dave Yin, *Making Reference to 'State Secrets,' China Moves to Restrict Vulnerability Disclosures*, , CX Tech, dated 21 November 2019, https://www.caixinglobal.com/2019-11-21/making-reference-to-state-secrets-china-moves-to-restrict-vulnerability-disclosures-101485876.html.

[141] Chris Udemans, *China Working On Rules To Regulate Vulnerability Disclosures*, TechNode, dated 22 November 2019, https://technode.com/2019/11/22/china-vulnerability-disclosures-risks/.

[142] Press Release dated 12 July 2019, Ministry of Home Affairs, Government of India, https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226.

establishment of the Indian Cyber Crime Coordination Centre (I4C) to handle issues related to cybercrime in the country in a comprehensive and coordinated manner.[143] We suggest that an online portal should be made available for the reporting of all cyber crimes, and not be restricted to crimes against women and children.

In 2017, the Central Government created the Cyber and Information Security Division (C&IS) under the Ministry of Home Affairs with four proposed wings- i. Security Clearance, ii. Cyber Crime Prevention, iii. Cyber Security and iv. Information Security.[144] Measures such as the creation of the I4C, Central Cybercrime Portal (for reporting crimes against women and children), setting up of cyber-investigation labs, etc. have been carried out under the ambit of the Cyber Crime wing of the C&IS Division.[145]

To develop capacity in law enforcement agencies, the MHA has also set up the National Cybercrime Training Centre (NCTC) or "CyTrain" as part of the I4C for combating cybercrimes, impact containment and investigations.[146] CyTrain also focuses on standardization of course curriculum, development of hands-on training modules for cybercrime detection, containment and reporting using simulated cyber environments, development of MOOCs (Massive Open Online Courses) and establishment of cyber labs.[147]

Special consideration should also be given to the fact that the "police" falls in the State List under the Constitution and is the prerogative of the states. The Central Government may take the lead by laying down Model SOPs for preservation and analysis of electronic evidence and investigation of cyber crimes to guide and assist State Governments. For instance, the MHA has provided a grant of Rs. 93.12 crore to all the States/ Union Territories under the Cyber Crime Prevention against Women and Children (CCPWC) scheme to set up cyber forensic cum training laboratories,

[143] Ibid.

[144] Press Release dated 17 January 2018, Ministry of Home Affairs, Government of India, https://pib.gov.in/newsite/mbErel.aspx?relid=175699.

[145] Government of India, Ministry of Home Affairs, Divisions of MHA, https://mha.gov.in/division_of_mha/cyber-and-information-security-cis-division.

[146] Government of India, Ministry of Home Affairs, CyTrain, https://cytrain.ncrb.gov.in/local/staticpage/view.php?page=CyTrain.

[147] Ibid.

hiring of junior cyber consultant and training/ capacity building to provide hands-on training to Law Enforcement Agencies (LEAs) personnel, prosecutors and judicial officers.[148] According to the relevant press release, these cyber forensic cum training laboratories have already been commissioned in the states of Arunachal Pradesh, Himachal Pradesh, Madhya Pradesh, Telangana, Uttarakhand, Uttar Pradesh and.[149] MeitY has also set up cyber forensic training labs in Ghaziabad (CBI Academy), Mumbai, Pune, Bangalore, Kolkata, Kerala, Uttarakhand and all north eastern States for training in cyber-crime detection, seizing, preservation and imaging of digital evidence, etc.[150]

At the state level, the government of Maharashtra has launched a "Cyber Maharashtra" project with a budget of 1000 crores[151]. Andhra Pradesh[152] and Telangana[153] are following suit.

These capacity building measures are welcomed, but they need to be amplified both at the central and state levels. Like the UK and Australia, India should strengthen its threat sharing and analysis platforms to cyber-crime units to enable them to more effectively investigate, apprehend and prosecute cyber crimes.

At the same time, similar to the US, India should also place emphasis on cooperation at the international level for investigative efforts in cyber-crimes. India can also enter into global partnerships to build capacity for its local cyber-crime units. Joint drills, exchange missions and so on will result in better training for Indian cyber-crime units. Subject to proper oversight, compliance with local laws and due regard for constitutional rights and doctrine of checks and balances between Central and State

---

[148] Press Release dated 9 July 2019, Ministry of Home Affairs, Government of India, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1577948.

[149] Ibid.

[150] Ibid.

[151] Priyanka Pugaokar, *Maha Govt Invests 1000 Cr In 'Cyber Maharashtra' Project*, ChannelTimes.com, dated 28 August 2016, https://www.channeltimes.com/story/maha-govt-invests-1000-cr-in-cyber-maharashtra-project/.

[152] Sridhar Raavi, *AP – First in India to have 24X7 Cyber Security*, Mirchi9, dated 30 November 2014, https://www.mirchi9.com/politics/ap-first-in-india-to-have-24x7-cyber-security/.

[153] Express News Service, *Telangana government formulates cyber security policy*, The New Indian Express, dated 16 September 2016, http://www.newindianexpress.com/states/telangana/2016/sep/16/Telangana-government-formu- lates-cyber-security-policy-1520023.html.

Governments, India should also adopt new technologies to better equip cyber-crime units to deal with the constantly evolving threat landscape of cyber-crimes.

4. Information Sharing Mechanisms

While India has taken major steps by establishing CERT-In and several sectoral CERTs for the financial sector and the power sector[154] (one each for Transmission, Thermal, Hydro and Distribution), it is yet to establish a cross-sectoral information sharing platform where relevant threat information is shared, collated and analysed for better understanding of existing and future threats.

The Joint Working Group on Engagement with the Private Sector on Cyber Security (2012) recommended the setting up of Information Sharing and Analysis Centres ("ISACs") for cross-sectoral information sharing.[155] Although it was recommended that these centres be set up by the private sector in the context of public-private sector collaboration and coordinate with CERTs (both CERT-In and sectoral CERTs)[156], these centres would be instrumental in facilitating threat information sharing with the required support from Government. It is relevant to note that the ISAC also functions as a public-private-partner with the NCIIPC for advancing its mission which includes certification programs as well as organizing conferences and seminars to further cybersecurity research and developments.[157]

The government has established an ISAC at the Institute for Development and Research in Banking Technology for financial services which is a positive step, but while there were plans announced to establish similar ISACs in power and petroleum sectors[158], it is not clear whether these have in fact been established.

---

[154] Press Release dated 20 March 2017, Ministry of Power, Government of India, https://pib.gov.in/newsite/PrintRelease.aspx?relid=159537.

[155] Recommendations of the Joint Working Group on Engagement with the Private Sector on Cyber Security (2012), National Security Council Secretariat, Government of India, https://cii.in/WebCMS/Upload/JWG%20report.pdf.

[156] Ibid.

[157] Information Sharing and Analysis Centre and the National Critical Information Infrastructure Protection Centre, https://www.isac.io.

[158] Press Release dated 28 November 2014, Ministry of Communications, Government of India, https://pib.gov.in/newsite/PrintRelease.aspx?relid=112078.

CERT-In has also established an automated threat information and intelligence sharing platform among some "select stakeholders".[159] CERT-In stated in its Annual Report (2018) that one of its future plans was to create "a full-fledged automated Threat Information and Intelligence sharing platform for sharing Indicators of Compromise (IoCs) across stakeholders in the coming year"[160], but the progress of this plan is unclear. We hope that CERT-In's Annual Report for 2019, when it is released, will include details on progress made in this area.

There is much to be gained from cooperation and intelligence sharing on the international level and it appears that CERT-In has recognized its importance.[161] It is vital that India maximizes benefits from existing international threat sharing platforms such as the Asia-Pacific CERTs which comprises of 28 teams from 20 economies across the region.

5. Supply Chain Security

Our study of cybersecurity strategies reveals that most countries have acknowledged the importance of supply chain security and risk management, particularly for governmental infrastructure.[162] Even though supply chain cyber security is highly relevant for the private sector as well[163], we restrict our comments to issues of supply chain security relevant for governmental cyber infrastructure. Some basic measures include buying only from trusted vendors and creation and maintenance of testing infrastructure and facilities. This was acknowledged in the 2013 Policy as well.[164]

---

[159] Annual Report (2018), Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & Information Technology, Government of India, Para 1.2, p. 4, https://www.cert-in.org.in.

[160] Annual Report (2018), Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & Information Technology, Government of India (CERT-In), Para 6, p. 14, https://www.cert-in.org.in.

[161] Annual Report (2018), Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & Information Technology, Government of India (CERT-In), p. 11-13, https://www.cert-in.org.in.

[162] See Annexure 'A' to the Dossier.

[163] Bruce Schneier, *Every Part of the Supply Chain Can Be Attacked*, The New York Times, dated 25 September 2019, https://www.nytimes.com/2019/09/25/opinion/huawei-internet-security.html.

[164] National Cyber Security Policy, 2013, Department of Electronics and Information Technology, Ministry Of Communication And Information Technology, Government of India, p. 13.

Countries such as the United States have developed a multi-pronged approach to dealing with supply chain security (a) improve management of supply chain security of governmental cyber infrastructure, (b) designate specific authorities for ensuring this task and standardizing IT systems across governmental structures and lastly (c) strengthen the systems security of government contractors.[165] As part of this approach, the US national cyber strategy focuses on the need for securing federal infrastructure by centralizing its management and oversight[166], which it hands over to the Department of Homeland Security ("DHS").[167] The US Strategy envisages government-wide deployment of centralized capabilities, tools and services through the DHS. The US Strategy also contemplates alignment of risk management and IT activities through "Chief Information Officers" in different departments, by both empowering and holding them accountable for aligning cybersecurity risk management and IT procurement.[168] COOs are authorities who oversee federal spending, federal IT policy and strategic planning of all federal IT investments.

Additionally, the US Strategy also envisages federal review and oversight of its contractors risk management practices, federal contracts incorporating terms to this effect as well as sharing relevant threat and vulnerability information with its contractors.[169]

India can also enhance its own governmental supply chain security by similarly empowering a particular agency or authority to centralize and standardize its IT systems across all levels of government. India also needs to consider embedding supply chain security in its procurement processes**.** In this regard, CCG is currently working on a research paper to analyse how our procurement processes can be re-calibrated to enhance security and access to cutting-edge technology in the cyber domain.

Maintaining a register of approved vendors who are certified and tested by central agencies and utilizing only those vendors for government work would also help.

[165] National Cyber Strategy of the United States of America, White House, p. 6.

[166] National Cyber Strategy of the United States of America, White House, p. 6-7.

[167] National Cyber Strategy of the United States of America, White House.

[168] National Cyber Strategy of the United States of America, White House, p. 7.

[169] National Cyber Strategy of the United States of America, White House, p. 7-8.

Should such a step be taken, the Government must necessarily also modify its contracts allowing it to maintain regular review and oversight of its contractor's cyber security policies. Monitoring and evaluation processes must also be established.

Another point to note is that the US Strategy also makes a distinction between federal civilian infrastructure for which the Department of Homeland Security is responsible and federal military infrastructure/ national security systems, for which the Department of Defence and the relevant intelligence agencies are responsible.[170] India can similarly prioritize and consider separate treatment of IT security for its national security related infrastructure vis-à-vis other governmental infrastructure.

6. Testing and Certification Standards

In order to ensure access to safe and reliable cybersecurity products and services to the population, in accordance with the 'whole-of-nation' approach, the government must take the lead in establishing a framework to establish and maintain trust and security on cybersecurity products and services for a population that is still striving to achieve universal digital literacy. Drawing up certification schemes which set a minimum standard for all products and services will provide much needed guidance for the private sector. It will also provide criteria to enable assessments establish the degree of adherence of products, services and processes against specific requirements. These requirements can also be incorporated in government contracts for procurements of such goods and services and relevant legislations to ensure compliance.

Countries such as the UK have taken a follow-the-government approach whereby the government sets the trend and the private sector follows.[171] The UK's strategy also contemplates having "security ratings" for products.[172] These are some practices that India can consider adopting.

Generally, Indian certification standards consist of the standards issued by the Bureau of Indian Standards, the Telecommunications Engineering Centre under the

[170] National Cyber Strategy of the United States of America, White House, p. 6.

[171] UK National Cyber Security Strategy 2016, Para 4.15, p. 27.

[172] UK National Cyber Security Strategy 2016, Para 5.2.6, p. 36.

Department of Telecommunication, and the Standardization Testing and Quality Certification Directorate under MeitY. Global certification standards include Critical Security Controls by the Centre for Internet Security, the NIST Cyber Security Framework, the ETSI Cyber Security Technical Committee as well as the Factor Analysis of Information Risk (FAIR) standards.

As per CERT-In's Annual Report, government and critical sector organizations are implementing ISO 27001 standard and the periodic advice issued by CERT-In.[173]

C. Cyber Security Skills and Awareness

1. Access to Cyber Security Products and Services

In accordance with the 'whole-of-nation' approach emphasized by the Secretariat in the Call for Comments on the NCSS 2020, and our conceptualization of the broader realm of the 'national cyberspace', we believe that there is substantial strategic and economic value to ensuring equitable access to safe and reliable cyber security products to the population at large. This is important for three reasons: (1) this would enable individuals and other juridical entities who possess the necessary skills to protect themselves from malicious actors in cyber space to do so, and contribute to building a secure and resilient cyber space, (2) this would lay the foundation for building an ecosystem of trust among stakeholders and (3) ensure maximum possible protection to the constitutional rights of citizens in cyberspace.

A salient example which illustrates this point is the recent incidents of compromise of encrypted communications services of WhatsApp by use of the Pegasus spyware. Such incidents hamper the cyber security of the individual, which eventually erodes the cybersecurity of the state at large and undermines trust in the national cyberspace. Elevating the standards of protection accorded to the digital security and privacy of citizens in law and policy could also potentially open the doors for information sharing with law enforcement agencies of other nations, especially the United States under the CLOUD Act and other States party to the Budapest Convention. This could in turn, boost the efforts of our investigative agencies to

[173] Annual Report (2018), Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & Information Technology, Government of India (CERT-In), p. 9, https://www.cert-in.org.in.

access data stored in foreign jurisdictions to expedite and strengthen the investigation of cyber-crimes in India.

In the previous section, we suggested the use of standardisation, quality testing and certification of cyber security products and services as one means of building trust in the national cyber space. Another approach is 'secure-by-design', where the software has been designed from the foundation to be secure. This has become the mainstream approach of several countries including the UK[174] and Singapore[175], when dealing with cyber security. India could also consider adopting this approach in its own strategy since it is important to start thinking of cyber security from the grassroot level. India can also consider the UK's Secure-by-default approach, which is to ensure that products and services used by the government (and even consumers) have built-in security by default, requiring the user to actively switch it off should they so choose.[176]

2. Capacity Building and Skilling for 'Cyber Warriors'

With the Digital India programme enhancing the digital literacy of the Indian population, there is a need to also begin similar dedicated programmes for enhancing (1) the pool of skilled professionals in cybersecurity, and (2) cybersecurity literacy and awareness at large.

An important fact to be noted is that India already has an existing pool of educated professionals to tap. Almost 10 lakh engineering graduates are added to the workforce per month.[177] Cybersecurity capacity can be built by re-skilling existing professionals in cybersecurity. This method is adopted by countries such as the United States.[178] Private public partnerships should be established to drive these reskilling efforts as well.

---

[174] UK National Cyber Security Strategy 2016, Para 8.4, p. 64.

[175] Singapore National Cyber Security Strategy, p. 12.

[176] UK National Cyber Security Strategy, Para 5.2.3, p. 64.

[177] Payel Majumdar Upreti, *Engineering Crisis*, The Hindu, dated 11 May 2018, https://www.thehindubusinessline.com/blink/cover/engineering-crisis/article23849534.ece.

[178] National Cyber Strategy of the United States of America, White House, p. 17.

Yet, the demand for cybersecurity skilled professionals in India still exceeds the supply. A survey conducted by Capgemini found that 68% of organizations in India reported high demand for cybersecurity skills.[179] The report also predicts an increase in this requirement by 2020.[180] Cisco has made similar predictions.[181] Therefore, it is apparent that there is an urgent need to develop a strong cyber-security enabled workforce. We believe that the most productive means of doing so is to mainstream cybersecurity education at the university level, inject more funds and provide more State support to research and development activities to encourage the creation of innovative solutions to India's cyber security problems, and boost the development, production and provision of cyber security products and services by Indian companies.

Blockchain and Cryptocurrencies

India should not lose out on the benefits of cutting-edge research on emerging technologies such as blockchain and cryptocurrency. Cryptocurrency remains an outlier despite the government's push for a digital economy. A circular by the Reserve Bank of India ("RBI") in 2018 has effectively blocked dealing in cryptocurrency.[182] However, on the positive side, steps such as the RBI setting up a Blockchain and Cryptocurrency research unit to understand how to regulate these technologies are encouraging.[183] Blockchain and cryptocurrency gain particular significance for their potential for stronger forms of cybersecurity and are already being used by several governments across the world including in Estonia, Dubai, Georgia and Switzerland.[184]

---

[179] Capgemini Research Institute, *Cybersecurity Talent: The Big Gap in Cyber Protection* (2018), p. 2, https://www.capgemini.com/in-en/wp-content/uploads/sites/6/2018/10/Cybersecurity-Talent-Gap_Digital-1.pdf.

[180] Ibid.

[181] CISCO White Paper, *Security in India- Enabling a New Connected Era* (2016), p. 2, https://www.cisco.com/c/dam/en/us/products/collateral/security/security-benchmark-study-india-paper.pdf.

[182] Sriram Iyer and Nupur Anand, *India Cracks Down On Bitcoin And Hints It May Launch Its Own Digital Currency*, Quartz India, dated 5 April 2018, https://qz.com/india/1245586/reserve-bank-of-india-cracks-down-on-bitcoin-and-hints-it-may-launch-its-own-digital-currency/.

[183] Dipen Pradhan, *RBI sets up Blockchain and Cryptocurrency Research Unit*, Inc42, dated 28 August 2018, https://inc42.com/buzz/rbi-sets-up-blockchain-cryptocurrency-research-unit/.

[184] Akash Takyar, *A Detailed Insight into Blockchain Government Initiatives*, Leeway Hertz, https://www.leewayhertz.com/blockchain-government-public-sector-initiatives/.

Artificial Intelligence

Artificial Intelligence (AI) is another area in which India is lagging behind. Indian AI research is already behind China's and the United States', with the United States leading in terms of its standing in the AI economy.[185] NITI Ayog's Discussion Paper on a National Strategy for Artificial Intelligence is a positive step. Identifying the focus areas for AI intervention as healthcare, agriculture, education, smart cities and infrastructure, and smart mobility and transportation, the paper recommends adopting an inclusive approach, not only focusing on economic growth but also social inclusion, with the catchphrase #AIforAll.[186] The paper also deals with ethics and privacy issues in AI.[187]

India should consider partnerships with leading private sector companies such as Microsoft, Google and Amazon Web Services, with due consideration for privacy and national security concerns, to lead the way in embedding AI in governmental services. **We should consider providing incentives for Indians abroad with specializations in AI, cloud computing, machine learning and deep learning to return to India and contribute to AI development.** This will also help in reducing brain drain and retaining cyber-capacity.

India can also consider setting up initiatives along the lines of Israel's CyberSpark which is "a concentrated and powerful cyber security ecosystem consisting of Israeli startups, global companies, academia and civilian and military cyber security centers – all within walking distance of one another."[188]

3. Information Security Education and Awareness

MeitY's Information Security Education and Awareness (ISEA) programme has as one of its key objectives the identification and development of the right kind of

[185] Daniel Castro, Michael McLaughlin and Eline Chivot, *Who Is Winning the AI Race: China, the EU or the United States?*, dated 19 August 2019, Center for Data Innovation, https://www.datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/.

[186] Discussion Paper, National Strategy for Artificial Intelligence #AIFORALL, NITI Ayog, Government of India, June 2018, https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.

[187] Ibid, p. 85-89.

[188] Israel National Cyber Security Strategy in Brief, National Cyber Directorate, Prime Minister's Office, State of Israel, p. 17.

qualified and well trained human resources, who could take up Research & Development (R&D), develop indigenous solutions / software, secure and maintain various systems including critical infrastructure.[189] The ISEA programme is implemented by partnering with (a) 51 institutes for academic activities including the Indian Institute of Science (Bangalore)[190], Indian Institutes of Technology at Bombay[191], Guwahati[192] and Madras[193], (b) 16 implementing agencies for training of Government Official with one coordinating agency i.e. NIELIT Centre Gorakhpur[194] and (c) several awareness programs with the coordinating agency being the Centre for Development of Advanced Computing (C-DAC) in Hyderabad.[195] The partner universities are also required to introduce cybersecurity modules formally as part of their curriculums.[196]

The main targets of ISEA's training mandate are Central & State Government Officials as well as legal and police personnel.[197]

Beyond Government functionaries, similar to approaches in other countries such as the UK[198], the goal of achieving universal cybersecurity literacy also requires incorporation into school curriculums. Positive steps in this direction are the NCERT

[189] Government of India, Ministry of Electronics & Information Technology, Information Security Education and Awareness Project, https://isea-pmu.in/about/.

[190] Government of India, Ministry of Electronics & Information Technology, Information Security Education and Awareness Project, Indian Institute of Science, Bangalore, https://isea-pmu.in/home/institutes/isrdc/iiscb/.

[191] Government of India, Ministry of Electronics & Information Technology, Information Security Education and Awareness Project, Indian Institute of Technology, Bombay & Tata Institute of Fundamental Research, Mumbai, https://isea-pmu.in/home/institutes/isrdc/iitb-and-tifrm/.

[192] Government of India, Ministry of Electronics & Information Technology, Information Security Education and Awareness Project, Indian Institute Of Technology, Guwahati, https://isea-pmu.in/home/institutes/isrdc/iitg/.

[193] Government of India, Ministry of Electronics & Information Technology, Information Security Education and Awareness Project, Indian Institute of Technology, Madras, https://isea-pmu.in/home/institutes/isrdc/iitm/.

[194] Government of India, Ministry of Electronics & Information Technology, Information Security Education and Awareness Project, Implementation & Structure, https://isea-pmu.in/implementation_structure/introduction/.

[195] Ibid.

[196] Government of India, Ministry of Electronics & Information Technology, Information Security Education and Awareness Project, Objectives, https://isea-pmu.in/about/.

[197] Government of India, Ministry of Electronics & Information Technology, Information Security Education and Awareness Project, Introduction, https://isea-pmu.in/training/.

[198] UK National Cyber Strategy, Para 7.1.9, Page 56.

having accepted the syllabus suggested by C-DAC for adoption/inclusion into existing ICT curriculum of schools.[199] CBSE has also placed the ISEA web link in the website of all schools in India for creating awareness among students, teachers and parents.[200] The draft cyber security curriculum for 3rd standard to 12th standard for schools has been prepared and submitted to CBSE/NCERT for adoption.[201]

At the University level, CCG has been teaching an experimental curriculum on National Security Law and Policy, with a substantial focus on cyber security and cyber warfare as an elective Seminar Course offered to fourth and fifth year law students at the National Law University Delhi since 2017. In this course curriculum, we aim to (1) recognize and develop National Security Law as a discrete discipline of legal studies, which lies at the intersection of domestic criminal law, Constitutional law and the geopolitics of international law and (2) impart basic levels of cyber security education and information security practices among tomorrow's lawyers. Measures such as these, when replicated, will go a long way in supplementing cybersecurity literacy penetration to all age-groups, professions and sectors.

For better outreach, existing efforts can be supplemented with programmes similar to the UK's Cyber Aware Campaign (earlier called Cyber Streetwise) which disseminates simple, basic but effective cybersecurity advice such as using three random passwords, latest software downloads, etc. through targeted messaging delivered through social media, advertising and in partnership with business promoters.[202] Similar to this practice, we suggest a much wider dissemination of Common Vulnerabilities and Exposures (CVE) Reports regularly issued by the CERT-In and NCIIPC to the public at large, who should be able to opt-in and subscribe to receiving such updates in the form of periodic newsletters, or at least, urgent updates and warnings, where required.

While collaborative and concerted effort by all stakeholders is the need of the hour, it must be kept in mind that achieving universal cybersecurity literacy, or even digital

[199] C-DAC, INFOSEC Depot 2019, p. 12, https://www.infosecawareness.in/gallery/annual-magazines/InfoSec-Depot-19/00_Indulge.pdf.

[200] Ibid.

[201] Ibid.

[202] UK National Cyber Security Strategy 2016, p. 43.

literacy, is a long-term objective and more likely achieved over the next 20 years, rather than the next 5.[203] Any action plan must keep this in mind, but remain geared towards accelerating and expanding outreach to all stakeholders in the 'national cyberspace'.

D. Monitoring and Evaluation of Strategic and Policy Goals

For any policy to be effective, it is important that it has some key features in place. The policy has to be quantifiable in such terms where the outcomes can be predicted and measured. Although it is difficult to encapsulate this idea with respect to cyberspace where it's hard to anticipate how the emerging technology and threats would look like, it is nonetheless important to have a measurable matrix for performance indicators. This would ensure that the strategy document is not just a vision statement but a prescriptive document with measurable outcomes.

On the whole, there are Government initiatives on the education and research fronts, but there needs to be an active review and monitoring and evaluative mechanism. A National Apex Committee under the Chairmanship of Secretary, MeitY is setup to carryout mid-term review of the program and suggest mid-course corrections if any.[204] Additionally, a Program Review and Steering Committee (PRSC) under the chairmanship of the Group Coordinator (MeitY) will evolve overall implementation framework, continuously supervise the implementation and also periodically monitor the progress of the programme.[205] These bodies will be required to actively monitor, review and evaluate the success of these programmes against certain tangible parameters as well as make the results public.

With a view to monitoring and evaluating the outcomes of the National Cyber Security Policy 2013, we have analysed the Union expenditure on cyber security since FY 2013-14 as an indicator of implementation of policy objectives to identify

[203] The United Kingdom has noted this approach. See UK National Cyber Security Strategy 2016, Para 7.1.4, p. 55.

[204] Government of India, Ministry of Electronics & Information Technology, Information Security Education and Awareness Project, Institutional Mechanism, https://isea-pmu.in/implementation_structure/institutional_mechanism/.

[205] Ibid.

whether any patterns and trends in expenditure emerge and where these expenses may be rationalized through synergising functions of the ‘Whole-of-Government’.

V. THE THIRD PILLAR: 'SYNERGISE' (RESOURCES, COOPERATION AND COLLABORATION)

In Part III on the First Pillar 'Secure', we discussed the *horizontal dimension* of strategy wherein we presented a range of principled approaches to identifying and interacting with allies and adversaries in cyberspace in accordance with the international and domestic legal framework that applies to cyberspace. In Part IV on the Second Pillar of Strategy 'Strengthen', we addressed the *vertical dimension* of strategy, which deals with the dynamic between strategy, and operational and administrative concerns that give rise to *friction* in India's architecture of institutions and agencies entrusted with cybersecurity related functions. We presented recommendations and suggestions in both these parts with a view to minimizing such friction, which could pose a hinderance to the realization of our strategic and policy goals.

In this part, we examine the interplay and dynamic between the *horizontal* and *vertical dimensions* of strategy. It is this dynamic that will determine the quantum of financial and technical resources that we need to invest in these efforts. Indeed, the quantum of resources that can be diverted towards cybersecurity is limited by budgetary constraints. Accordingly, in this part we present analyses of:

A. The allocation and utilization of budgetary resources by relevant Government departments since the National Cyber Security Policy 2013 to formulate a 'Whole-of-Government' approach as a core component of the 'Whole-of-Nation' approach espoused by the Secretariat in its Call for Comments.

B. A principled 'Whole-of-Nation' approach based on Common but Differentiated Responsibility (CBDR) towards building Public-Private Partnerships with domestic and international stakeholders for the apportionment of roles and responsibilities in the building, maintenance and strengthening of India's cyber defence based on the level of technical expertise of stakeholders.

C. The implications of CBDR at the international level and measures to enhance international cooperation to bolster national efforts towards building a safe, secure, trusted, resilient and vibrant cyber space for our nation's prosperity.

A. A 'Whole-of-Government' Approach

The building of robust cyber defences for the 'national cyberspace' is an unprecedented opportunity to enhance cooperation between the civilian and military wings of the Government. The inherent dual-use nature of cybersecurity products and services necessitates that the Government also take on a dual role of administrator and where necessary, guardian of the cybersecurity of all relevant stakeholders. In doing so, it is imperative to accord centrality to the Government's role as administrator, and guard against the over-securitization of cyberspace to ensure that technological innovation is not stifled.

With these objectives in mind, in this section, we analyse the expenditure of various Departments entrusted with functions that are most relevant to cybersecurity.

We have compiled the data on allocations (budgeted and revised) and actual expenditure from the Demands for Grants of Ministries as approved by Parliament and presented in the Annual Expenditure Budget of various ministries and their respective departments which are related to cybersecurity from FY 2013-17 to FY 2019-20.

The departments have been identified from publicly available information represented in the organograms presented as Annexure 'B' We understand a 'relevant department' to mean those departments which are either directly related to cybersecurity and/or support the functioning of the security aspects of internet governance at large. A detailed note on research methodology for this analysis is appended as Annexure 'C' to this submission.

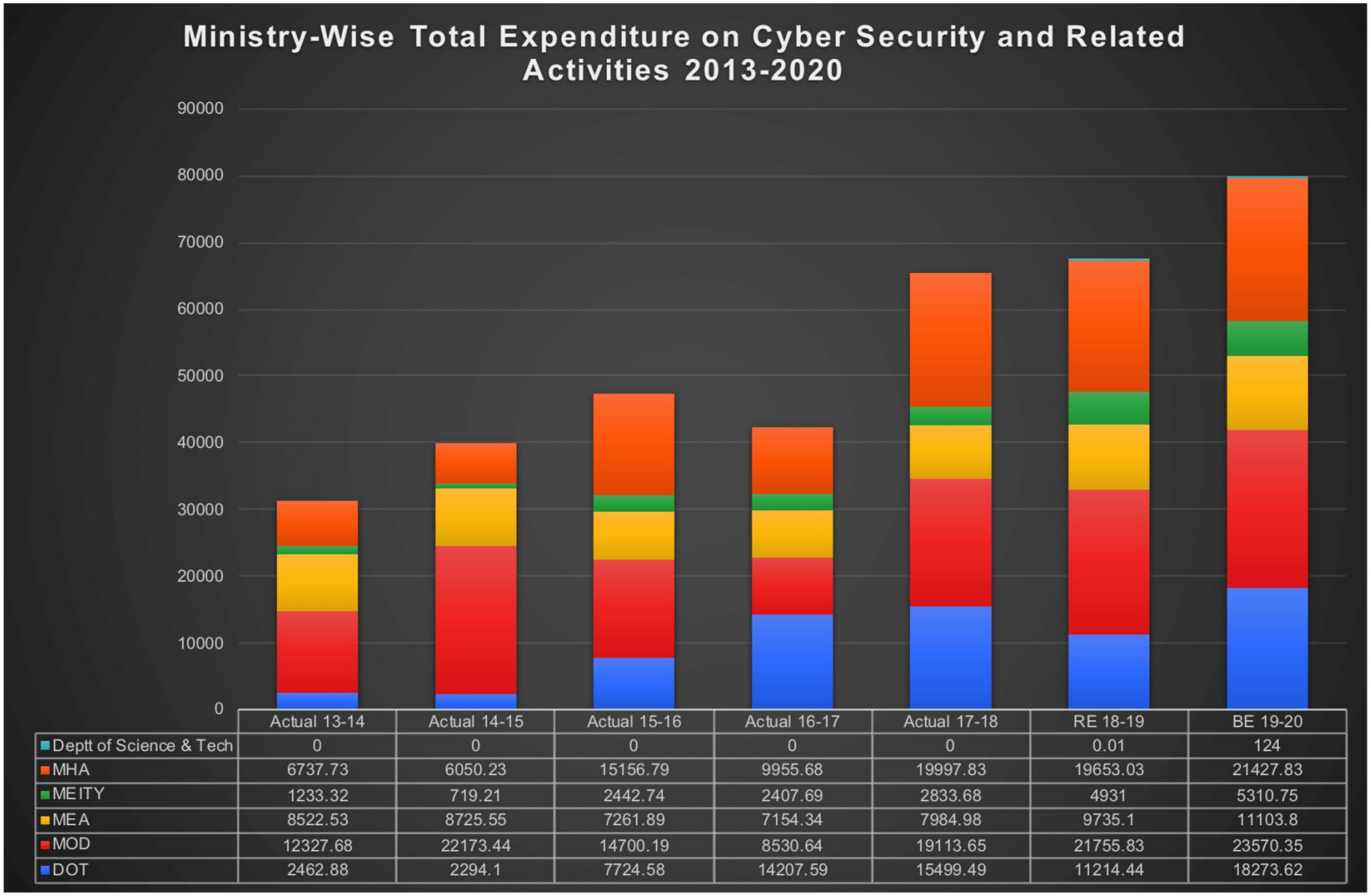
We then identified those budget heads under the Union Budgets for FY 2013-14 through FY 2019-2020, which correspond most closely to the departments identified and highlighted in Annexure 'B' to calculate the total allocation to ministries for cybersecurity related activities.

Figure 9 depicts actual expenditure (from FY 2013-14 to FY 2017-18), the Revised Expenditure (RE) for FY 2018-19 and Budgeted Expenditure for FY 2019-20. With the exception of FY 2016-17, we can see a clear trend of increasing allocations for expenditure towards cyber-security related activities, especially for the DoT. It is

relevant to point out that this representation also includes the expenditure on Departments playing a supporting role in cybersecurity activities, such as the IDS/Joint Staff and R&D under the Ministry of Defence (MoD) as well as the MEA's expenditure on international technical cooperation. As the expenditure incurred on cybersecurity related activities alone cannot be inferred from these budget heads, they have been treated as Departments playing a supporting role for cybersecurity efforts and included in overall expenditure.

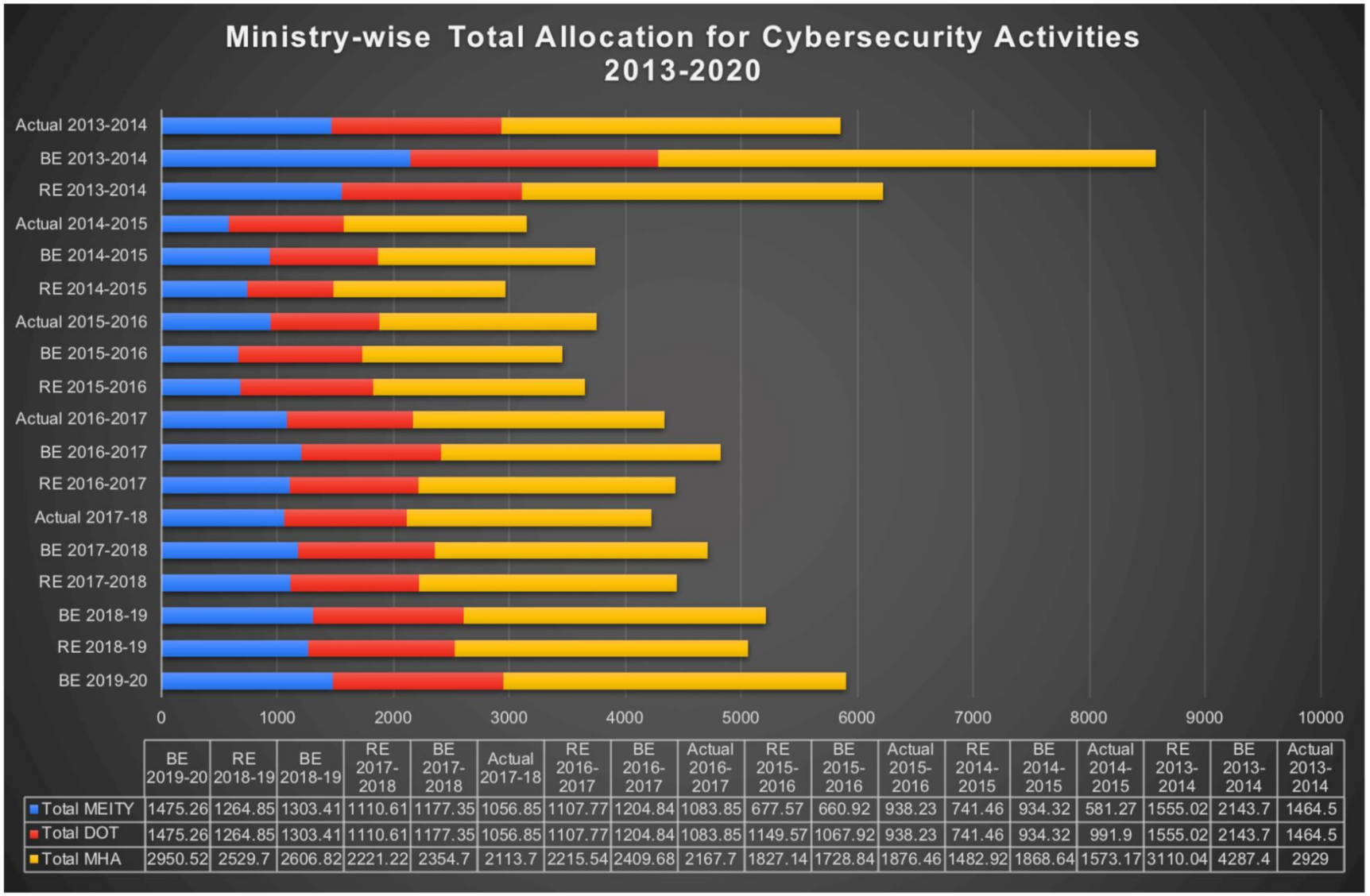
Figure 10 is a narrower subset of the expenses indicated in Figure 9. It represents the allocations to Departments in Ministries that have been entrusted with core activities that contribute towards cybersecurity operations, R&D, e-Governance and internet governance at large. These include, to name a few, the promotion of electronics and IT hardware manufacturing and other initiatives such as Digital India, C-DAC, NCCC and other similar programmes under MeitY, TRAI, C-DoT and the 5G test bed under the authority of the DoT and MHA's expenses towards modernization of police forces, forensics, and initiatives such as the Indian Cyber Crime Coordination Centre. A full list of relevant departments and programmes can be found in Annexure 'C'.

Figure 10 reveals an immediate upsurge in such allocations in the time period during and immediately after the formulation of the National Cyber Security Policy 2013, after which the allocations begin to dwindle in FY 2014-15. We can also note that with the exception of FY 2015-16 actual expenditure is consistently lower than the Budgeted Expenditure allocated to all these Ministries for cybersecurity related activities.



	Actual 13-14	Actual 14-15	Actual 15-16	Actual 16-17	Actual 17-18	RE 18-19	BE 19-20
Deptt of Science & Tech	0	0	0	0	0	0.01	124
MHA	6737.73	6050.23	15156.79	9955.68	19997.83	19653.03	21427.83
MEITY	1233.32	719.21	2442.74	2407.69	2833.68	4931	5310.75
MEA	8522.53	8725.55	7261.89	7154.34	7984.98	9735.1	11103.8
MOD	12327.68	22173.44	14700.19	8530.64	19113.65	21755.83	23570.35
DOT	2462.88	2294.1	7724.58	14207.59	15499.49	11214.44	18273.62

Figure 9: Ministry-Wise Total Expenditure on Cybersecurity and Related Activities 2013-2020



	BE 2019-20	RE 2018-19	BE 2018-19	RE 2017-2018	BE 2017-2018	Actual 2017-18	RE 2016-2017	BE 2016-2017	Actual 2016-2017	RE 2015-2016	BE 2015-2016	Actual 2015-2016	RE 2014-2015	BE 2014-2015	Actual 2014-2015	RE 2013-2014	BE 2013-2014	Actual 2013-2014
Total MEITY	1475.26	1264.85	1303.41	1110.61	1177.35	1056.85	1107.77	1204.84	1083.85	677.57	660.92	938.23	741.46	934.32	581.27	1555.02	2143.7	1464.5
Total DOT	1475.26	1264.85	1303.41	1110.61	1177.35	1056.85	1107.77	1204.84	1083.85	1149.57	1067.92	938.23	741.46	934.32	991.9	1555.02	2143.7	1464.5
Total MHA	2950.52	2529.7	2606.82	2221.22	2354.7	2113.7	2215.54	2409.68	2167.7	1827.14	1728.84	1876.46	1482.92	1868.64	1573.17	3110.04	4287.4	2929

Figure 10: Ministry-Wise Total Expenditure on Cybersecurity and Related Activities 2013-2020

It is interesting to note that if we convert the absolute figures represented in Figure 10 into percentages, and represent the same data set as such, it reveals a remarkable consistency and a clear pattern emerges in burden-sharing between these three Ministries (MHA, MeitY and DoT under the Ministry of Communications).

Figure 11 depicts the same allocations indicated as absolute figures in Figure 10 as percentages of the total expenditure on core cybersecurity activities. It is clear that the MHA consistently bears the bulk of expenses on cyber security related activities, clearly with an emphasis on cyber crimes. The remaining half seems to be divided between MeitY and DoT more or less equally. FY 2015-16 allocations and actual expenditure in FY 2014-15 is the only exception to this equal distribution.

To further analyse how these allocations are being utilized, we have re-categorized the expenditures mentioned in Department/Ministry wise allocation into five categories, each of which have been identified as constituent elements of the three Pillars of Strategy namely:

i. Human Resource Development Component (Strengthen)

ii. Technical Research and Development Component, Capacity Building (Strengthen/Synergize)

iii. International Cooperation and Investment Promotion Component (Secure/Synergise)

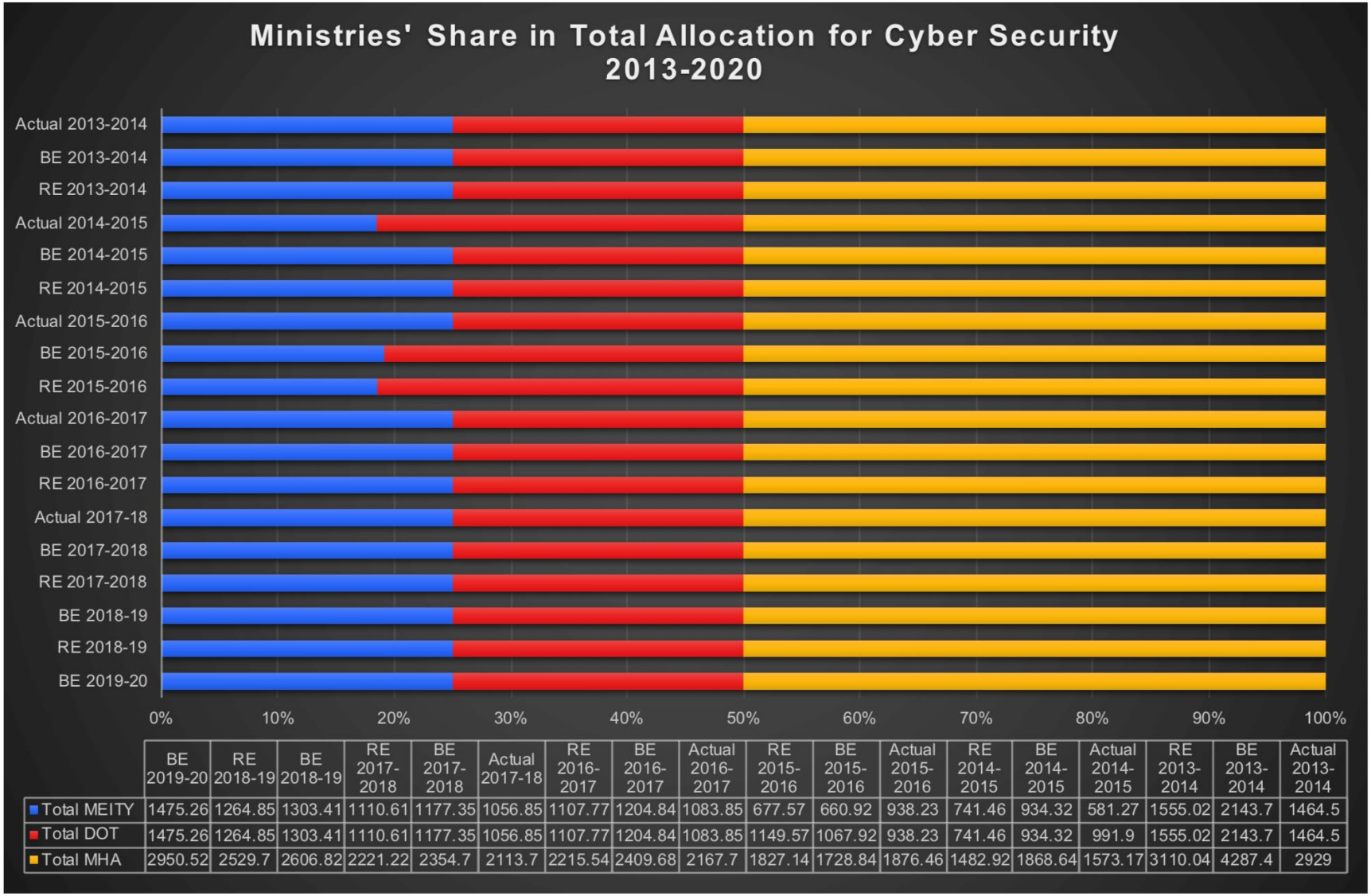
iv. Standardization, Quality Testing and Certification Component (Strengthen)

v. Active Cyber Incident Response/ Cyber Defence Operations and Security Component (Secure/Strengthen)

The total expenses incurred for these allocations are calculated to identify if any trends or patterns emerge to identify which activities are being prioritized according to the actual expenditure incurred by the relevant ministries. It is important to note that none of these categories include any expenses earmarked for cyber defence operations under

the MoD, as the budget heads do not permit drawing such an inference in its current format.

In this reclassification, we have included one budget head each for two other Departments that do not figure in the data represented in Figures 9, 10 or 11. Namely, these are (1) the allocation towards corporate data management under the authority of the Ministry of Corporate Affairs, which has been included in category (v) indicated above and (2) the allocation towards technical and economic cooperation with other countries for the Department of Economic Affairs under the Ministry of Finance, which has been included in category (iii) indicated above.



	BE 2019-20	RE 2018-19	BE 2018-19	RE 2017-2018	BE 2017-2018	Actual 2017-18	RE 2016-2017	BE 2016-2017	Actual 2016-2017	RE 2015-2016	BE 2015-2016	Actual 2015-2016	RE 2014-2015	BE 2014-2015	Actual 2014-2015	RE 2013-2014	BE 2013-2014	Actual 2013-2014
Total MEITY	1475.26	1264.85	1303.41	1110.61	1177.35	1056.85	1107.77	1204.84	1083.85	677.57	660.92	938.23	741.46	934.32	581.27	1555.02	2143.7	1464.5
Total DOT	1475.26	1264.85	1303.41	1110.61	1177.35	1056.85	1107.77	1204.84	1083.85	1149.57	1067.92	938.23	741.46	934.32	991.9	1555.02	2143.7	1464.5
Total MHA	2950.52	2529.7	2606.82	2221.22	2354.7	2113.7	2215.54	2409.68	2167.7	1827.14	1728.84	1876.46	1482.92	1868.64	1573.17	3110.04	4287.4	2929

Figure 11: Ministry-Wise Total Allocation for Cybersecurity and Related Activities 2013-2020

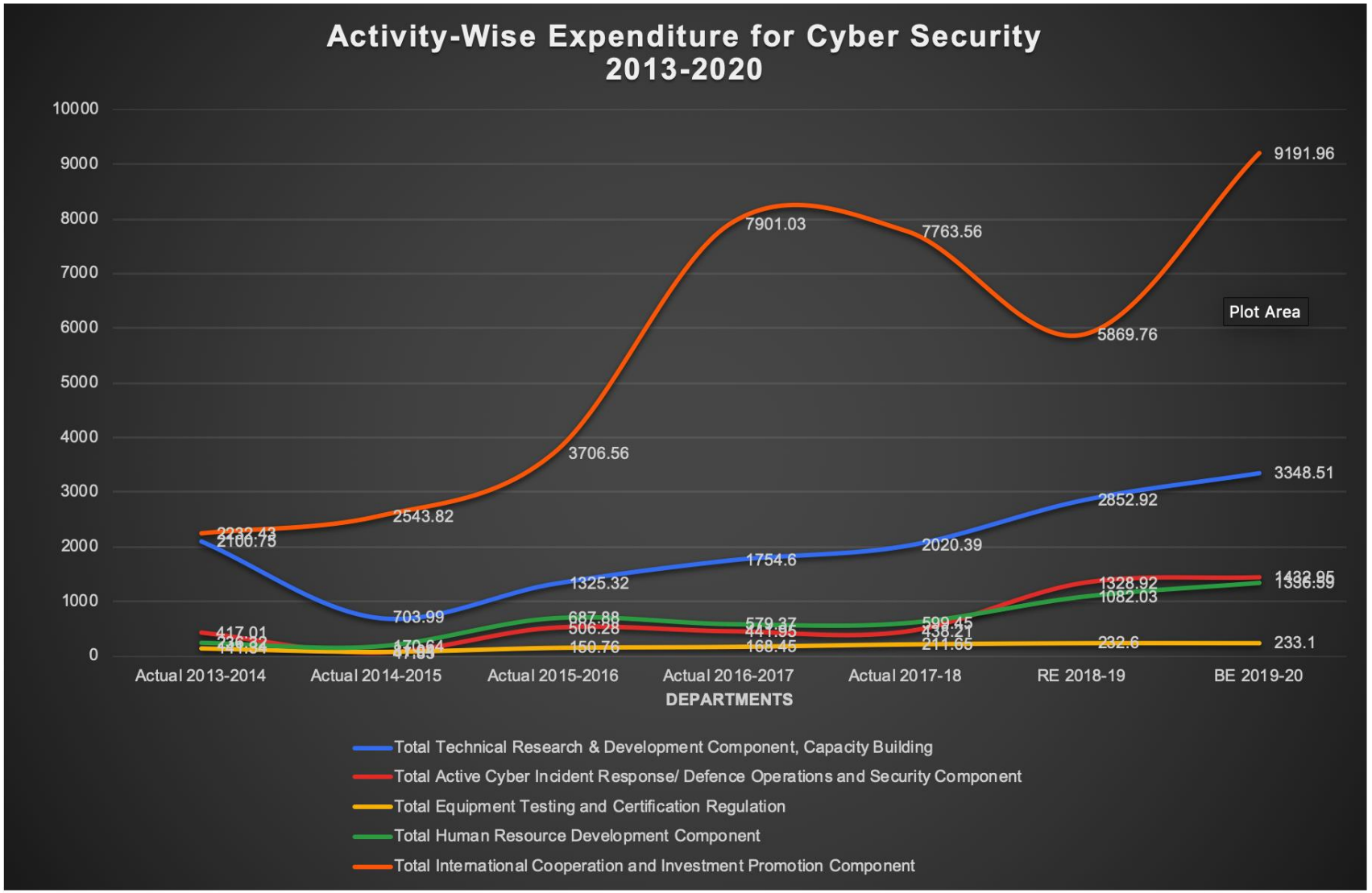


Figure 12: Activity Wise Expenditure for Cyber Security 2013-2020

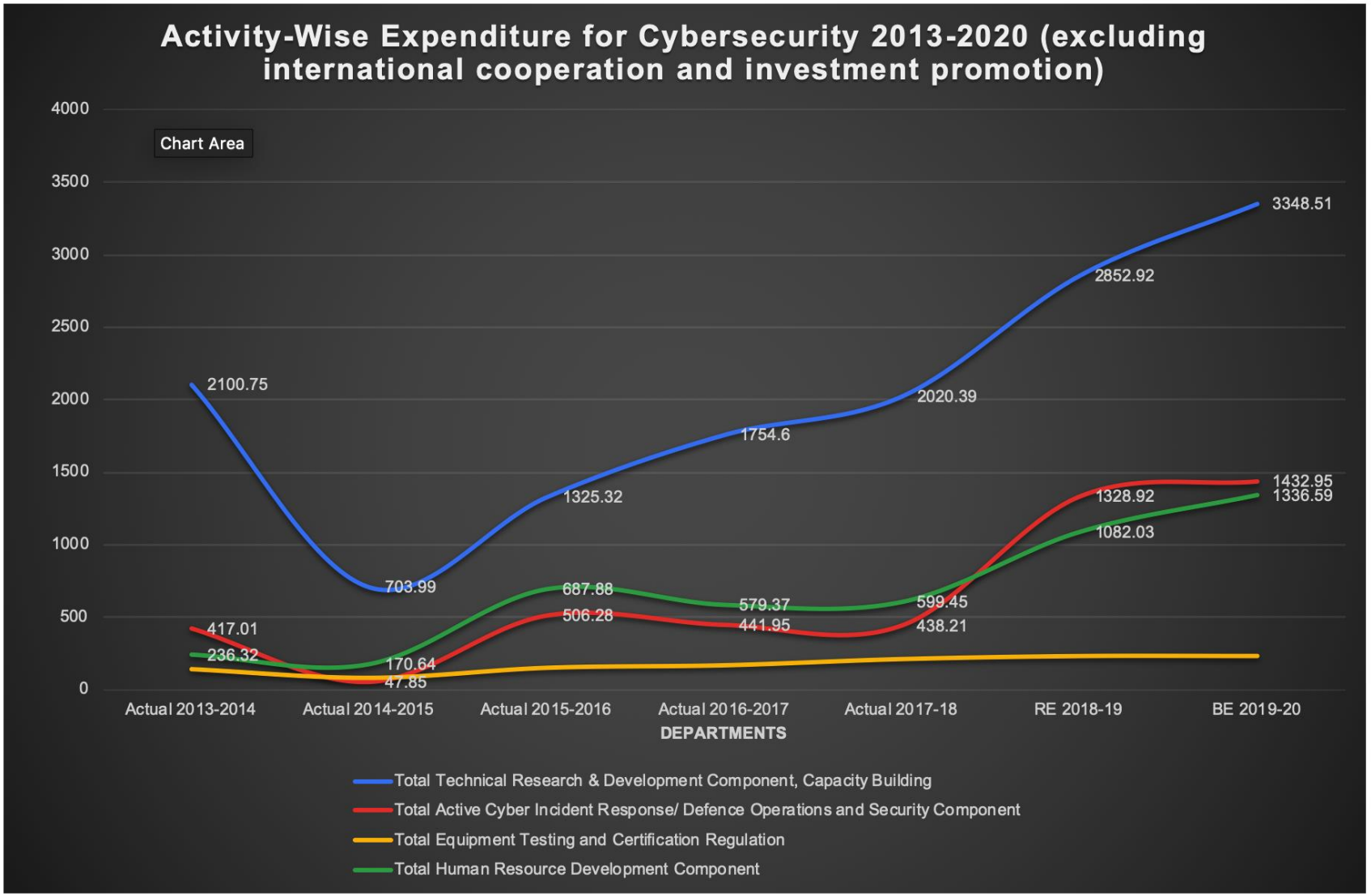


Figure 13: Activity-Wise Expenditure for Cybersecurity 2013-2020 (excluding international cooperation and investment promotion)

Figure 12 represents activity-wise trends in these Ministries' actual expenditure. The figures for FY 2018-19 and FY 2019-20 represent the RE and BE for those years, respectively. It is not surprising that the expenditure on international cooperation and investment promotion towers over all other activities, as the allocated expenses would contribute to overall cooperation efforts at the international level and the promotion of investment broadly, and not only cybersecurity. Nonetheless, these are crucial contributions to enhancing India's cybersecurity posture at home and abroad. For a clearer analysis, we remove the indicator for expenses towards international cooperation and investment promotion in Figure 13.

From Figure 13, we can clearly infer which of the four activities at the core of the Government's cybersecurity efforts are being prioritized in terms of allocation of budgetary resources. Clearly, emphasis on equipment testing and certification needs to be sharpened. There is an apparent tension between the funds that are made available for active cybersecurity operations and programmes on the one hand, and investments in human resource development on the other.

We submit that in both these areas, the Government must look to the private sector to create synergies and supplement the financial resources available for these particular activities. We also recommend that the expenditure earmarked for quality testing, development of technical standards and certification should be increased, and accorded greater priority than before.

If we try to contextualize the utilization of funds made available for cybersecurity-related activities against the total allocations to relevant Ministries, there is no identifiable trend in expenditure patterns of the MEA, MeitY and DoT. Figure 14 represents the total expenditure on cybersecurity-related activities as a percentage of the total expenses allocated to the relevant Ministry. Cybersecurity-related activities appear to be fluctuating in terms of the priority accorded to them over time, in the diversion of financial resources towards this area. The contribution of the Department of Science and Technology towards R&D in cybersecurity has been consistently low, almost negligible. This has only changed

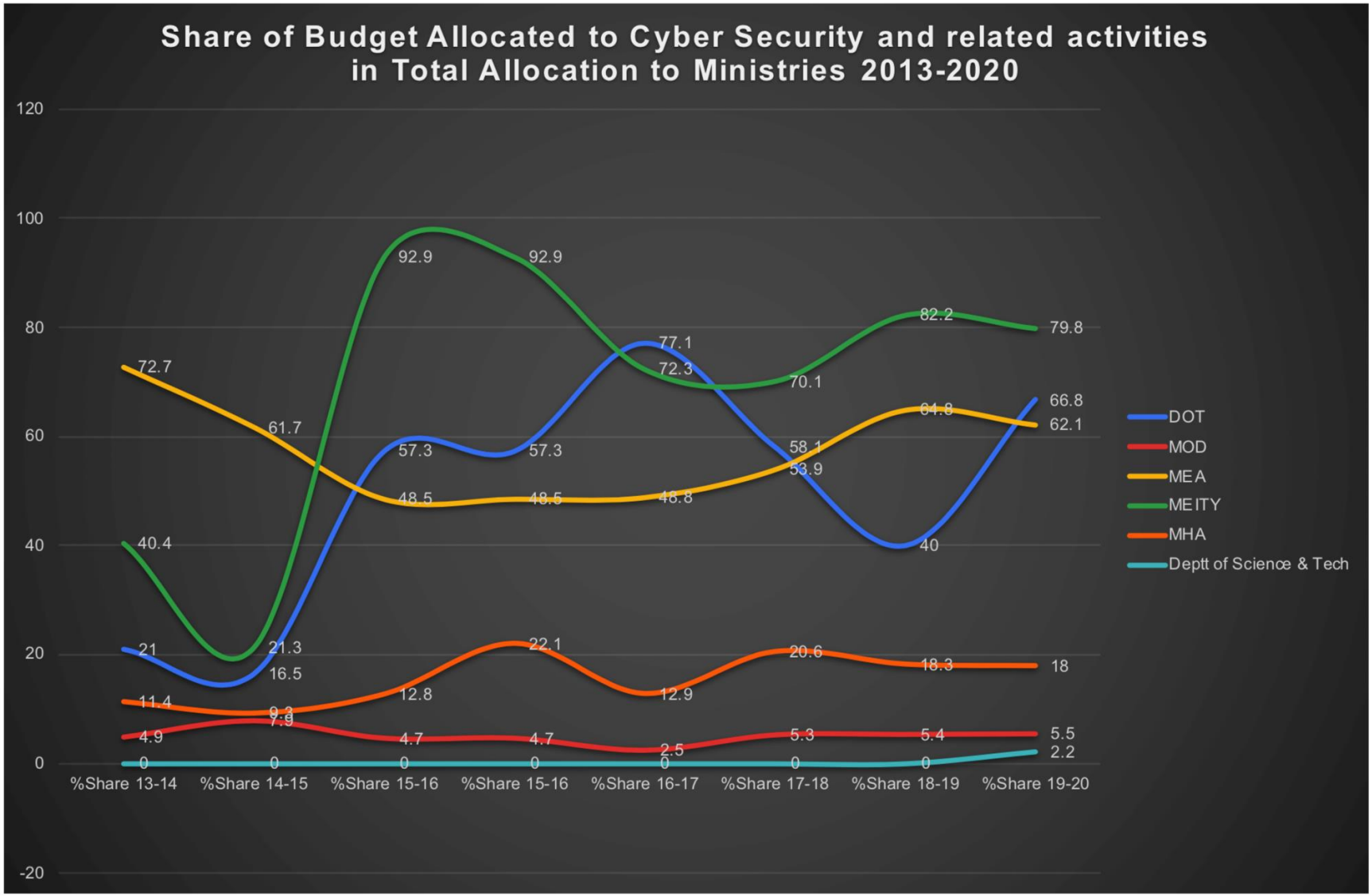


Figure 14: Share of Cybersecurity-related Activities in Total Budget Allocated to Ministries 2013-2020

with the establishment of the National Mission on Interdisciplinary Cyber Physical Systems in FY 2018-19. has been MHA's share of expenditure on cybersecurity activities appears relatively more consistent, and could potentially be leveraged to create synergies for the rationalization of expenditure across Ministries.

B. Whole-of-Nation Approach

In this section, we build further on the principle of 'Common but Differentiated responsibilities' that we proposed for consideration and adoption by the Secretariat in Part III.

The importance of cybersecurity in ensuring that levels of economic development achieved by developing economies like India remain sustainable cannot be over emphasized. In its previous iterations of policies on data protection and governance, the Government has indicated its inclination to treat data as a 'public good' or a 'national commons'. We submit that this notion can be extended to the entire realm of cyberspace, with the natural implication that the responsibility for ensuring safety and security of this realm is vested in all stakeholders. However, this common responsibility ought to take into consideration the varying levels of digital literacy across regions and sectors. We believe that the most cyber capable stakeholders are also the the ones held most responsible for ensuring peace, stability and security in cyberspace.

Therefore, we draw inspiration from the principles enshrined in the Rio Declaration of 1992 to govern "global commons" such as the high seas, Antarctica etc. to advocate for the application of the principle of Common but Differentiated Responsibility (CBDR) in this domain. Applied to realm of cybersecurity, the principle of Common but Differentiated Responsibility (CBDR) would apportion common responsibilities between multiple stakeholders across the public and private sectors for preventing and tackling malicious actors and threats in cyber space, based on their technological capacity and capabilities.

At this stage, it is imperative to clarify that we are not advocating for the application of CBDR to interpretations of due diligence obligations of States under international

law as understood in the Tallinn Manual[206], which remains at odds with our national interests.[207] Primarily, this is because such obligations under international law attach to states, but not non-state actors. The International Group of Experts who drafted the Manua assert that a state may enjoy prescriptive jurisdiction over the activities of its companies abroad, but lack the ability to control the cyber infrastructure they operate[208]. Their interpretation in practice would imply that due diligence obligations would be lowest for states with the most extensive cyber infrastructure due to the difficulties of managing and monitoring these vast networks. Effectively, this implies that the most technologically capable states would be considered least responsible for preventing cyber attacks from originating or passing through cyber infrastructure in their territory.

Admittedly, the principle originated in international environmental law, but we believe that its transposition into domestic policy would be in the interest of (1) bridging the digital divide and integrating the next half billion of the population into the networked economy and (2) identifying equitable principles to underpin the governance of cyberspace in India and through this medium, nurture the country's economic growth in a sustainable manner. CBDR is useful to ensure that the most cyber-capable stakeholders are also the ones held most responsible for the development, maintenance and protection of cyber infrastructure as well as ensuring peace, stability and security in cyberspace. This would imply that the most technologically advanced corporations would also be expected to carry the burden of cybersecurity risks associated with the use of their products and services by the population at

[206] FN

[207] The International Law Association's Study Group on Due Diligence, 7 March 2014 states at p. 27, "The due diligence standard also varies in many contexts on the basis of common but differentiated responsibilities. It is well-established that developing States may not be able to control the activities in their territory in a similar manner to developed States, and that this will effect the evaluation of whether they have breached their due diligence obligation", accessible at https://olympereseauinternational.files.wordpress.com/2015/07/due_diligence_-_first_report_2014.pdf; See also Michael N Schmitt, *In Defense of Due Diligence in Cyberspace,* The Yale Law Journal Forum, July 2015, accessible at https://www.ilsa.org/Jessup/Jessup16/Batch%202/SchmittDueDiligence.pdf; See also Scott J Shackelford; Scott Russell and Andreas Kuehn (2016) "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors," Chicago Journal of International Law: Vol. 17: No. 1, Article 1, accessible at https://chicagounbound.uchicago.edu/cjil/vol17/iss1/1/.

[208] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed. (2017), Michael N. Schmitt and Liis Vihul (eds.), Cambridge University Press (New York), at p. 33.

large. Such a principled approach to management of risks arising in privately-owned and controlled CII would also boost the domestic cybersecurity insurance sector in India, which is still in a nascent stage of development. This principle would also imply that the Government takes a sector-specific, but flexible, case-by-case view of what may be considered "reasonable security practices" based on varying levels of technological capacity of each sector of industry within the meaning of Section 31 of the draft Data Protection Bill.

A combination of policy instruments including but not limited to clearly defined contractual obligations in agreements for public-private partnership in this strategic sector, civil liability for cybersecurity breaches and fiscal/monetary incentives for the sharing of critical technologies and associated intellectual property rights, technical know-how, as well as obligations for timely information and intelligence sharing could be utilised to enforce higher levels of accountability.

Bearing in mind the presence of many foreign as well as trans-national corporations within our jurisdiction, such a principle would necessarily have ramifications that extend beyond our national borders. We delve into these concerns in the following section.

C. International Cooperation

CBDR in the realm of international relations in cyberspace would necessitate, as it did in the field of international environmental law a recalibration of expectations and conduct the most technologically advanced countries to align with a more equitable view of the global governance of cyberspace. On a theoretical level, such a principled approach would contribute to the maintenance of a rules-based order in international law and also abate what the Study Group of the International Law Commission in its 2006 report referred to as "the fragmentation of international law", arising from the diversification and expansion of international law[209]. Accordingly, we recommend that Secretariat takes appropriate steps to commission an in-depth study on how CBDR can be leveraged through the Legal and Treaties Division

[209] Report of the Study Group of the International Law Commission, *Fragmentation of International Law: Difficulties Arising from the diversification and expansion of international* law, https://legal.un.org/ilc/documentation/english/a_cn4_l682.pdf.

and/or the Policy Planning and Research Division under the MEA. A more detailed, comprehensive analysis of the potential costs and benefits of leveraging existing rights and obligations under international law would enable the Secretariat to articulate a coherent, principled position that is in line with our national interests. A principled approach would also enable us to better negotiate bilateral agreements and build coalitions for collective security arrangements with like minded nations facing similar issues in strengthening cyber capabilities.

The setting up of the New, Emerging and Strategic Technologies Division in the MEA[210] is a step in the right direction to enhance efforts to bolster international cooperation and the transfer of technologies. Under the authority of the MEA, we would also recommend, along the lines of practices of countries including the Netherlands, Australia, the appointment of a Cyber Ambassador-at-large to renew national efforts and take the lead in clearly articulating and actively protecting India's interests at multilateral and multi-stakeholder fora involved in the development and formulation of international legal norms for responsible State behavior in cyberspace.

[210] Dipanjan Roy Chaudhary, *MEA sets up Emerging Technologies Division,* The Economic Times, 2 January 2020, https://economictimes.indiatimes.com/news/politics-and-nation/mea-sets-up-emerging-technologies-division/articleshow/73063773.cms.

VI. CONCLUSION AND RECOMMENDATIONS

Bearing in mind the contemporary threat landscape for India in cyberspace and taking note of Governmental efforts to build a safe, secure, trusted, resilient and vibrant cyber space for the nation's prosperity against the backdrop of rapidly expanding militarization of cyberspace, we have thoroughly examined and reviewed relevant materials with a view to building a principled, coherent strategic framework to drive cyber policy making across the country and arrived at the following recommendations:

I. On Incidence and Reporting of Cyber Crimes and other Malicious Cyber Activity

4. Data reveals that the threats of cyber espionage as well as other economically motivated cybercrime demand the most attention from investigation and law enforcement agencies for their direct impact on economic growth.

5. We recommend that the Government address this by formulating clear directions to CERT-In and the NCRB to emphasize the need for accurate, consistent and reliable data on the incidence of cyber-crimes and other malicious cyber activity which can form the basis for evidence-based policy making for -

    a. the enforcement of law and order in cyberspace; and

    b. raise the general levels of cybersecurity awareness by widely disseminating information on the incidence of cyber-crimes to encourage reporting and self-help.

6. Overall, we also recommend that full and correct data on the incidence of cyber-crimes be made available publicly, and disseminated widely, in order that individuals may be made aware of the kinds of cyber-crime and cyber malicious activity are most prevalent in India's cyber space. This would enable taking at least basic security measures and ensure some, even if crude, form of cyber defense from attacks and intrusions.

II. The First Pillar: 'Secure'

1. CCG recommends clearly understanding and articulating stances on inter-related and inter-linked concepts such as data sovereignty and cyber sovereignty. In this regard, India should also actively monitor developments in these ongoing processes for the formulation of international norms for responsible State behaviour in cyberspace, and be prepared to take an active part in their formation and formulation.

2. India should consider the benefits of articulating its own position on international legal principles in cyberspace. To do so, we recommend that the Secretariat take up the issues of applicability of international law, especially Article 2(4) and Article 51 of the UN Charter, to cyberspace by commissioning an in-depth study of the implications thereof, as it has a significant impact on the range of legal remedies available to India in cases of State-sponsored cyber espionage and other wrongful acts in cyber space.

3. We submit for the consideration of and adoption by the Secretariat, in its formulation of the NCSS 2020, the principle of peaceful uses of cyberspace which is most consistent with protecting our national interests in cyber space as well as India's international legal obligations.

4. We also submit for consideration and adoption, the principle of 'common but differentiated responsibility' for assigning roles and responsibilities to the public and private sectors in the protection of cyberspace.

5. For conceptual and operational clarity in domestic law and policy on cyber-sovereignty, CCG submits that the Secretariat should consider demarcating the contours of "the sovereign cyberspace", as a narrower subset of the broader realm of "the national cyberspace", which remains and is most likely to remain a layer that is permeable to foreign/external actors in the networked economy. The perimeters of the "sovereign cyberspace" should include (1) defence communications and operational networks, (2) security of the intra-Government communication networks (3) security of classified and privileged information within Government Ministries, departments and/or agencies that

form part of the cybersecurity architecture, including critical data which may be notified under Section 33(2) of the Personal Data Protection Bill 2019.

6. For a better demarcation of responsibilities between first responders within the military (DCyA) and civilian sectors (NCIIPC and CERT-In), the MoD ought to notify the above listed infrastructure as explicitly entrusted to the newly-constituted Defence Cyber Agency (DCyA) for appropriate action and protective measures with appropriate directions.

7. As regards the broader "national cyberspace", we recommend that cybersecurity in this realm be treated as a public good at least until we can achieve universal digital / cybersecurity literacy, as well as endorse and adopt the principle of common-but-differentiated-responsibility (CBDR) to govern the apportionment of roles and responsibilities in and between the public and private sectors in responding to cybersecurity incidents.

8. We submit that in the interest of (1) bridging the digital divide and integrating the next half billion of the population into the networked economy and (2) evolving equitable principles to underpin the governance of cyberspace in India, the CBDR principle is useful to ensure that the most cyber-capable stakeholders are also the ones held most responsible for ensuring peace, stability and security in cyberspace.

III. The Second Pillar: 'Strengthen'

1. After an in-depth examination of the existing cybersecurity architecture, CCG concludes that greater clarity and division of responsibility is required on the protection of critical information infrastructure. The critical information infrastructure of Defence and Strategic Enterprises undoubtedly demands a higher degree of inputs from intelligence agencies, and can be retained within the MoD/ DRDO heirarchy**.** However, with respect to civilian sectors that have a bigger presence of the private sector, in view of their centrality to sustaining and promoting India's economic growth and development as well as to allow for more open and transparent public-private partnerships, we recommend that the Cyber and Information Security Division under the Ministry of Home Affairs be entrusted with this responsibility.

2. Processes such as cyber incident response, vulnerability disclosures, information sharing mechanisms and supply chain mechanisms need to be strengthened. All the nodal agencies including the NCIIPC, CERT-In and the DRDO should consistently and constantly share threat-information in a streamlined manner.

3. Further, given the hindrances to cybersecurity researchers and white hat hackers in researching vulnerabilities, we recommend that the Secretariat engage in further study of the relevant provisions under the IT Act, 2000, with a view to introducing amendments that may encourage and incentivise independent cyber security researchers to responsibly discover and report vulnerabilities and supplement the efforts of Government agencies. We also recommend the formulation of clear and instructive guidelines on vulnerability reporting across first responders in relevant government agencies.

4. We recommend that CERT-In report the progress made on its plan to establish a "a full-fledged automated Threat Information and Intelligence sharing platform for sharing Indicators of Compromise (IoCs) across stake holders".

5. Standardized supply chain security needs to be implemented across all government infrastructure on an urgent basis. This can be achieved by a re-calibration of procurement processes and procedures and bringing together required technical expertise to lay down testing and certification standards.

6. To address cyber capacity building and skilling for cyber-warriors, we recommend mainstreaming cybersecurity education at the university level through greater push to the ISEA partnership with universities, injecting more funds and increase State supported R&D to encourage the creation of innovative solutions to India's cyber security problems, as well as the private ICT.

7. We recommend that the existing pool of tech-savvy, educated professionals should be re-skilled to meet the skill gap in cybersecurity. Policy-measures for capacity building should be framed keeping in mind that this is a long-term

objective which must take into account the rapid innovations in emerging technologies including but not limited to AI, blockchain and cryptocurrencies.

8. To increase digital and cybersecurity awareness, we recommend a much wider dissemination of Common Vulnerabilties and Exposures (CVE) Reports regularly issued by the CERT-In and NCIIPC to the public at large, who should be able to opt-in and subscribe to receiving such updates in the form of periodic newsletters, or at least, urgent updates and warnings, where required.

9. We have also emphasized the importance of establishing strong and active monitoring and review mechanisms to measure progress in the achievement of strategic and policy goals.

IV. **The Third Pillar: 'Synergize'**

1. We are mindful of budgetary constraints in government expenditure on cybersecurity. These can be dealt with by looking to the private sector to create synergies that may supplement the financial capacity and technological capabilities.

2. We also recommend that the expenditure earmarked for quality testing, development of technical standards and certification should be increased, and accorded greater priority than before. Given that the MHA's share of expenditure on cybersecurity activities appears relatively more consistent, it could potentially be leveraged to create synergies for the rationalization of expenditure across Ministries.

3. While we remain cognizant of the fact that responsibility for ensuring safety and security of the cyber domain is vested in all stakeholders, the principle of Common-But-Differentiated-Responsibility (CBDR) takes into consideration the varying levels of Digital Literacy across regions and sectors. We suggest that the most cyber-capable stakeholders are also the ones to be held most responsible for ensuring peace, stability and security in cyberspace.

4. When applied to the realm of cybersecurity, the principle of CBDR would apportion common responsibilities between multiple stakeholders across the public and private sectors for preventing and tackling malicious actors and threats in cyber space, based on their technological capacity and capabilities.

5. This principle would also allow the Government to take a sector-specific, but flexible, case-by-case view of what may be considered “reasonable security practices” based on varying levels of technological capacity of each sector of industry within the meaning of Section 31 of the draft Data Protection Bill.

6. Accordingly, we recommend that the Secretariat take appropriate steps to commission an in-depth study on how CBDR can be leveraged through the Legal and Treaties Division and/or the Policy Planning and Research Division under the authority of the MEA. A more detailed, comprehensive analysis of the potential costs and benefits of leveraging existing rights and obligations under international law would enable the Secretariat to articulate a coherent, principled position that is in line with our national interests.

7. Lastly, we recommend the appointment of a Cyber Ambassador-at-large along the lines of practices of countries including the Netherlands and Australia, to renew national efforts and take the lead in clearly articulating and actively protecting India’s interests at multilateral and multi-stakeholder fora involved in the development and formulation of international legal norms for responsible State behavior in cyberspace.

CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

ANNEXURES TO THE COMMENTS TO THE NATIONAL SECURITY COUNCIL SECRETARIAT ON THE NATIONAL CYBER SECURITY STRATEGY 2020 (NCSS 2020)

AUTHORED BY

Gunjan Chawla, Programme Manager, Technology and National Security, Centre for Communication Governance at National Law University Delhi

Sharngan Aravindakshan, Programme Officer, Technology and National Security, Centre for Communication Governance at National Law University Delhi

and

Vagisha Srivastava, Research Assistant, Centre for Communication Governance at National Law University Delhi

TABLE OF CONTENTS

ANNEXURE 'A'

SUMMARIES OF CYBERSECURITY STRATEGIES OF AUSTRALIA, BRAZIL, CANADA, CHINA, FRANCE, GERMANY, ISRAEL, JAMAICA, JAPAN, NEW ZEALAND, RUSSIA, SINGAPORE, SOUTH AFRICA, SRI LANKA, THE UNITED KINGDOM, THE UNITED STATES OF AMERICA

AUSTRALIA

Country- Australia

Document Title- Australia National Cyber Security Strategy[1]

Date- 2016

Prepared By- Department of Home Affairs

PARAMETERS	CONTENTS/DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	The discernable objective of the strategy appears to be "To Secure our Prosperity in a Connected World".	P. 5
Basic Pillars	The Strategy identifies 5 themes of action- **1.** A national cyber partnership **2.** Strong cyber defences **3.** Global responsibility and influence **4.** Growth and innovation **5.** A cyber smart nation	P. 5
Identified Threats / Challenges	Not specifically identified. However, the Strategy variously refers to threats such as "malicious cyber activity" or "malicious cyber actors", "organized criminal networks, state-sponsored actors and issue motivated groups" in the context of malicious cyber actors. (P.16) The Prime Minister's Foreword has also identified "malicious cyber actors" as "serious and organized crime syndicates" and "foreign adversaries" who are using cyberspace to further their aims.	P. 15 to P. 16 P. 2
Approach specified (if any)	The Strategy explicitly adopts the multi-stakeholder approach.	P. 41
Definitions of Key Concepts	None	
Period of Validity	2016- 2020	P. 5

[1] Accessible at https://cybersecuritystrategy.homeaffairs.gov.au.

Allocated Budgetary Resources (If any)	More than $230 million	P. 3
First responders in Cyber Incident Management and Response	No entity explicitly mentioned. But the Strategy does mention boosting the "capacity of the Australian Cyber Security Centre to respond to cyber security threats and cybercrime."	P. 28
Institutions (Civilian) Institutions (Military)	The Strategy outlines the following structure – -Australian Cyber Security Coordinator for Department of Defense -Minister /Special Advisor on Cybersecurity for PMO and Cabinet -Cyber Ambassador for Foreign Engagement Scope and overlap in governance functions to be overseen by the Special Advisor on Cyber Security.	P. 24
Role of Intelligence Agencies	Not specified, but the Strategy does mention that the already existing Australian Cyber Security Centre (ACSC) brings together the Australian Government's operational cyber security capabilities in one location to share threat information and combat sophisticated cyber security threats and its partners include – • Australian Crime Commission • Australian Federal Police • Australian Security Intelligence Organisation • Australian Signals Directorate • Computer Emergency Response Team (CERT) Australia • Defence Intelligence Organisation The strategy also specifies that the Govt will establish joint cyber threat sharing centres. It also specifies a layered approach to cyber threat sharing – (i) Online cyber threat sharing portal for sharing threat information by broad range of organizations; (ii) Joint Cyber threat Centres - Australian governments, businesses and the research community partner in joint cyber threat sharing centres in key capital cities	P. 31 P. 32

	to exchange sensitive cyber threat information; (iii) Australian Cyber Security Centre- The Australian Government partners with key businesses within the Australian Cyber Security Centre to share highly classified information on critical services.	
Offensive Cyber Capabilities	Not specified	
Declared stance on international norms for responsible State behaviour in cyberspace	The Strategy acknowledges that "State behaviour in cyberspace is governed by international law and reinforced by agreed norms of state behaviour and practical confidence building measures to reduce the risk of conflict." The Strategy envisages (i) the creation of a Cyber Ambassador to better engage on international platforms and (ii) publishing an international cyber engagement strategy.	P. 41 P. 39
Declared stance on free and open nature of the internet	The Strategy states that Australia has always advocated for an open, free and secure Internet based on our values of freedom of speech, right to privacy and rule of law.	P. 41
International Cooperation and Information Sharing Mechanisms	While addressing the issue of "Global Responsibility and Influence", the Strategy acknowledges the need for international cooperation to shore up cybersecurity. The Strategy also mentions that currently- (i)Australia is a member of the Budapest Convention; (ii)CERT-Au chairs the steering committee of the Asia Pacific Computer Emergency Response Team (comprising 28 teams from 20 economies across the region) and shares threat information with other response teams around the world. (iii) The Australian Attorney-General's Department provides assistance to Pacific Island countries to reform their criminal justice frameworks to address cybercrime. (iv) Australia is taking part in global efforts to	P. 41

	prevent counter terrorism. This includes Australia being a lead partner in the East Asia Summit and Asia-Pacific Economic Cooperation's efforts to counter online extremism and combat online terrorist propaganda.	
Relationship between the public and private sector	Under the heading "National Cyber Partnership", the Strategy lists out actions that the Government will take – • host annual cyber security leaders' meetings, where the Prime Minister and business leaders set the strategic cyber security agenda and drive this Strategy's implementation. • streamline its cyber security governance and structures to improve interaction between the private and public sectors and will relocate the Australian Cyber Security Centre to allow for its growth and to enable the Government and the private sector to work more effectively together. • work with the private sector and academic community to better understand the cost of malicious cyber activity to the Australian economy.	P.21
Preventive measures for cyber crime	The Strategy recognizes the need for "Strong Cyber Defences" and lists out the priority actions to achieve this as – (i) Detect, deter and respond: Open jointly operated cyber threat sharing centres and an online cyber threat sharing portal. Tackle cyber threats with improved intelligence, analytic and response capability. (ii) Raise the bar: Co-design voluntary cyber security governance 'health checks', national good practice guidelines, conduct joint exercisers and develop and leverage advanced technology to make Australia a harder target against cyber threats. Conduct cyber security assessments of Government agencies.	P. 11 P. 32

	Specifies layered approach to cyber threat sharing – (iv) Online cyber threat sharing portal for sharing threat information by broad range of organizations; (v) Joint Cyber threat Centres - Australian governments, businesses and the research community partner in joint cyber threat sharing centres in key capital cities to exchange sensitive cyber threat information; (vi) Australian Cyber Security Centre- The Australian Government partners with key businesses within the Australian Cyber Security Centre to share highly classified information on critical services. Other Preventive Measures- The Government is committed to equipping the Australian Cyber Security Centre with the resources and tools it needs to fight the rising tide of malicious cyber activity and keep our cyberspace safe. The Government will boost the capacity of the ACSC agencies to tackle cyber security threats by: • increasing the capacity of the national Computer Emergency Response Team (CERT) Australia to scale up their work with Australian businesses, in particular those providing critical services. The additional capacity will also improve CERT Australia's technical capability to support businesses and to partner internationally to prevent and shut down malicious cyber activity; and • funding new specialist officers for the Australian Crime Commission and the Australian Federal Police to tackle cybercrime. There will also be new training, including new modules in entry colleges and eLearning for existing personnel, which will boost the digital investigation skills of specialist officers to create a cyber smart law enforcement and criminal intelligence workforce.	P. 33
Investigation of and punitive measures for	None specified.	

cyber crime		
Status of Data Protection Laws	Not specified. Interestingly, the Prime Minister's foreword states that external malware isn't the Government's biggest risk but whistleblowers or "warmware" are. Quoted text – "*As the Snowden disclosures demonstrate, often the most damaging risk to government or business online security is not 'malware' but 'warmware'; the ability of a trusted insider to cause massive disruption to a network or to use legitimate access to obtain classified material and then illegally disclose it.*"	P. 2
Skilling and Capacity Building for Cybersecurity Personnel	Recognizing the importance of becoming a "Cyber Smart Nation" as a goal, the Strategy refers to measures such as – • addressing the shortage of cyber security professionals in the workforce through targeted actions at all levels of Australia's education system, starting with academic centres of cyber security excellence in universities and by increasing diversity in this workforce. • working with the private sector and international partners to raise awareness of the importance of cyber security across our community. The Strategy addresses these in detail under the heads "Develop the right skills and expertise" and "Raise National Cyber Security and Awareness".	(P. 51) P. 53-55
Economic Growth of the ICT sector generally	The Strategy recognizes the need for "Growth and Innovation." To achieve this, the priority actions are – (i) Enable Cybersecurity Innovation - Drive investment in cyber security innovation through the Cyber Security Growth Centre and innovation network to strengthen cyber defences, grow our economy and create jobs.	P. 10

	(ii) Enable cyber security businesses to develop and expand - Support new businesses and promote the export of Australian cyber security products and services. (iii) Enable cyber security research and development- Ensure our cyber security R&D is responsive to the challenges.	
Approach to foreign investment	Not specified	
Supply chain risk management	As one of the measures to develop a "Strong Cyber Defence", the Strategy recognizes the need for support to Government agencies to improve their cyber security, including guidance for Government agencies to manage supply chain security risks for ICT equipment and services.	P.28
Government initiatives, campaigns and programmes for cyber space	Cyber Security Challenge Australia (organized by the Government in partnership)	P. 54
Other relevant strategies or policy documents	National Cyber Strategy Action Plan Cloud Computing Policy 2014 (mandating cloud first policy for all government agencies and stressing the security of cloud services)	P. 57 P. 19

BRAZIL

Country- Brazil

Document Title- National Information Security Policy ("PNSI")[2]

Date- 2018

Prepared By- Deputy Head of Legal Affairs, General Secretariat, Presidency of the Republic

PARAMETERS	CONTENTS / DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	Ensuring the availability, integrity, confidentiality and authenticity of information at the national level. Objectives - I - contribute to the security of the individual, society and the State, through the orientation of information security actions, observing the fundamental rights and guarantees; II - foster scientific research, technological development and innovation activities related to information security; III - continuously improve the legal and normative framework related to information security; IV - promote the formation and qualification of the human resources necessary for the area of information security; V - strengthen the culture of information security in society; VI - guide actions related to: a) security of data held by public entities;	Article 1, Chapter 1 Article 4, Chapter III

[2] Original Document in Portuguese, translated to English via Google Translate and accessible at http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Decreto/D9637.htm.

	b) information security of critical infrastructures; c) protection of information of individuals who may have their security or the security of their activities affected, subject to specific legislation; and d) processing of information with restricted access; and VII - contribute to the preservation of the Brazilian cultural memory.	
Basic Pillars	While the Strategy does not use the term “pillars”, it does identify the following principles – I - national sovereignty; II - respect and promotion of human rights and fundamental guarantees, in particular freedom of expression, the protection of personal data, the protection of privacy and access to information; III - comprehensive and systemic view of information security; IV - Country responsibility for coordinating efforts and establishing policies, strategies and guidelines related to information security; V - scientific and technological exchange related to information security between the organs and entities of federal public administration; VI - preservation of the national historical collection; VII - education as a fundamental foundation for fostering culture in information security; VIII - orientation to risk management and information security management; IX - prevention and treatment of information security incidents; X - articulation between cyber security, cyber defense and data protection and information assets actions; XI - the duty of public bodies, entities and agents to ensure the confidentiality of information essential to the security of society and the State and the inviolability of the privacy of privacy, honour and image of persons; XII - need to know for access to confidential	Article 3, Chapter II.

	information, under the terms of the legislation; XIII - consent of the owner of confidential information received from other countries, in the cases of international agreements; XIV - cooperation between investigative bodies and public bodies and entities in the process of accreditation of persons for access to confidential information; XV - integration and cooperation between the Government, the business sector, society and academic institutions; and XVI - international cooperation in the field of information security.	
Identified Threats / Adversaries	Not specified.	
Approach specified (if any)	Approach is not expressly specified. However, the Strategy appears to adopt the multi-stakeholder approach from the following – Integration and cooperation between the Government, the business sector, society and academic institutions is identified as a principle. Further, The construction of the National Information Security Strategy will have the broad participation of society and the public authorities.	 Article 3(XV), Chapter II Article 6, Chapter IV
Definitions of Key Concepts	The term “Information Security” is defined to include cyber security, cyber defense, physical security and protection of organizational data and actions designed to ensure the availability, integrity, confidentiality and authenticity of information.	Article 2, Chapter I
Period of Validity	Not specified	
Allocated Budgetary Resources (If any)	Not specified	
First responders in Cyber	Not specified	

Incident Management and Response		
Institutions (Civilian)	The Strategy identifies the following institutes – a) Office of Institutional Security of the Presidency of the Republic (advised by the Information Security Steering Committee) to establish macro-level policies and strategies for information security as well as to establish minimum security requirements for product use; b) Information Security Committee to deliberate on matters related to the Strategy	Article 12, Section I, Chapter VI Article 15(IV), Section IV, Chapter VI
Institutions (Military)	The Strategy identifies the Ministry of Defense for Office of Institutional Security of the Presidency of the Republic in activities related to cyber security as well as elaborating the defense guidelines, devices and procedures that act in the systems related to the national defense against cyber attacks.	Article 13(II), Section II, Chapter VI
Role of Intelligence Agencies	Not specified	
Offensive Cyber Capabilities	Not specified	
Declared stance on international norms for responsible State behaviour in cyberspace	Not specified	
Declared stance on free and open nature of the internet	The Strategy identifies as one of its principles “respect and promotion of human rights and fundamental guarantees, in particular freedom of expression, the protection of personal data, the protection of privacy and access to information.”	Article 3(II), Chapter II
International Cooperation and	Not specified. The Strategy only recognizes “International cooperation in the field of information	Article 3(XVI), Chapter II

Information Sharing Mechanisms	security" as a principle. Not a member of the Budapest Convention.	
Relationship between the public and private sector	Not specified	
Preventive measures for cyber crime	Not specified. The Strategy only recognizes "prevention and treatment of information security incidents" as a principle.	Article 3(IX), Chapter II
Investigation of and punitive measures for cyber crime	Not specified. The Strategy only recognizes cooperation between investigative bodies and public bodies and entities "in the process of accreditation of persons for access to confidential information" as a principle.	Article 3(XIV), Chapter II
Status of Data Protection Laws	While coherence between data protection, cyber security, cyber defense is identified as a principle, data protection framework is not dealt with.	Article 3(X), Chapter II
Skilling and Capacity Building for Cybersecurity Personnel	No measures fleshed out, but the Strategy mandates implementing training government officials.	Article 12, Chapter VI
Economic Growth of the ICT sector generally	Not specified	
Approach to foreign investment	Not specified	
Supply chain risk management	Not specified	
Government initiatives, campaigns	Not specified	

and programmes for cyber space		
Other relevant strategies or policy documents	Not specified	

CANADA

Country- Canada

Document Title- National Cyber Security Action Plan (2019-2024) and National Cyber Security Action Plan (2019-2024)[3]

Date- 2019

Prepared By- Department of Public Safety and Emergency Preparedness

PARAMETERS	CONTENTS / DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	To achieve *security and prosperity in the digital age.*	P. 2
Basic Pillars	The Strategy emphasizes on the following pillars – • **Secure and Resilient Canadian Systems**: with enhanced capabilities and in collaboration with partners, the Government of Canada will better protect Canadians from cybercrime, respond to evolving threats, and help defend critical government and private sector systems. • **Cyber Innovation**: The Government of Canada will support advanced research, foster digital innovation, and develop cyber skills and knowledge to position Canada as a global leader in cyber security. • **Leadership and Collaboration**: In collaboration with provinces, territories, and the private sector, the federal government will take a leadership role to advance cyber security in Canada, and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour.	P. 17 P. 19 P. 26
Identified Threats / Challenges	The Strategy broadly identifies threats as including individual hackers and insider threats, criminal networks, nation states, terrorist organizations, and state-sponsored actors.	P. 12

[3] Accessible at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

Approach specified (if any)	Not specified.	
Definitions of Key Concepts	The Strategy's Glossary defined the following terms – App/Application, AI, Blockchain, Cloud Computing, Critical Infrastructure, Cyber Attack, Cyber Incident, Cyber Security, Cyber Threat, Cybercrime, Cyberspace, Data Breach, DDOS, e-commerce, encryption, hacker, insider threat, intellectual property, internet of things, malicious software/malware, quantum computing, ransomware, smart cities, spear phishing, phishing.	P. 33
Period of Validity	2019-2024	
Allocated Budgetary Resources (If any)	Budget 2018 allocated $500 million over five years.	Page II (Foreword)
First responders in Cyber Incident Management and Response	Not identified.	
Institutions (Civilian)	Not identified.	
Institutions (Military)	Not identified.	
Role of Intelligence Agencies	Not identified.	
Offensive Cyber Capabilities	Not identified.	
Declared stance on international norms for responsible State behaviour in cyberspace	Not specified.	
Declared stance on free and open nature of the internet	Yes, the Strategy acknowledges the need for a free internet.	P. 32

International Cooperation and Information Sharing Mechanisms	Not specified. A member of the Budapest Convention.	
Relationship between the public and private sector	The Strategy talks about boosting the private sector in broad terms.	P. 26-29
Preventive measures for cyber crime	The Government of Canada will maintain and improve cyber security across all federal departments and agencies to protect the privacy of Canadians' information held by the federal government and the confidentiality, integrity, and availability of critical services for Canadians. The Government of Canada will enhance law enforcement capacity to respond to cybercrime. It will support coordination across law enforcement agencies and with federal, provincial, territorial, and international partners. The Government will enhance cybercrime investigative capacity and make it easier for Canadians to report cybercrime. Small and medium organizations often lack the knowledge and resources to implement cyber security regimes, even if doing so would offer a competitive advantage. The Government of Canada will help support these organizations — making cyber security more accessible. In response to cyber threats of increasing sophistication, the Government of Canada will consider how its advanced cyber capabilities could be applied to defend critical networks in Canada and deter foreign cyber threat actors. Some cyber systems — such as electricity grids, communications networks, or financial institutions — are so important that any disruption could have serious consequences for public safety and national security. The federal government will work with provinces, territories, and the private sector to help define requirements to protect this digital infrastructure.	P. 17 P. 18
Investigation of and	Not specified.	

punitive measures for cyber crime		
Status of Data Protection Laws	Not specified.	
Skilling and Capacity Building for Cybersecurity Personnel	The demand for qualified cyber security professionals is surging. A global shortage of qualified professionals represents an immediate and growing opportunity for Canada's highly educated workforce. We can encourage more students to move into science, technology, engineering, and mathematics (STEM) fields. We can encourage graduates from both STEM programs and other disciplines (such as psychology, sociology, or management) to specialize in the skills needed for cyber security jobs. Attracting this multidisciplinary talent, both domestically and from abroad, is essential for Canadian governments and businesses. It also helps to ensure that Canadian companies are able to safely grow and innovate as they expand their use of digital technology.	P. 22
Economic Growth of the ICT sector generally	Under the umbrella of “Cyber Innovation”, the Strategy broadly outlines the need to build on the benefits of digital technology. Specifies research focus on quantum computing and blockchain technology.	P. 19
Approach to foreign investment	Not specified.	
Supply chain risk management	Nothing specified. However, the Strategy briefly acknowledges “commercial supply chains” as being important in the Foreword.	P. II (Foreword)
Government initiatives, campaigns and programmes for cyber space	The Strategy mentions the “Get Cyber Safe” campaign as an awareness-outreach measure under the previous strategy (2010).	P. 6
Other relevant	National Cyber Security Action Plan (2019-2024).	

strategies or policy documents	(Not mentioned in the Strategy)	

CHINA

Country- China

Document Title- National Cyberspace Security Strategy[4]

Date- 27 December 2019

Prepared By- Cyberspace Administration of China, approved by the Central Network Security and Informatization Leading Group

PARAMETERS	CONTENTS / DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	"Through active and effective international cooperation, we will establish a multilateral, democratic and transparent international Internet governance system to jointly build a peaceful, secure, open, cooperative and orderly network space." Guided by the overall national security concept, the Strategy aims to implement the development concepts of innovation, coordination, greenness, openness, and sharing, enhance risk awareness and crisis awareness, coordinate the two domestic and international situations, coordinate the two major events of security development, and actively defend and respond effectively. Promote peace, security, openness, cooperation, and order in cyberspace, safeguard national sovereignty, security, and development interests, and achieve the strategic goal of building a cyber power.	Conclusion/last sentence The Goal
Basic Pillars	Xi Jinping's "Four Principles" on advancing the transformation of the global Internet governance system and the "five-point proposition" of (1) building a community of shared destiny in cyberspace (2) clarify China's major position on the development	

[4] Original in Chinese, translated into English via Google Translate and accessible at https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

	and security of cyberspace (3) guide China's cybersecurity work, and (4) maintain the State's sovereignty, security, and development interests in cyberspace. The Strategy articulates and operationalizes the following principles: (1) Respect for maintaining cyberspace sovereignty (2) Peaceful use of cyberspace (3) Governing cyberspace according to law Coordinating network security and development	
Identified Threats / Challenges	Asserts that national sovereignty extends to cyberspace, and that cyberspace sovereignty has become an important part of national sovereignty. Cyberspace, as the new territory of national sovereignty presents the challenges in the following domains: (1) Network penetration to interfere in internal affairs, large scale network monitoring, and [data] theft harms **political** security (2) Cyber attacks against critical infrastructure and networks threaten **economic** security (3) Harmful information on the Inter net erodes **cultural** security and threatens traditional culture and mainstream values (4) Cyber terror and illegal crimes undermine **social** [order, harmony, stability and] security **International** competition for control of strategic resources in cyberspace is on the rise; individual countries have strengthened their network deterrence strategies and intensified the cyber arms race.	
Approach specified (if any)	None specified. However, the strategy endorses four (multilateral) principles as anchoring its approach: (1) Respect for maintaining cyberspace sovereignty, which it considers 'inviolable' (2) Peaceful use of cyberspace is considered in the common interest of mankind, all countries should jointly resist the cyberspace arms race and prevent cyberspace conflicts (3) Governing cyberspace according to law to promote the rule of law in cyberspace (4) Coordinating network security and development through informatization.	

Definitions of Key Concepts	None	
Period of Validity	Not specified	
Allocated Budgetary Resources (If any)	Not specified	
First responders in Cyber Incident Management and Response	Not explicitly stated, but mentions the building of a "network space protection force" (Cyber Defence Force?)	Eighth Strategic Task
Institutions (Civilian)	Not specified. However, the Strategy places emphasis on protection of critical information infrastructure, considered the responsibility of the government, enterprises and the whole society.	
Institutions (Military)	Not specified. However, the Strategy places emphasis on protection of critical information infrastructure, considered the responsibility of the government, enterprises and the whole society.	
Role of Intelligence Agencies	Not specified.	
Offensive Cyber Capabilities	Not specified, endorses the principle of peaceful uses of cyberspace. Emphasizes the vigorous development of network security defense methods, timely discovery and resistance of network intrusions and building a strong backing for national security.	Second Principle Eighth Strategic Task
Declared stance on international norms for responsible State behaviour in cyberspace	Endorses the principle of peaceful uses of cyberspace. Mandates that the State "make more use standards to standardize cyberspace behaviour". Aims to strengthen international cyberspace dialogue and cooperation and promote the transformation of the Internet global governance	Second Principle Seventh Strategic Task Ninth Strategic

	system on the basis of mutual respect and mutual trust. Envisions China playing a leading role in supporting the United Nations to promote the development of universally accepted international rules on cyberspace, cyberspace international counter-terrorism conventions, sound judicial assistance mechanisms against cybercrime, deepening policy and law, technological innovation, standards and norms, emergency response, and critical information infrastructure International cooperation in areas such as protection. As regards public attribution, the Strategy makes a reference to "individual countries" having strengthened their network deterrence strategies and intensified the cyberspace arms race.	Task Challenges
Declared stance on free and open nature of the internet	No such stance declared, but the Strategy links cyberspace security to "the common interests of mankind".	Second para.
International Cooperation and Information Sharing Mechanisms	A safe, stable and prosperous cyberspace is of great significance to countries and the world. China is willing to work with other countries to strengthen communication, expand consensus, deepen cooperation, actively promote the reform of the global Internet governance system, and jointly maintain peace and security in cyberspace. The strategy recognizes that "All countries in the world have closer cooperation in the fields of technology exchange, combating cyber terrorism and cybercrime. The multilateral, democratic and transparent international Internet governance system is sound and perfect, and the cyberspace destiny community with cooperation and win-win as the core has gradually formed." Aims to deepen bilateral and multilateral network security dialogues and information exchanges with countries, effectively managing difference and actively participating in global and regional organisations' network security cooperation, and promote the internationalization of basic resource management such as Internet addresses and root	Ninth Strategic Task

	name servers. Intends to strengthen support for Internet Technology diffusion and infrastructure construction in developing and underdeveloped regions, and strive to bridge the digital divide. Establish a global Internet sharing and governance platform, such as the World Internet Conference, to jointly promote the healthy development of the Internet Not a member of the Budapest Convention.	
Relationship between the public and private sector	Seeks to establish an orderly sharing mechanism for cybersecurity information of government, industry and enterprises, and give full play to the important role of enterprises in protecting key information infrastructure. Mentions the conduct of security reviews on important information technology products and services purchased by party and government organs key industries. (under "Protection of critical information infrastructure")	Third Strategic Task
Preventive measures for cyber crime	Strengthening the network's anti-terrorism, anti-spyware and anti-stealing capabilities, and cracking down in cyber terror and cyber espionage activities is one of the strategic tasks outlined in the strategy. It includes severe crack downs on illegal activities such as cyber fraud, cyber theft, drug trafficking, infringement of citizen's personal information, dissemination of obscene pornography, hacking, infringement of intellectual property rights.	Fifth Strategic Task
Investigation of and punitive measures for cyber crime		Fifth Strategic Task
Status of Data Protection Laws	Not specified, but seeks to improve he security and controllability of products and services, and prevent product and service providers and other information organizations from exploiting unfair competition or harming the interests of users.	Third Strategic Task

Skilling and Capacity Building for Cybersecurity Personnel	Mentions an increased investment in management, technology, talents, funds etc. (Protection of critical information infrastructure) Vigorously carry out the national network security publicity and education. Promote cybersecurity education into teaching materials, enter the school, enter the classroom, improve the network media literacy, enhance the cyber security awareness and protection skills of the whole society.	Third Strategic Task Seventh Strategic Task
Economic Growth of the ICT sector generally	Recognizes that network and information systems have become the backbone of critical infrastructure and even the entire economic society. Seeks to encourage the development of new business, create new products, create a network culture brand that reflects the spirit of the times, and continuously improve the scale of the network culture industry. (under "strengthening the construction of network culture") Adhere to innovation-driven development, pool resources and strength, take enterprise as the main body, combine production, study and research, coordinate research… and make breakthroughs in core technologies as son as possible… Vigorously develop network economy. (under "Consolidating the foundation of network security")	Challenges Fourth Strategic Task Seventh Strategic Task
Approach to foreign investment	Not specified.	
Supply chain risk management	Yes, seeks to strengthen supply chain security management. Pay attention to software security and accelerate the promotion and application of secure and trusted products.	Third Strategic Task. Seventh strategic task.
Government initiatives, campaigns and programmes for cyber space	"The Internet+" initiative The network security talent project	Seventh Strategic Task

Other relevant strategies or policy documents	Plans to improve network security laws and regulations system, and formulate laws such as the Cyber Security Law and the Minor Network Protection Regulations, clarify the responsibilities and obligations of all aspects of society, and clarify the requirements for network security management. (Improve the network governance system)	Sixth Strategic Task
	Mentions a “national big data strategy”	Seventh Strategic Task
	Promote the construction of the “Belt and Road”, improve the level of international communication and interconnection, and smooth the information silk road.	Ninth Strategic Task

FRANCE

Country- France

Document Title- French National Digital Security Strategy[5]

Date- 2015

Prepared By- French National Cybersecurity Agency (ANSSI)

PARAMETERS	CONTENTS / DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	5 objectives identified - - to ensure France's freedom of expression and action as well as the security of its critical infrastructures in case of a major cyberattack; - to protect the digital lives of citizens and businesses and combat cyber-criminality; - to ensure the education and training required for digital security; - to contribute to the development of an environment that is conducive to trust in digital technology; - to promote cooperation between Member States of the European Union (EU) in a manner favourable to the emergence, of a European digital strategic autonomy, a long-term guarantor of a cyberspace that is more secure and respectful of our values.	P. 9
Basic Pillars	No pillars discernible from the Strategy.	
Identified Threats / Challenges	Not identified.	

[5] Accessible at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/information-systems-defence-and-security-frances-strategy.

Approach specified (if any)	The Strategy does not use the term "multi-stakeholder" but acknowledges the importance of "collective responsibilities of three communities of stakeholders".	P. 8
Definitions of Key Concepts	None defined.	
Period of Validity	Not specified.	
Allocated Budgetary Resources (If any)	Not specified	
First responders in Cyber Incident Management and Response	The Strategy indicates that the ANSSI will be the responding agency.	P. 33
Institutions (Civilian) Institutions (Military)	ANSSI already existing and is the "identified State contact in case of serious cybersecurity incidents that affect the ad- ministrations and operators of vital importance". Strategy envisages creation of – (i) Expert Panel for Digital Trust (Civilian)- - Under State Secretariat for Digital Technology and the National Authority for the Security of Information Systems. - Multistakeholder in nature. The Strategy identified its functions as the following- (a) identify the key technologies for which in-depth knowledge is required for cybersecurity professions; (b) evaluate the initial and continuing education needs, will monitor Research; (c) Will be implemented along with industry orgs like French Security Industries Sector Association (CoFIS). (ii) MoD + National Authority on Information Systems Security (Military) -Will continue to implement a cyber defence reserve	P. 15

	for operational purposes to face major information technology crises. (iii) Mentions the EU-CERT and NATO as being responsible for cyber defence of "their respective institutions"	P. 17 P. 17
Role of Intelligence Agencies	Apart from National Authority on Information Systems Security, the Strategy also mentions the European Union Agency for Network and Information Security (ENISA)	P. 17
Offensive Cyber Capabilities	Not specified.	
Declared stance on international norms for responsible State behaviour in cyberspace	Acknowledges the applicability of international law to cyberspace. Nothing specified on public attribution.	P. 8, 38, 40
Declared stance on free and open nature of the internet	Yes, the Strategy adopts a free-and-open-internet stance.	P. 21
International Cooperation and Information Sharing Mechanisms	The Strategy mentions the following in this regard – - Advance Budapest Convention mechanisms for better information sharing. - NATO and ENISA also mentioned as international cooperation frameworks to be utilized. A member of the Budapest Convention.	P. 23
Relationship between the public and private sector	The Strategy fleshes out the following measures regarding public private cyber-relationship – - Developing and accentuating the national and European offer of security products and services.	P. 31- 34

	- Transferring acquired knowledge to the private sector to contribute to the handling of its cybersecurity. - Preparing a safer digital world through better anticipation of uses, adapted support and stakeholders' information. - Integrating the requirements for cybersecurity in public contracting and support. - Supporting export and internationalisation of the businesses in the sector.	
Preventive measures for cyber crime	The Strategy fleshes out the following measures – - Advocating and defending our values on electronic communication networks and in international proceedings. - Providing local assistance to victims of cyber-malevolent acts. - Measuring cybercrime. - Protecting the digital lives, privacy and personal data of the French people. - Recommending technical solutions aimed at securing digital life and which are accessible to all businesses and the general public. - Reinforcing the operational mechanisms of legal international mutual aid and universalising the principles of the Budapest Convention on Cyber-crime.	P. 21- 23
Investigation of and punitive measures for cyber crime	Not specified. Apart from prosecution.	P. 7
Status of Data Protection Laws	The Strategy dedicates a portion to the European Regulation on electronic identification (eIDAS - Electronic Identification and Trust Services) and how France will establish a clear road map for "digital identity delivered by the State".	P. 22- 23

	The Strategy also states that “an identification system adapted and shared with the participating States and consistent with the European work carried out in the framework of the European Regulation related to the protection of personal data will be established during 2016.”	
Skilling and Capacity Building for Cybersecurity Personnel	- Raising the awareness of all French people. - Integrating cybersecurity awareness into all higher and continuing education programmes. - Integrating cybersecurity training into all higher education that includes some information technology. - Recording and anticipating the initial and continuing education needs.	P. 26-27
Economic Growth of the ICT sector generally	(Refer Relationship between Public and Private Sectors)	
Approach to foreign investment	While no particular approach is specified, the Strategy makes a mention of 5G tech and stresses on the importance of privacy of citizens. The Strategy also specifies that the National Authority on Information Systems Security to monitor and inform of factors that might present a danger in terms of digital use.	P. 15
Supply chain risk management	Not addressed specifically. But the Strategy recognizes the importance of secure services. Further, privacy of citizens stressed. National Authority on Information Systems Security to monitor and inform of factors that might present a danger in terms of digital use.	P. 15
Government initiatives, campaigns and programmes for cyber space	Not specified.	

Other relevant strategies or policy documents	The Strategy mentions a White Paper on Defence and National Security in 2008.	

GERMANY

Country- Germany

Document Title- Cyber Security Strategy for Germany[6]

Date- 2011

Prepared By- Federal Ministry of the Interior, Berlin

PARAMETERS	CONTENTS / DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	Not explicitly stated, but the Strategy in the Introduction states that it is intended to improve the framework conditions of availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace and ensuring cyber security.	P. 2
Basic Pillars	No basic pillars identified. But, the Strategy outlines the philosophy of the Strategy under "Basic Principles of the Cybersecurity Strategy" which includes "making a substantial aim to secure cyberspace" by the Federal Govt and "maintaining and promoting economic and social prosperity in Germany.	P. 4
Identified Threats / Challenges	The Strategy broadly identifies threats as including "criminals, terrorists and spies". The Strategy also acknowledges possibility of "military operations" being behind attacks. The Strategy also explicitly mentions the Stuxnet example in the context of the importance of critical information infrastructures.	P. 3

[6] Accessible at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany.

Approach specified (if any)	Not explicitly, but the Strategy refers to different stakeholders and the need for coordination.	P. 8
Definitions of Key Concepts	The Strategy defines cybersecurity as "*the sum of all national and international measures taken to protect the availability of information and communications technology and the integrity, authenticity and confidentiality of data in cyberspace.*" Other defined terms include cyberspace, Cyberattack, cyber espionage and cyber sabotage, Cyber security and civilian and military cyber security and critical infrastructures.	P. 4
Period of Validity	Not specified.	
Allocated Budgetary Resources (If any)	Not specified.	
First responders in Cyber Incident Management and Response	Not specified. But it appears from the Strategy that the National Cyber Response Centre may possibly play a role.	P. 8
Institutions (Civilian) Institutions (Military)	The Strategy identifies the following organizations – (a)National Cyber Response Centre:- *Hierarchy*- will report to the Federal Office for Information Security (BSI) and cooperate directly with the Federal Office for the Protection of the Constitution (BfV) and the Federal Office of Civil Protection and Disaster Assistance (BBK). *Functions*- (i)Quick and close information sharing on weaknesses of IT products, vulnerabilities, forms of attacks and profiles of perpetrators enables the National Cyber Response Centre to analyse IT incidents and give consolidated recommendations for action; (ii) the Cyber Response Centre will submit recommendations to the National Cyber Security Council both on a regular basis and for specific incidents. If the cyber security situation reaches the	P. 9- 10

	level of an imminent or already occurred crisis, the National Cyber Response Centre will directly inform the crisis management staff headed by the responsible State Secretary at the Federal Ministry of the Interior. (b)National Cyber Security Council:- Will comprise members of both the government, private actors and academia if required (P. 9). The National Cyber Security Council is intended to coordinate preventive tools and the interdisciplinary cyber security. approaches of the public and the private sector. The National Cyber Security Council will complement and interlink IT management at federal level and the work of the IT Planning Council in the area of cyber security at a political and strategic level.	
Role of Intelligence Agencies	Not specified.	
Offensive Cyber Capabilities	Not specified.	
Declared stance on international norms for responsible State behaviour in cyberspace	The Strategy mentions a “code for state conduct in cyberspace (cyber code)” that should be established, which is signed by as many countries as possible and includes confidence- building security measures. The Strategy also mentions current G8 efforts on anti-botnet activities. Nothing specified on public attribution.	P. 11
Declared stance on free and open nature of the internet	Not specified.	
International Cooperation and Information Sharing Mechanisms	The Strategy stresses the need for a Euro-centric cybersecurity approach through ENISA (European Network and Information and Agency) and the “pooling of IT competences in EU institutions”, the EU Internal Security Strategy and the Digital Agenda provide guidance for further activities. The Strategy also states that German interests will be pursued the United Nations, the OSCE, the	P.11 P. 11

	Council of Europe, the OECD and NATO. The Strategy also expressed willingness to adopt any norms that NATO might come up with for CNI protection. As for other information sharing mechanisms, the Strategy states the following – -To improve the exchange of know how in this area we intend to set up joint institutions with industry with the participation of the competent law enforcement agencies, which will act in an advisory capacity. -Use the Budapest Convention and achieve harmonization of laws. A member of the Budapest Convention.	P. 10 P. 10
Relationship between the public and private sector	Protection to the private sector is provided by the government in the form of support to small and medium enterprises in the secure use of their IT systems. The Strategy also mentions improving economic capacities of core IT competencies.	P. 7 P. 11
Preventive measures for cyber crime	In relation to this, the Strategy specifies the following – - Strengthen capabilities of law enforcement; - Improve exchange of know how by setting up joint institutions with indus- try with the participation of the competent law enforcement agencies, which will act in an advisory capacity; - Projects to support partner countries with structural weaknesses will also serve the aim of combating cyber-crime. - Harmonization of criminal laws in acc with Budapest Conv. - Examine whether any additional convs are required at the UN level.	P. 10

Investigation of and punitive measures for cyber crime	Not specified.	
Status of Data Protection Laws	Not specified.	
Skilling and Capacity Building for Cybersecurity Personnel	The Strategy under “Personnel development in federal authorities” stresses the need for training in cybersecurity.	P. 12
Economic Growth of the ICT sector generally	Economic capacity of core IT competencies is a focus-issue.	P. 7
Approach to foreign investment	Not specified.	
Supply chain risk management	The Strategy acknowledges the importance of “reliable and trustworthy IT” and states that Germany will strengthen its “technological sovereignty and economic capacity” and that their aim is “to use components in critical security areas which are certified against an international recognized certification standard.”	P. 11-12
Government initiatives, campaigns and programmes for cyber space	None specified.	
Other relevant strategies or policy documents	The Strategy specifies that it adapts measures on the basis of the structures established by the CIP implementation strategy plan.	P. 6

ISRAEL

Country- Israel

Document Title- Israel National Cyber Security Strategy In Brief[7]

Date- 2017

Prepared By- Prime Minister's Office, State of Israel

PARAMETERS	CONTENTS / DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	Vision of Israel "to be a leading nation in harnessing cyberspace as an engine of economic growth, social welfare and national security."	P. 5
Basic Pillars	The Strategy identifies three operational layers / goals – -Aggregate robustness -Systemic Cyber Resilience -National Cyber Defence	P. 9
Identified Threats / Challenges	Not specified.	
Approach specified (if any)	Not specified.	
Definitions of Key Concepts	None	
Period of Validity	Not specified.	
Allocated Budgetary Resources (If any)	Not specified.	
First responders in Cyber Incident Management and Response	Not identified.	
Institutions (Civilian)	The Strategy mentions the establishment of the following pre-existing orgs –	
Institutions (Military)		

[7] Accessible at http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

<table>
<tr>
<td></td>
<td>2002- National Information Security Authority to instruct and protect vital computerized systems of selected public and private civil organizations.

2012- Israel National Cyber Bureau (INCB) reporting directly to the Prime Minister, tasked with- devising the State's national cyber policy and strategy, promoting national processes, developing national cyber capabilities and strengthening Israel's leadership in the field.

2015- National Cyber Security Authority (civilian) for working mainly with the private sector. Functions –

<table>
<tr><th>Aggregate Business</th><th>Systemic Resilience</th><th>National Defence</th></tr>
<tr><td>Critical Infrastructure Regulation</td><td>Nation-wide information sharing</td><td>Managing defensive campaigns within civilian sector</td></tr>
<tr><td>Security Guidance (mainly through sectoral regulators)</td><td>Assistance to organizations under attack</td><td>Coordination between agencies</td></tr>
<tr><td>National Knowledge Hub</td><td>Identification and investigation of attacks</td><td>National situation assessment</td></tr>
<tr><td>Cybersecurity market regulation</td><td>Support for sectoral SOCs</td><td></td></tr>
</table>

INCB and NCSA together constitute the INCD- Israel National Cyber Directorate.</td>
<td>P. 6

P. 6

P.15

P.6</td>
</tr>
<tr>
<td>Role of Intelligence Agencies</td>
<td>Not specified.</td>
<td></td>
</tr>
<tr>
<td>Offensive Cyber</td>
<td>Not specified.</td>
<td></td>
</tr>
</table>

Capabilities		
Declared stance on international norms for responsible State behaviour in cyberspace	Not specified. Nothing specified on public attribution as well.	
Declared stance on free and open nature of the internet	Not explicitly, but the Strategy states that “The State of Israel views international cooperation as a critical element in establishing cyberspace as a secure, free and global sphere of activity as well as a complementary component in its own national cyber security efforts.”	P. 18
International Cooperation and Information Sharing Mechanisms	No specific information sharing mechanism specified. Re International Cooperation, the Strategy states – “Cyberspace is a global sphere and cyber security is a global challenge. The State of Israel views international cooperation as a critical element in establishing cyberspace as a secure, free and global sphere of activity as well as a complementary component in its own national cyber security efforts. Israel is also engaged in efforts to assist partner nations in strengthening their national cyber security, while harnessing Israel's cyber capacities. Israel invites partners around the world to work together, to share knowledge, to develop new solutions on the global level and to fulfil our shared vision of a secure and prosperous cyberspace.” Not a member of the Budapest Convention.	P. 18
Relationship between the public and private sector	The Strategy broadly affirms protection to the private cyberspace sector and gives “CyberSpark” as an example – “*a concentrated and powerful cyber security ecosystem consisting of Israeli startups, global companies, academia and civilian and military cyber security centers – all within a walking distance of one another.*”	P. 17

Preventive measures for cyber crime	Not specified.	
Investigation of and punitive measures for cyber crime	Not specified.	
Status of Data Protection Laws	Not specified.	
Skilling and Capacity Building for Cybersecurity Personnel	The Strategy makes reference to a previous policy introduced in 2011 i.e “Advancing National Cyberspace Capabilities” to strengthen Israel's scientific and technological cyber capabilities and innovation processes. Its goals were – - Research, development, and implementation of national level security capabilities and technologies; - Strengthening the national science and technology (S&T) base in cyber: (a)promoting industrial innovation, (b)supporting academic research (including the establishment of six research centers in Israel’s leading universities), (c)enhancing the nation’s human capital in the cyber field and fostering an ecosystem for mutual enrichment. This includes the unique CyberSpark project – a concentrated and powerful cyber security ecosystem consisting of Israeli startups, global companies, academia and civilian and military cyber security centers – all within a walking distance of one another.	P. 17
Economic Growth of the ICT sector generally	Not specified.	
Approach to foreign investment	Not specified.	

Supply chain risk management	Not specified.	
Government initiatives, campaigns and programmes for cyber space	CyberSpark- a concentrated and powerful cyber security ecosystem consisting of Israeli start-ups, global companies, academia and civilian and military cyber security centers – all within a walking distance of one another.	P. 17
Other relevant strategies or policy documents	Governmental Resolution (August 2011) establishing the INCB; Governmental Resolution (Feb 2015) establishing the National Cyber Security Authority.	P. 6

JAMAICA

Country- Jamaica

Document Title- National Cyber Security Strategy[8]

Date- 2016

Prepared By- Government of Jamaica

PARAMETERS	CONTENTS/DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	The Strategy identifies the following objectives – 4 key areas to ensure a robust cyber security framework: (1)Technical Measures (2) Human Resource and Capacity Building (3) Legal and Regulatory (4) Public Education and Awareness	P. 20
Basic Pillars	There are 6 guiding principles- (i) Leadership (ii) Shared Responsibilities (iii) Protection of Fundamental Rights and Freedom (iv) Risk Management (v) Innovation and Business Development (vi) Sustainable Resources	P. 17
Identified Threats / Challenges	<u>Threats / Areas of Concern</u> (i) Financial Sector- Most targeted by cyber criminals, it includes phishing, identity theft, and creation of fake banking apps (ii)Critical Infrastructure <u>Adversaries / Actors-</u> (i) Organised International Groups	P. 10 P. 11 P. 11

[8] Accessible at https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf, last accessed on 5 January 2020.

Approach specified (if any)	The Strategy specifies a multistakeholder approach.	P. 17
Definitions of Key Concepts	The Strategy defines the following terms – Botnet; Critical Infrastructure; Cybercrime; Cyber Security; Cyber Incident Response Team; Denial of Service; Information Security; National Cyber Security Task Force; Phishing; Self-regulation; Stove-piped; Unauthorised Access; Unauthorised Modification.	P. 31
Period of Validity	Not specified.	
Allocated Budgetary Resources (If any)	Not specified.	
First responders in Cyber Incident Management and Response	A national CIRT, with a direct reporting line to the Ministry with portfolio responsibility for ICT, will be established.	P. 21
Institutions (Civilian)	Not specified.	
Institutions (Military)	Not specified.	
Role of Intelligence Agencies	Not specified.	
Offensive Cyber Capabilities	Not dealt with.	
Declared stance on international norms for responsible State behaviour in cyberspace	Not specified. Nothing specified on public attribition either.	
Declared stance on free and open nature of the internet	Not specified.	
International Cooperation and	1. Leveraging Regional and International Partnerships- “Cooperation with regional and	P. 22

Information Sharing Mechanisms	international partners for purposes of information sharing as well as incident response is … critical." 2. "Partner with local, regional and international bodies to promote and incentivise innovation and creativity in ICT and cyber security solutions." 3. "The legislative framework should support regional and international collaboration for example, investigations across borders and successful prosecution of trans-border crimes. Additionally, consideration will be given to being party to international conventions and mechanisms that support Jamaica's vision and is in line with the Constitution." 4. "Promote the exchange of information, intelligence and expertise with respect to cybercrimes and encourage cooperation with national, regional and international entities." 5. "Actively pursue bilateral and multilateral agreements to support law enforcement activities in cross border attacks against Jamaican citizens." 6. "Conduct a stakeholder mapping exercise and develop a strategic outreach programme for the engagement of regional and international partners." 7. "Utilize regional and international cooperation to improve the technical capacity of cyber security professionals within the government and private sector to enhance the capability to respond to cyber threats." 8. "Establish mechanisms for secure information sharing with regional and international stakeholders." 9. "Pursue areas of collaboration with other CIRTs (regionally and internationally)." Not a member of the Budapest Convention.	P. 22 P. 23 P. 38 P. 36 P. 36 P. 36 P. 36
Relationship between the public and private sector	Not exactly but specific focus has been given to certain groups as follows: "It is the Government's responsibility to establish measures which protect the vulnerable in our society, such as, the elderly, youth and persons with disabilities, as they often lack the wherewithal to do	P. 24

	so themselves. As the guardian of their interests it is the Government's responsibility to ensure that they are not overlooked but are informed and aware of the risks."	
Preventive measures for cyber crime	1. Ensuring that Critical Infrastructure Systems are Resilient in the face of Current and Future Cyber Threats 2. National Capability for Ensuring Timely and Effective Response to Cyber Incidents is Established and Maintained	P. 20 P. 21
Investigation of and punitive measures for cyber crime	No specific investigatory measures specified other than the following: (i) "There is need for greater sensitization of and/or training for other arms such as the Jamaica Defence Force, prosecutors in the Resident Magistrate Courts, as well as, the judiciary. Therefore, there will be targeted sensitization and training in cyber security and cybercrimes for these stakeholders." (ii) "The legislative framework should support regional and international collaboration for example, investigations across borders and successful prosecution of trans-border crimes. Additionally, consideration will be given to being party to international conventions and mechanisms that support Jamaica's vision and is in line with the Constitution." (iii) "Broaden and improve the capabilities of the bodies responsible for investigating and prosecuting cybercrimes (including judiciary, law enforcement and prosecutors)." (iv) "Establish a line of communication between the CIRT and law enforcement when cyber incidents are detected for their investigation and conversely to the CIRT whenever a threat is detected by law enforcement." (	P. 38 P. 23 P. 35
Status of Data Protection Laws	They find a mention as follows: 1. "Recognizing that all businesses are affected by	

	cyber related issues; it is the aim of this Strategy to ensure both online and offline transactions are taken into account. The legislative landscape will be periodically reviewed to ensure it is adept to treat with subject areas, such as data protection and electronic transaction and authentication and therefore support a robust business environment, while remaining compatible with international best practices." 2. "Establish a continuous review process to ensure that there is an updated and robust legislative framework that is appropriately aligned with international best practice and creates a safe environment for all activities within the cyber domain including: data protection" The Strategy also mentions the following - "There will be dedicated efforts to ensure that the legislative framework for cybercrime adequately addresses emerging threats and trends while preserving the right to privacy and other fundamental rights and freedoms. There will be no discrimination in the application of the law; as once a person falls victim to a cybercrime within the jurisdiction there will be legal recourse."	P. 24 P. 37 P. 24
Skilling and Capacity Building for Cybersecurity Personnel	Stated Goal:- This Strategy will seek to ensure that there exists an available cadre of knowledgeable and highly skilled professionals in the area of Information Security. Actions:- 1. An available pool of skilled and knowledgeable professionals in the field of information security is maintained:- a. More universities to provide Information Security and Network Security Programmes b. Ensure that academia supports growth and development of this field	P. 22 P. 22

	c. Constant training and education required 2. Jamaica has an Active and Dynamic culture of Research and Development a. R & D will be encouraged b. “Partner with local, regional and international bodies to promote and incentivize innovation and creativity in ICT and cyber security solutions.” c. Explore possibility of establishment of a fund for cyber security R & D projects. d. Exchange of Information on experiences and evolving trends The other relevant points in the policy are as follows: 1. “Develop joint research and development projects between public and private sectors and academia (nationally, regionally and internationally) to build innovative cyber security solutions.” 2. “Explore the opportunities for the establishment of a fund dedicated to capacity building in cyber security through public private partnership.” 3. “Promote scholarship programmes or funding for the development of cyber security innovations.” 4. “Actively engage in talent recruitment initiatives in the cyber security field.” 5. Promoting careers in Information Security.	P. 38 P. 38 P.38 P. 36 P. 36
Economic Growth of the ICT sector generally	Not specified explicitly but it does mention: “Create an environment that supports the exchange of information in the area of cyber security both nationally and internationally.”	P. 37
Approach to foreign investment	Not specified.	
Supply chain risk management	Not specified	
Government	Not specified.	

initiatives, campaigns and programmes for cyber space		
Other relevant strategies or policy documents	• The National Information and Communications Technology Strategy 2007-2012 • The National Development Plan 2030 (Vision 2030 Jamaica) • The Information and Communications Technology Policy, 2011 • The National Security Policy 2014	P. 14

JAPAN

Country- Japan

Document Title- Cybersecurity Strategy[9]

Date- July 27, 2018

Prepared By-

PARAMETERS	CONTENTS/DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	The Strategy identifies the following objectives- 1. Improve socio-economic vitality and sustainable development. 2. Building a safe and secure society for the people. 3. Contributing to peace and stability of the international community and national security. 4. "Japan aims to realize a society in which cyberspace develop sustainably as "frontier generating infinite values," where new values and services are generated continuously, bringing abundance to the people."	P. 9 P. 11
Basic Pillars	The Strategy identifies the basic pillars as follows – (i) Assurance of the free flow of information (ii) Rule of Law (iii) Openness (iv) Autonomy (v) Collaboration among multi-stakeholders	P. 9
Identified Threats / Challenges	<u>Threats / Areas of Concern</u> (i) "The risk of economic and social loss or damage in real space is expected to expand and accelerate exponentially." (ii) Latent risk that the providers of these technologies and services will lose the ability to	P. 2 P. 6

[9] Accessible at https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf, last accessed on 5 January 2020 (Provisional Translation)

	control them." (iii) Malicious actors can utilise new technologies such as AI and Blockchain to carry out their activities. (iv) Increased concerns over potential attempts to target weaknesses in IoT, supply chains, and open innovation, and for unintended behavior to occur in these systems." (v) Major effects on society due to Interruptions in Business, Functions, and Services. (vi) Financial Theft and Fraud. (vii) Reduced Competitiveness Due to the Loss or Breach of Information. (viii) Small and medium-sized enterprises will suffer greater damage in case of an attack. (ix) Massive cyberattacks can be expected to cause simultaneous damages to services that are normally relatively unrelated, and the country must work as one to address risk management for threats in cyberspace to protect society and the people from those threats." <u>Adversaries / Actors</u>- (i) "There have also been massive incidents suspected to have been state-sponsored." (ii) Terrorist Organisations	P. 7 P. 7 P. 8 P. 8 P. 19 P. 34 Page 7; 37 P. 38
Approach specified (if any)	Multi-stakeholder approach	P. 3, 10 and 11
Definitions of Key Concepts	None	
Period of Validity	Three years. However, "The "Cybersecurity Policy" is scheduled for review following the Tokyo 2020 Games.	P. 3 and P. 25
Allocated Budgetary Resources (If any)	Not specified	

First responders in Cyber Incident Management and Response	Not specified	
Institutions (Civilian)	All relevant public and private stakeholders led by the National centre of Incident readiness and Strategy for Cybersecurity with regard to defense, the ministries and agencies responsible for response measures with regard to deterrence, and information gathering and investigative organizations with regard to situational awareness will closely cooperate on a daily basis and proceed with the initiatives related to national security, under the overall coordination by the National Security Secretariat. When necessary, deliberation and decision will be made at the National Security Council.	P. 37
Institutions (Military)	Ministry of Defense, Self-Defense forces – Role will be to continue to strengthen the defense of the networks and infrastructure on which their operations depend, while further enhancing the capabilities of cyber defense units against cyberattacks, and deepen collaboration with stakeholders involved in the mission assurance of the Self-Defense Forces.	P. 38
Role of Intelligence Agencies	Not specified / dealt with	
Offensive Cyber Capabilities	In the context of “measures for effective deterrence”, the Strategy states that the Cabinet Secretariat as its core in order to make timely and appropriate responses, promote as a whole inter-agency and cross-sectoral efforts in a comprehensive manner, and the government will also strengthen capacity at the relevant authorities including law enforcement authorities and the Self-Defense Forces. The Strategy states in this regard, the acquisition of capabilities to prevent malicious cyber actors from using cyberspace may be considered.	P. 39

Declared stance on international norms for responsible State behaviour in cyberspace	The Strategy acknowledges the application of existing international law to cyberspace. Not specified stance on public attribution.	P. 36
Declared stance on free and open nature of the internet	Stated Goal: Commitment to a Free, Fair, and Secure Cyberspace Actions: 1. Communicating the Ideas of a Free, Fair, and Secure Cyberspace: “Japan will aim to ensure the safety in cyberspace through the coordination and collaboration among multi-stakeholders on efforts to ensure cybersecurity, rather than through control and regulation such as controlling the flow of information by states.” 2. Protecting the Rule of Law in Cyberspace.	 P. 36 P. 36
International Cooperation and Information Sharing Mechanisms	1. The government will “work on the development of a business environment that facilitates international adoption by taking strict action through international cooperation against measures inhibiting free trade in the name of cybersecurity”. 2. Sharing Expertise and Coordination Policy 3. International Collaboration for Incident Response 4. Cooperating for Capacity Building 5. Collaboration between National Police Agency and other relevant ministries, as well as agencies in foreign countries by leveraging frameworks such as the Convention on Cybercrime, mutual legal assistance treaties, and the ICPO.” 6. Confidence building measures among states 7. International collaborations for tapping into human resource development overseas and contributing to overseas as well using Japan’s own knowledge in this regards. 8. Virtuous circle of information sharing between R & D and security operations companies. 9. Strengthen R&D related international	P. 18 P. 41 P. 41 P. 41 P. 36-37 P. 39 P. 45 P. 46 P. 46

	partnerships in the public and private sectors with like-minded countries Stated Goal: Building an Information Sharing/ Collaboration Framework that Extends beyond Traditional Frameworks Actions: 1. Promoting Information Sharing and Collaboration between Multi-Stakeholder 2. Towards a New Stage in Information Sharing and Collaboration: Attach benefits to active cooperation and collaboration; government to take a lead in sharing information in its possession A member of the Budapest Convention.	P. 33 P. 33-34
Relationship between the public and private sector	The Strategy states the following: 1. “Regarding measures aimed at enterprises to promote cybersecurity, the government will follow up on the use of incentives for investment in cybersecurity so that they function effectively, and consider required measures as necessary.” 2. “The government will support the challenges towards new value creation using such advanced technologies not only by major enterprises but also venture enterprises. Specifically, the government will work in cooperation with private sectors to analyze and clarify cybersecurity risks associated with the use of advanced technologies and to prepare and disseminate guidelines based on such analysis and clarification.” 3. “It is also necessary for the government to work with the private sector to build a system to create and manage a list of devices and services for which trustworthiness has been proven so that suppliers in the supply chain can verify that trustworthiness when using devices or equipment.” 4. “[T]he government will prepare easy-to-understand case studies of cybersecurity measures for small and medium-sized enterprises	P. 17 P. 17 P. 19 P. 19

	that include models for the safe use of information systems, and will promote the use of insurance in cybersecurity. The government will also strengthen the consultation system for small and medium-sized enterprises on cybersecurity incidents." 5. "Japan will promote the establishment of cybersecurity for governmental bodies and critical infrastructure operators in order to assure the execution of the missions of those governmental bodies related to national security and to provide services essential for the people and the society." 6. "Local governments nationwide have been undertaking the fundamental reinforcement of measures, and the national government will update its guideline on security policy as necessary in light of the necessity to achieve a high level of security. The government will also work to achieve the necessary security levels for operational networks and promote initiatives to secure and develop cybersecurity human resource, enhance systems as well as securing the necessary budget while being mindful of the need for smooth operations by local governments."	P. 38 P. 27
Preventive measures for cyber crime	The Strategy fleshes out the following detailed measures - 1. The government will carry out response training and exercises across both cyberspace and real space while strengthening the preparations to respond to cyberattacks through training and exercises in order to work on risk management for both cyberspace and real space. The government will also promote training of personnel capable of analyzing cyberattacks, the sharing of information through a framework for public and private sector coordination, and the advancement of Internet monitoring in an effort to improve data collection and analysis capabilities and emergency response capabilities in cyberspace. 2. Promoting R&D for detecting threats, increased situational awareness capabilities, fundamentally important technologies for national security, etc. 3.Building Secure IoT Systems	P. 34- 35 P. 46-47 P. 20-21

	a. Improving Structural Framework for IoT Systems and International Standard b. Preparing a Formation for Vulnerability Countermeasures 4. Building a Safe and Secure Cyber Environment for Users a.Proactive Cyber Defense b. Development of dependable information infrastructure c. The government will work with providers of cryptocurrency services to promote measures so that the people may safely engage in the trading of cryptocurrencies. Also, with regard to self-driving vehicles and drones, the government will promote measures to avoid the occurrence of unauthorized operations due to cyberattacks as they may cause risks to human life. Stated Goal: Ensuring National Resilience Actions: 1. Mission Assurance: "The execution of the missions of these governmental bodies relies on the services provided by critical infrastructure operators and other business operators which maintain social system." Thus, promotion of cybersecurity for the same. 2. Protection of Japan's Advanced Technologies and Defense Related Technologies: "Japan will work to adopt a system to ensure the safe sharing of information, establish new information security standards for contractors, and revise contractual provisions. 3. [G]overnment will strengthen the collection and analysis of information on the activities of terrorist organizations in cyberspace and take any other necessary measures in collaboration with the international community, while also guaranteeing the basic human rights including the freedom of expression. Stated Goal: Protection of Critical Infrastructure through Public and Private Sector Cooperation Actions: 1. Primary Initiatives Based on the "Cybersecurity Policy" a. Promotion of Risk Management b. Improvement and Promotion of Safety Principles c. NISC Cyber Incident Severity Scale for CIS Outages	P. 22-23 P. 37-39

	d. Joint Training and Exercises between Public and Private Sectors e. Security Measures for Industrial Control Systems (ICS) 2. Strengthening and Enhancing Security in Local Governments Stated Goal: Strengthening and Improving Security in Governmental Bodies and Government-Related Entities Actions: 1. Advancing and Visualizing Security Measures for Information Systems a. Increasing Defensive Capabilities and Conditional Awareness for Information Systems b. Preventing Damages and the Spread Thereof through the Advanced Cross-Organizational Collaboration among the Agencies 2. Promoting Use of the Cloud for Effective Security Measures 3. Preemptive Efforts Utilizing Advanced Technology 4. Raising the Cybersecurity Level through Auditing 5. Improving Organizational Response Capability	
Investigation of and punitive measures for cyber crime	The Strategy fleshes out the following detailed measures. – 1. Enhancing Measures against Cybercrimes a. Continue to work to grasp the actual state of cybercrime and promote a crackdown on such crime. b. Improvement of investigative and technological capabilities. Stated Goal: Enhancing Deterrence Capabilities Actions: 1. Measures for Effective Deterrence: IL applies to cyberspace, cyber operations may amount to force in some cases, may resort to proportionate countermeasures. “Japan will utilize political, economic, technological, legal, diplomatic, and all other viable and effective means and capabilities, depending on the threat, and take resolute responses against cyber threats that undermine	P. 23-24 P. 39

	our national security, including those possibly state-sponsored." The government will strengthen the coordination system among relevant governmental bodies with the Cabinet Secretariat as its core in order to make timely and appropriate responses, promote as a whole inter-agency and cross-sectoral efforts in a comprehensive manner, and the government will also strengthen capacity at the relevant authorities including law enforcement authorities and the Self-Defense Forces. In this regard, the acquisition of capabilities to prevent malicious cyber actors from using cyberspace may be considered. No specific investigatory measures specified other than the following: (i) "In order to deter increasingly serious cyberattack, in addition to enhancing response capabilities, adequate capabilities to detect, investigate, and analyze cyberattacks are necessary to make the attackers accountable. To this end, the government will quantitatively and qualitatively improve the information collection and analysis capabilities of the relevant governmental bodies." (ii) The government will also carry out initiatives related to counter-cyber intelligence.	P. 40
Status of Data Protection Laws	The Strategy acknowledges the importance of data protection in the following manner - 1. Data protection initiatives will also be carried out for all Agencies to prevent information leakage when incidents occur. 2. Privacy to be maintained - Free flow of information in cyber space, morality and common sense. They are also found in a way as follows: 1. "These initiatives will include not only sector-	P. 28 P. 10

	specific issues weighing on the actors in the public and private sectors but also common issues such as their scope, definitions, physical safety measures, demarcation points of responsibility (including the legal responsibilities of each actor including product liability of the manufacturers and the safety management obligations of the operator, etc. for incidents concerning the response to known vulnerabilities), and privacy issues." (In the context of IoT, Page 20).	
Skilling and Capacity Building for Cybersecurity Personnel	1.Ensuring a safe and secure Educational and Research Environment at Universities, etc. 2. Development and Assurance of Cybersecurity Human Resource 3. Joint Training and Exercises between Public and Private Sectors 4. "... [T]he government will work in cooperation with private sectors to discover and train personnel who are capable of explaining and discussing cybersecurity measures with senior executives while hosting seminars for senior executives to promote a change in thinking."	P. 30 P. 42- 45 P. 26 P. 16
Economic Growth of the ICT sector generally.	1. Enabling Socio-Economic Vitality and Sustainability Development: "Cybersecurity measures should be regarded as "investments" as the basis to drive those trends, rather than unwanted "costs." 2. Advancement of Research and Development	P. 15- 18 P. 46
Approach to foreign investment	Not specified.	
Supply chain risk management	1. "[T[here are expectations for realizing high quality products or services related to cybersecurity by estimating the risks beforehand and including cybersecurity measures in the processes of creating those products or services (security by design). 2. Important to place the concept of security by design at the foundation of new initiatives.	P. 17 P. 17 P. 38

	3. “Deliberations will be carried out with the assumption that these measures [higher cyber security standards discussed in this section] will be applied to the entire supply chain for the defense industry, including subcontractors, through the collaboration between the public and private sectors.” 4. Promoting R & D for ensuring built in security. “In particular, the government will promote R&D on certification and generating trust, and ensuring traceability in the value creation processes of supply chains, and on detection of and defense against attacks in these areas”. Stated Goal: Achieving a Supply Chain that Creates Values through Diverse Connections Actions: 1. Formulating Cybersecurity Framework for supply chain risk 2. Building a System to Confirm Cybersecurity in the Supply Chain 3. Promoting Initiatives by Small and Medium-sized Enterprises	P. 46 P. 18 P. 19
Government initiatives, campaigns and programmes for cyber space	Cooperation by Everyone who is the Main Player in Cybersecurity: The government “will develop a comprehensive strategy and specific action plan for public awareness on cybersecurity and disseminate necessary information and handle inquiries by the people. The government will also promote practical action by the stakeholders by utilizing committees in which representatives of various communities in industry, academia, and the public and private sectors participate.”	P. 48
Other relevant strategies or policy documents	Basic Act on Cybersecurity 2014 General Framework for Secure IoT Systems (October 2016, Cybersecurity Strategic	P. 2 P. 20

	Headquarters)	

NEW ZEALAND

Country- New Zealand

Document Title- New Zealand Cyber Security Strategy 2019[10]

Date- 2019

Prepared By- Department of Prime Minister and Cabinet

PARAMETERS	CONTENTS / DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	The discernible objective of the strategy appears to be to the following – "New Zealand is confident and secure in the digital world- it is about enabling New Zealand to thrive online"	P. 8
Basic Pillars	The Strategy identifies 5 priority areas – 1. Cyber Security aware and active citizens 2. Resilient and Responsive New Zealand 3. Strong and capable cyber security workforce and ecosystem 4. Proactively tackle cybercrime 5. Internationally active	P. 10
Identified Threats / Challenges	The Strategy identifies "cybercriminals" and "threat actors". The Strategy specifically mentions the NotPetya and WannaCry ransomware attacks as having been "publicly attributed" to North Korea.	P. 4 P. 4
Approach specified (if any)	The Strategy explicitly adopts the multistakeholder approach.	P. 13

[10] Accessible at https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf.

Definitions of Key Concepts	The Strategy's glossary defines – 5G Technology, AI, Credential harvesting, Critical infrastructure, Cyber-attack, Cyber incident, Cyber security, Cyber terrorism, Cyber-crime, Cyber-enabled crime, Cyberspace, DDOS, Encryption, Information system / computer system, Internet of Things, Malicious software/malware, Phishing, Quantum Computing, Ransomware, Software.	P. 16
Period of Validity	2019-2023	
Allocated Budgetary Resources (If any)	Not specified	
First responders in Cyber Incident Management and Response	Not specified	
Institutions (Civilian)	Not specified	
Institutions (Military)	Not specified	
Role of Intelligence Agencies	Not specified	
Offensive Cyber Capabilities	Not specified	
Declared stance on international norms for responsible State behaviour in cyberspace	The Strategy acknowledges that international law is applicable to cyberspace. Also, while the Strategy does not specify New Zealand's own policy towards attribution, it does mention examples of public attribution of other states- including North Korea and Russia.	P. 13
Declared stance on free and open nature of the internet	The Strategy explicitly aspires for a free and open internet.	P. 13
International	The Strategy specifies certain measures to	P. 15

Cooperation and Information Sharing Mechanisms	proactively tackle cybercrime– "Work continues on implementing the 2015 National Plan to Address Cybercrime, including consideration of accession to the Council of Europe Convention on Cybercrime (the Budapest Convention). We will also continue to work with others on issues related to encryption: ensuring that law enforcement can access the information it needs while balancing the rights of New Zealanders to protect their privacy and security. Any action to address online harms, such as the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online, will be consistent with New Zealand's wider cyber policy positions, including the importance of maintaining a free, open and secure internet and the application of international human rights law online." Not a member of the Budapest Convention.	
Relationship between the public and private sector	The Strategy, while not fleshing out any specific measures to protect the private sector, acknowledges the benefits of cooperation with the private sector as per the following – (i) Partnerships are crucial – The government has a leadership role to play in cyber security – but not on its own. Close partnerships are required with the private sector, non-government organisations and the international community. Businesses drive the New Zealand economy and depend on the internet and networked technologies. They must protect the information that is critical to their commercial success. The private sector and technical community have considerable cyber security expertise, and we need to work with international partners in order to combat trans-national threats. (P. 9) (ii) Economic Growth is enhanced –	P. 9 (P. 9)

	Strong cyber security practices result in businesses remaining productive, profitable and transparent to customers and shareholders. New Zealand will be recognised as a desirable place to do business, store data, and invest. Information and communication technologies and enhanced connectivity will continue to boost economic growth, and minimise costs of cyber insecurity. New Zealand and New Zealand businesses can benefit from the growth of the digital economy and new technologies can help drive innovation.	
Preventive measures for cyber crime	The Strategy lists out measures to achieve a "Resilient and responsive New Zealand" – ● vigorously protecting New Zealand's most important information infrastructures ● supporting businesses, NGOs, community organisations, and individuals to be protected and resilient to major cyber incidents ● using cyber tools and partnerships to further New Zealand's interests, including national security and law enforcement activities ● supporting critical national infrastructure organisations and ensuring those organisations take responsibility for the security of their systems ● improving the information security capabilities and resilience of the public sector.	P. 15
Investigation of and punitive measures for cyber crime	None specified.	
Status of Data Protection Laws	Not specified.	
Skilling and Capacity Building for Cybersecurity Personnel	To develop a "Strong and Capable Cyber Security Workforce and Ecosystem" – ● incentivising and increasing the supply of skilled cyber security workers ● supporting the expansion of roles and	P. 12

	opportunities for cyber security workers • incentivising the growth of the cyber security industry in New Zealand • supporting industry and professional organisations to promote responsible management of cyber security across their organisations and workplaces • encouraging the development of a world-class cyber security academic research community • supporting high-quality cyber security research and encouraging links between academia and industry.	
Economic Growth of the ICT sector generally	Not specified.	
Approach to foreign investment	Not specified	
Supply chain risk management	Not dealt with.	
Government initiatives, campaigns and programmes for cyber space	Not specified.	
Other relevant strategies or policy documents	2011 and 2015 Cyber Security Strategies mentioned.	

RUSSIA

Country- Russia

Document Title- Information Security Doctrine of the Russian Federation[11] (hereinafter 'the Doctrine') (unofficial translation)

Date- 5 December 2016

Prepared By- Moscow Kremlin/ Approved by Decree of the President of the Russian Federation

PARAMETERS	CONTENTS/DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	Ensuring the national security of the Russian Federation in the information sphere. Outlines strategic goals and direction for information security in 5 core areas (1) military and armed forces (2) state and public security including critical information infrastructure (3) economic sphere and (4) science, technology and education (5) strategic stability and equitable strategic partnerships.	Para 1 Strategic goals outlined in detail at paras 20 to 29.
Basic Pillars	None specified.	
Identified Threats / Challenges	A 'threat to the information security of the Russian Federation'/ 'information threat' is defined as a set of actions and factors, endangering national interests in [the] information sphere. Key information threats Include: (1) Expanding scope of IT and its role in economic development and improving public institutions, without linkages with information security (2) Foreign countries' building of IT capabilities with impacts on information infrastructure for military purposes and intensifying technical intelligence operations against Russian institutions and industry. (3) Scaling up of use by states of information-psychological operations aimed at	Para 2(b) Para 10 Para 11 Para 12

[11] Accessible at https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

	destabilization of political and social situations, undermining sovereignty and territorial integrity, generating bias against Russian media and journalists and erosion of traditional Russian spiritual and moral values. (4) Terrorist and extremist organizations whipping up interethnic and social tensions, spreading hatred, enmity and propaganda, and damaging critical information infrastructure. (5) Scale of cybercrime, increasing sophistication not restricted to the financial sector, but also impacts privacy, personal and family secrets, personal data processing. (6) **Information security in the field of defense**: Increased application by states and other organizations of IT to undermining sovereignty, socio-political stability and territorial integrity of Russia and its allies. (7) Increasing complexity, scale and coordination of computer attacks on critical information infrastructure objects . (8) **Information Security in Science, Technology and Education**: insufficient effective research in innovation, implementation issues, low staffing and low awareness of information security issues. Desire of individual states to use technological superiority for domination of the information space. Lack of international Law governing interstate relations in the information space and mechanisms for their application to IT makes the achievement of strategic stability and equitable strategic partnerships difficult.	Para 13 Para 14 Para 15 Para 16 Para 17 Para 18
Approach specified (if any)	Although the Strategy does not explicitly use the terms, it appears multi-sectoral and multi-stakeholder with a view to building 'strategic stability' and 'equitable strategic partnerships'.	
Definitions of Key Concepts	a) 'information sphere' b) 'national interests in the information sphere' c) 'a threat to the information security of the Russian Federation'/ 'information threat' d) 'information security' e) 'ensuring information security' f) 'information security forces' g) 'means of ensuring information security'	Para 2, (a) to (h)

	h) 'information security system' i) 'information infrastructure of the Russian Federation'	
Period of Validity	Not specified.	
Allocated Budgetary Resources (If any)	Not specified.	
First responders in Cyber Incident Management and Response	Not specified.	
Institutions (Civilian) Institutions (Military)	Combination of legislative, [executive], law enforcement, and judicial control and other state bodies in cooperation with local government bodies, organizations and citizens. An 'information security system' is under construction based on delimitation of powers of legislative, executive and judicial bodies, local government and other bodies of state power; its constitution is to be determined by the President of the Russian Federation. Participants in the information security system also include - owners of critical information objects infrastructures and organizations operating such facilities, - mass media and mass communication organizations - monetary, foreign exchange, banking and other areas of financial market operators, telecom operators, - information system operators, - organizations involved in the creation and operation information systems and communication networks for the development, production and operation of information security facilities the provision of information security services, - organizations engaged in educational activities in this areas, public associations, other organizations and citizens, who participate in solving problems of and providing	Para 30 Para 31, 32 Para 33

	information in accordance with Russian legislation.	
Role of Intelligence Agencies	Not specified, could be read into the term 'other forms of activities of state bodies' mentioned at para 30.	Para 30
Offensive Cyber Capabilities	Not specified.	
Declared stance on international norms for responsible State behaviour in cyberspace	Asserts that activities of state bodies to ensure information security should be based on compliance with generally recognized principles and norms of international law, international treaties of the Russian Federation, as well as the legislation of the Russian Federation. In defining its national interests in the information sphere, the Doctrine advocates the promotion of the formation of a system of 'international information security aimed at countering threats to the use of information technology in order to violate strategic stability, to strengthen equitable strategic partnerships in the field of information security, as well as to protect the sovereignty of the Russian Federation in information space'.	Para 34(e) Para 8(e)
Declared stance on free and open nature of the internet	No. Makes a reference to the development of a 'national management system for the Russian segment of the internet'. Indeed, insofar as cross-border circulation of information is used to achieve geopolitical, contradictory international law of military-political as well as terrorist, extremist, criminal and other illegal purposes to the detriment of international security and strategic stability, the Doctrine treats it as an information security threat.	Para 29(e) Para 10
International Cooperation and Information Sharing Mechanisms	The Doctrine directs the promotion of positions of the Russian Federation providing for [equal] security and mutually beneficial cooperation of all stakeholders in the information field within the framework of the activities of international organizations. Observer status to the Budapest Convention.	Para 29(d)

Relationship between the public and private sector	Not specified, but recognizes certain stakeholders as 'participants' in information security'.	Para 33
Preventive measures for cyber crime	The Doctrine notes the increasing scale and sophistication of computer crimes, earlier restricted to the financial sector now also extends to violation of citizens' constitutional rights and freedoms, relating to privacy, personal and family secrets, with personal data processing using information technology. The Doctrine recognizes, in the field of state and public security, the need to increase the effectiveness of prevention of crimes committed using information technology, and counteraction to such offenses.	Para 14 Para 23(f)
Investigation of and punitive measures for cyber crime	The Doctrine recognizes, in the field of state and public security, the need to increase the effectiveness of prevention of crimes committed using information technology, and counteraction to such offenses.	Para 23(f)
Status of Data Protection Laws	Not specified.	
Skilling and Capacity Building for Cybersecurity Personnel	Tasks state bodies in the framework of development and improvement of the information support system security to 'improve the forms and methods of interaction of forces information security in order to increase their preparedness for countering information threats, including through regular training (exercises)'.	Para 36(b)
Economic Growth of the ICT sector generally	The Doctrine recognizes the effective application of information technology as a factor in accelerating economic development, and that it gives rise to new information threats. The Doctrine also recognizes that the state of information security in the economic area is	Para 7, 10 Para 17

	characterised by underdevelopment of competitive information technologies and heir use for the production of goods and services. Consequently, there is a high level of dependence of domestic industry on foreign information technology regarding electronic component base, software, computing and communications, which makes the socio-economic development of the Russian Federation [dependent] on the geopolitical interests of foreign countries.	
Approach to foreign investment	Not specified	
Supply chain risk management	The elimination of dependence of domestic industry on foreign information technologies and means of information security support though the creation, development and wide introduction of domestic developments, as well as production and provision of services based on them is included as one of the main directions of providing information security in the economic sphere. This is complementary to increasing the competitiveness of Russian companies operating in the IT and electronics industry.	Para 25(b) Para 25(c) and (d)
Government initiatives, campaigns and programmes for cyber space	Not specified. However, the internet sovereignty law is relevant to the operationalization of this Doctrine. Federal Law dated 01.05.2019 No. 90-ФЗ "On Amendments to the Federal Law" On Communications "and the Federal Law" On Information, Information Technologies and the Protection of Information was signed by President Putin on 1 May 2019 and entered into force on 1 November 2019.	
Other relevant strategies or policy documents	(1) National Security Strategy Doctrine approved by Decree Of the President of the Russian Federation dated December 31, 2015 No. 683 (2) Annual report of the Secretary of the Security Council of the Russian Federation on the state of national security (to include results of	Para 5 Para 38

	monitoring the implementation of the Information Security Doctrine) (3) Other sectoral documents of strategic planning	Para 37

SINGAPORE

Country- Singapore

Document Title- Singapore's Cybersecurity Strategy[12]

Date- 2016

Prepared By- Cyber Security Agency of Singapore (Established under the PMO and managed by the Ministry of Communications and Information)

PARAMETERS	CONTENTS/DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	Objectives identified in the Strategy correspond to the pillars (see subsequent sections)	
Basic Pillars	The Strategy identifies the following pillars- (i) Building a Resilient Infrastructure (ii) Creating a safe cyberspace (iii) Developing a Vibrant Cybersecurity Ecosystem (iv) Strengthening International Partnerships	P. 4-5
Identified Threats / Challenges	**<u>Threats / Areas of Concern</u>** (i) Systems that run utility plants, transportation networks, hospitals and other essential services (ii) The advent of IoT worsening the threat (iii) Utilities, Services, and Transport highlighted to be the most important CIIs (iv) "Resilience in essential services is especially applicable to CIIs." (v) "Government systems are among the prime targets for cyber-attackers."	 P. 6 P. 6 P. 10-11 P. 17 P. 20

[12] Accessible at https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy, last accessed on 5 January 2020.

	<u>Adversaries / Actors-</u> Not explicitly highlighted	
Approach specified (if any)	Appears to be a multi-stakeholder approach: "It aims to catalyse participation by all stakeholders - government agencies, the cyber industry, professionals and students, academia and researchers, and providers of essential services."	P. 6
Definitions of Key Concepts	Not specified.	
Period of Validity	Not specified.	
Allocated Budgetary Resources (If any)	8 per cent of ICT expenditure on cybersecurity.	P. 20
First responders in Cyber Incident Management and Response	Three tiered response plan – Tier 1 for cyber campaigns that threaten national security, Tier 2 for cyber-attacks on a sector, and Tier 3 for cyber-attacks on a specific operator. National Cyber Incident Response Teams are part of Tier 1 and Tier 2 plans.	P. 16 P. 17
Institutions (Civilian)	The national response to a cyber-attack will be led by an inter-agency Cybersecurity Crisis Management Group, or CMG (Cyber). It is led by the Permanent Secretary of the Ministry of Communications & Information, supported by CSA, and comprises senior policy decisionmakers from government agencies overseeing the different critical sectors. CMG (Cyber) serves dual functions: (a) it is responsible for the development of cybersecurity policies and standards, and oversees the implementation of cybersecurity protection measures in the critical sectors; and (b) in a cyber crisis, it mobilises the necessary resources and directs the operational responses to provide a coordinated response to the threat.	P. 16

Institutions (Military)	Not specified.	
Role of Intelligence Agencies	Not specified.	
Offensive Cyber Capabilities	Not specified.	
Declared stance on international norms for responsible State behaviour in cyberspace	Not specified. Facilitate exchange on cyber norms and legislation: "Consensus and agreement among nations are key to ensuring the success of cybersecurity cooperation. Singapore aims to be an active participant in this area and will facilitate global and regional dialogues on cyber norms building and codes of conduct, cyber policy and legislation, cyber deterrence and cybercrime cooperation." Nothing specific on public attribution either.	P. 47
Declared stance on free and open nature of the internet	1. Singapore to push for a cleaner internet, ISPs having an essential role in achieving this.	P. 31
International Cooperation and Information Sharing Mechanisms	1. Forge international (such as INTERPOL) and ASEAN cooperation to counter cyber threats and cyber-crime for cyber incident reporting and response. 2. Champion international and ASEAN cyber capacity building initiatives. 3. Facilitate exchange on cyber norms and legislation. 4. Bringing global experts and thought leaders together 5. Building capacities and capabilities through collaboration at the regional and global levels. Not a member of the Budapest Convention.	P. 43, 29
Relationship between the public and private sector	Not exactly but the following is provided: 1. The new Cybersecurity Act will "[f]acilitate the sharing of cybersecurity information with and by CSA. Recognising that cybersecurity breaches will happen despite our best efforts, the Act will	P. 19

	empower CSA and sector regulators to work closely with affected parties to expeditiously resolve cybersecurity incidents and recover from disruptions." 2. "Businesses may find it challenging to keep pace with new cyber threats. SingCERT, which was set up in 1997 to facilitate the detection, resolution and prevention of cybersecurity related incidents, will deepen its threat discovery and analysis capabilities to deal with the evolving local cyber threat environment. SingCERT will expand its capacity to facilitate the sharing of cybersecurity"	P. 33
Preventive measures for cyber crime	1. "Implement across all critical sectors, a CII Protection Programme with robust and systematic cyber risk management processes. A key part of the CII Protection Programme is to grow a culture of cyber risk awareness across all levels of a CII organisation." 2. "Pre-empt cyber vulnerabilities by going upstream and promoting Security-by-Design practices." 3. "The Government will further enhance the capability of the NCIRTs to deal with more complex and challenging attack scenarios. It will also build up more NCIRTs by upgrading certain sectoral CIRTs and also consider raising additional NCIRTs from industry and academia. This will increase the national capacity to deal with large scale cyber-attacks." 4. "Conduct regular multi-sector cybersecurity exercises with more complex scenarios and involving more and more sectors." 5. "Strengthen the Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP) of essential services, especially against a cyber-attack." 6. Introduce a new Cybersecurity Act that will "equip CSA with the necessary powers to effectively address increasingly sophisticated threats to national cybersecurity". 7. Securing Government Networks: a. Reducing Attack Surface b. Enhancing Situational Awareness through Technology c. Preparing for Cyber breaches by sharpening skills of incident responders and stress testing the systems.	P. 12 P. 12 P. 17 P. 17 P. 17 P. 19 P. 26

	8. Educating and empowering the public to stay safe in cyberspace. Ensuring engagement of vulnerable groups, and providing a one-stop self-help portal against scams. 9. Reviewing the existing laws to plug any loopholes that might be exploited. 10. "Deep expertise to deal with cybercrimes need not just reside with the Government and can be found within the private sector and academia. Given the rapidly evolving nature of cybercrime, the Government will work closely with industry players and Institute of Higher Learning (IHLs) so that the necessary information and expertise to deal with the latest threat posed by cybercrime can be shared seamlessly." 11. Make cybersecurity a business priority: "We will also work with TACs to advocate the Security-by-Design approach and incorporate cybersecurity holistically into business risk management." 12. Raise Awareness	P. 28 P. 28 P. 33 P. 32
Investigation of and punitive measures for cyber crime	No specific investigatory measures specified other than the following: (i) "The Government is investing in technologies and systems that will strengthen and integrate the NCSC's [National Cyber Security Centre] three key functions of threat discovery, threat analysis and incident response. This will enable faster threat discovery and operational response for cross-sector cyber incidents." (ii) Enhancing the Singapore Police Force (SPF) Cybercrime Command. (iii) Boosting cybercrime investigation capabilities through several initiatives. One such example is DIGital Evidence Search Tool (DIGEST) that will automate the forensic processing of voluminous data. (iv) Strengthening coordination between SPF and government agencies.	P. 16 P. 27 P. 27 P. 27
Status of Data Protection Laws	They find a mention as follows: 1. "Work with organisations to embrace data protection as part of their corporate culture"	P. 30

	2. "Professionalise Data Protection Officers to support the effective implementation of data protection measures" 3. "Enhance Singapore's standing as a trusted data hub by introducing Data Protection Trustmarks and working with foreign Data Protection Authorities to facilitate crossborder data flows."	
Skilling and Capacity Building for Cybersecurity Personnel	1. Equipping public officers handling sensitive data with the relevant skills to combat cyber crime. 2. "Encourage existing professionals to remain and further their development in the industry. We will institute clear career pathways, promote certification, and foster strong communities of practice." 3. "Work with industry and IHLs to attract new graduates and convert existing professionals from related fields. IHLs will update their curriculum to be relevant to industry needs so as to facilitate the transition of new entrants to the workforce. We will offer cybersecurity scholarships and sponsorships to attract promising students. We will also offer up-skilling and re-skilling opportunities to cross-train mid-career professionals in cybersecurity for better job prospects."	P. 27 P. 36 P. 36
Economic Growth of the ICT sector generally	1. We will ensure the resilience of our national infrastructure and a safer cyberspace, supported by a vibrant ecosystem that provides good jobs and economic opportunities for Singaporeans." 2. "The Government has also collaborated with the private sector to jointly develop capabilities to respond to the latest cyber threats. For instance, SPF has partnered local research institutes to develop new cybercrime investigations and forensics capabilities. MHA has also worked with IHLs to create conducive environments for the development of cyber-related innovations. One example is MHA and Temasek Polytechnic's joint establishment of the Temasek Advanced Learning, Nurturing and Testing (TALENT) Lab, which serves as a platform for IHL students to design and validate innovations, to see if they are effective in dealing with cyber-threats." 3. "Trust is essential for a data-enabled economy and society. To build a trusted data ecosystem, our organisations have to shift from compliance to accountability." 4. "Support research into both technological and human-science aspects of cybersecurity through	P. 6 P. 28 P. 30

	the S$190 million National Cybersecurity R&D (NCR) Programme" 5. "Establish world-class facilities in specialised research areas and develop local talent to sustain the community." 6. "Collaborate more closely with academia and industry under the NCR Programme to develop innovative ideas and enhance translational capabilities. A stronger public-private partnership will ensure that R&D can address real-world problems in a more targeted manner, and move research products more quickly from the lab to the market." 7. "Attract and anchor companies with advanced capabilities in Singapore to inject know-how and dynamism into the local cybersecurity community." 8. "Support start-ups to boost the development of niche and advanced solutions." 9. "Partner with local companies that possess strategic cybersecurity capabilities to develop advanced solutions for Singapore." 10. "Develop opportunities for made-in-Singapore solutions in the global market and facilitate access to new market segments."	P. 40 P. 40 P. 40 P. 38 P. 38 P. 38 P. 38
Approach to foreign investment	Not specified.	
Supply chain risk management	Promotion of Security-by-Design: 1. "Progressively institutionalise Security-by-Design into the governance framework for CII protection." 2. "Promote the practice of penetration testing to discover vulnerabilities early for remediation at the design stage."	P. 14 P. 14
Government initiatives, campaigns and programmes for cyber space	1. Singapore will continue to contribute at existing ASEAN channels for cooperation such as the annual ASEAN CERT Incident Drill (ACID), ASEAN Network Security Action Council (ANSAC), ASEAN Regional Forum (ARF) Mechanisms as well as ASEAN cybersecurity and cybercrime workshops. 2. Singapore will host an annual Singapore	P. 45 P. 47

	International Cyber Week (SICW) to catalyse, stimulate and promote exchanges on current and emerging issues pertinent to the cyber community. 3. "The implementation of Security-by-Design has to be complemented with highly skilled professionals who can carry out security validation processes rigorously and proficiently. The introduction of CREST penetration testing certifications and accreditations in Singapore is one means of raising the professional competency standards."	P. 14
Other relevant strategies or policy documents	Not specified.	

SOUTH AFRICA

Country- South Africa

Document Title- National Cybersecurity Policy Framework for South Africa[13] (NCPF)

Date- 2015

Prepared By- Minister of State Security

PARAMETERS	CONTENTS / DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	The Strategy states that it addresses the following – - Centralise coordination of Cybersecurity activities, by facilitating the establishment of relevant structures, policy frameworks and strategies in support of Cybersecurity in order to combat cybercrime, address national security imperatives and to enhance the information society and knowledge-based economy; - Foster cooperation and coordination between Government, the private sector and civil society by stimulating and fostering a strong interplay between policy, legislation, societal acceptance and technology; - Promote international cooperation; - Develop requisite skills, research and development capacity; - Promote a culture of Cybersecurity; and - Promote compliance with appropriate technical and operational Cybersecurity standards.	P. 15
Basic Pillars	Not specifically identified, apart from the key objectives filled out above.	

[13] Accessible at https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf, last accessed on 5 January 2020.

Identified Threats / Challenges	The Strategy identifies cybercrime, cyber terrorism, cyber war and cyber espionage as threats and provides the example of the 2008 Estonia DDOS cyber-attacks.	P. 10
Approach specified (if any)	Yes, the Strategy explicitly acknowledges that it is adopting multi-stakeholderism. This is one of the key objectives in the Strategy.	P. 15
Definitions of Key Concepts	The Strategy defines National Critical Information Infrastructure, Computer Security Incident Response Team, Cybersecurity, Cybersecurity Hub, Cyberspace, Cyber Warfare, Cyber espionage, cyber terrorism, cybercrime, ICT, information society, JCPS CRS, malware, organization and user's assets, organ of state, phishing.	P. 12
Period of Validity	Not specified.	
Allocated Budgetary Resources (If any)	Not specified.	
First responders in Cyber Incident Management and Response	The Strategy envisages the JCPS Cybersecurity Response Committee for incident response, together with the CSIRT and Additional CSIRTs for specific sectors. Additionally, the Strategy envisages a Cybersecurity Centre to support the JCPS CRS operationally.	P. 15-19
Institutions (Civilian) Institutions (Military)	The Strategy mentions establishing several organizations such as the Justice, Crime Prevention and Security Cluster (JCPS), Cybersecurity Centre, CSIRT and the Additional CSIRTs (all appearing to be largely civilian in nature). The Strategy also envisages the establishment of the National Cybersecurity Advisory Council (NCAC)to advise the Telecom and Postal Services Ministry on cybersecurity policy. Military agencies- Department of Defence and Military Veterans (DOD&MV) has overall responsibility for coordination, accountability and implementation of cyber defence measures in the	P. 6 P.29 P. 29

	Republic as an integral part of its National defence mandate.	
Role of Intelligence Agencies	Ministry of State Security and its State Security Agency has overall responsibility and accountability for coordination, development and implementation of Cybersecurity measures in the Republic as an integral part of its National Security mandate. Cybersecurity Centre is to facilitate coordination regarding national intelligence, national defence and cybercrime.	P. 27 P. 28
Offensive Cyber Capabilities	Not specified.	
Declared stance on international norms for responsible State behaviour in cyberspace	Not dealt with. Under the heading "international cooperation", the Strategy simply states that South Africa will participate in international fora on cybersecurity. Nothing specified on public attribution either.	P. 23-24
Declared stance on free and open nature of the internet	The Strategy recognizes the "indispensability of extensive and free use of information technology of information technology to the functioning of open and modern societies".	P.11
International Cooperation and Information Sharing Mechanisms	Under the heading "international cooperation", the Strategy simply states that South Africa will participate in international fora on cybersecurity. Nothing specific on information sharing mechanisms with other countries. Observer status to the Budapest Convention.	P. 23-24
Relationship between the public and private sector	Not explicitly. Under "Role and Responsibility of Private Sector", the Strategy places the onus on the private sector of implementing cybersecurity measures at least equal to those of the State's. The Telecom Dept and the Cybersecurity Hub are to help.	P. 29

Preventive measures for cyber crime	The Strategy provides that the Ministry of State Security and the State Security Agency will- -Ensure that the JCPS cluster is properly capacitated and is able to perform its function as set out in this Policy framework including ensuring that the JCPS cluster has the necessary capacity to monitor, promote and guide the implementation of the NCPF. -Ensure, in consultation with the relevant stakeholders, the establishment of the Cybersecurity Response Committee, Cybersecurity Centre and proper function of the existing RSA Government CSIRT in line with the approved JCPS implementation plan. -Initiate and lead a process within the JCPS cluster for the development and approval of guidelines and National security norms for the establishment of various sector CSIRTs as provided for in the policy framework. -Have an overall responsibility for the development and formulation of National Cybersecurity in Republic and in consultation with stakeholders. This includes reviewing and amending existing Cybersecurity policies as well as prescribing regulations on information and communications technology security for the Republic in order to advance the National Security interests of the Republic -Provide information assurance and secure information and communications technology infrastructure of National importance in support of national security; This should include the development of State capacity to provide threat monitoring, alerting, C{}-ordination and response for information communications technology related incidents pertaining to National Critical Information Infrastructure of the State; -Prescribe a regulatory framework for the control by the State of the provision and application of cryptographic solutions, development of National strategy and regulations for the protection of National Critical Information Infrastructure, and prescribe information communications technology	P. 27-28

	security technical standards to which the electronic communications security products and services of organs of State must comply; Police Responsibilities- (a) The fight against child sexual/physical abuse material on the Internet; (b) Actions to counter massive attacks against information systems such as "denial-of service attacks (such as those affecting the banking sector); (c) Actions combating identity fraud; (d) The development of cross-border law enforcement cooperation; (e) Public-private cooperation to fight cybercrime (in particular between law enforcement authorities and private companies); and (f) Promote enhanced international cooperation to fight cybercrime by taking part in various international initiatives such the UN High Level Expert Group on Cybersecurity and the International Telecommunication Union.	P. 28
Investigation of and punitive measures for cyber crime	The Strategy states that the Department of Justice and Constitutional Development and the National Prosecuting Authority are responsible for prosecuting cybercrimes and also – -For implementation plan of review and alignment of all cybersecurity laws with the NCPF -Ensure relevant legislations are passed for cybercrimes and punishment	P.26
Status of Data Protection Laws	Not specified. However, the Strategy recognizes the need for review and updating of existing privacy regime.	P. 25

Skilling and Capacity Building for Cybersecurity Personnel	Department of Science and Technology (DST) has the responsibility for the development, coordination and implementation of national capacity development program. Furthermore, the Department shall be responsible for developing and facilitating the implementation of a national Cybersecurity research and development agenda for South Africa.	P. 29
Economic Growth of the ICT sector generally	Not specified.	
Approach to foreign investment	Not specified.	
Supply chain risk management	Not specified.	
Government initiatives, campaigns and programmes for cyber space	None specified.	
Other relevant strategies or policy documents	None mentioned.	

SRI LANKA

Country- Sri Lanka

Document Title- Information and Cyber Security Strategy of Sri Lanka[14]

Date- November 2018

Prepared By- Sri Lanka CERT|CC

PARAMETERS	CONTENTS/DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	The Strategy states that it seeks to show commitment to keep the nation safe, secure and prosperous. It aims to create a resilient and trusted cybersecurity ecosystem that will enable Sri Lankan citizens to realize the benefits of digital technology and facilitate growth, prosperity and a better future.	P. 1
Basic Pillars	The Strategy identifies its basic pillars as follows – 1. Establishment of a governance framework to implement the National Information and Cyber Security Strategy. 2. Enactment and formulation of legislation, policies, and standards to create a regulatory environment to protect individuals and organizations in the cyberspace. 3. Development of a skilled and competent workforce to detect, defend and respond to cyberattacks. 4. Collaboration with public sector authorities to ensure that the digital government systems implemented and operated by the, have the appropriate level of cybersecurity and resilience. 5. Raising awareness and empowering citizens to defend themselves against cybercrimes. 6. Development of public-private, local-international partnerships to create a robust	P. 1

[14] Accessible at https://www.cert.gov.lk/Downloads/NCSStrategy.pdf.

	cyber-security ecosystem.	
Identified Threats / Challenges	The Strategy identifies the following threats / challenges – **<u>Threats (Mentioned as reported incidents)</u>** 1. Phishing, DOS/DDoS 2. Privacy Violation 3. Scams 4. Malicious Software/Ransomware 5. Financial Frauds 6. Compromised Websites/Emails 7. Intellectual Property Violation 8. Unauthorized access 9. Social Media Incidents- fake accounts, photo abuse, cyberbullying etc **<u>Adversaries / Actors-</u>** Not specified.	P. 4
Approach specified (if any)	Not specified in the Strategy, however, emphasis is placed on public-private partnerships as one of the pillars.	P. 5
Definitions of Key Concepts	None	
Period of Validity	2019-2023	
Allocated Budgetary Resources (If any)	Not specified.	
First responders in Cyber Incident Management and Response	Not specified. However, the Strategy notes the CERT-SL will undertake computer emergency response handling services. CERT-SL is established under the Information and Communication Technology Agency (ICTA) and operates under the Ministry of Telecommunication, Digital Infrastructure and Foreign Employment.	Page 7 P. 6
Institutions (Civilian) Institutions (Military)	The Strategy informs that a Digital Infrastructure Protection Agency (DIPA) will be established as the apex body for all cyber security related issues in Sri Lanka.	P. 7

	The Strategy notes that under this DIPA – (a)CERT-SL will continue to operate to protect public and private users; (b)24X7 Cyber Security Call Centre will be established; (c)National Cyber Alert System to be established with involvement of ISPs, Telcos; (d)Digital Forensic Lab to be established; (e)National Cyber Security Operating Centre to monitor threats to government applications, CNI; (f)National Certification Authority to address limitations of Certification Service Providers; (g)Research Unit to be established. The Strategy also states that a Joint Military Security Operation Centre/ Defence CERT will be set up to improve coordination between Sri Lankan military, police and intelligence services.	P. 18
Role of Intelligence Agencies	Not specified	
Offensive Cyber Capabilities	Not specified	
Declared stance on international norms for responsible State behaviour in cyberspace	Not specified. Nothing specified on public attribution either.	
Declared stance on free and open nature of the internet	Not specified.	
International Cooperation and Information Sharing Mechanisms	The Strategy notes the importance of engaging with international organizations including the International Telecommunication Union, the European Union Agency for Network and Information Security (ENISA), Asia Pacific- CERT, ICANN, Forum for Incident Response Security Team (FIRST), UN Internet Governance Forum, Internet Society (ISOC), International Watch and Warning Network (IWWN), International Criminal Police Organization (Interpol) for-	P.18 (Para 6.7)

	-exchanging technical information on threats and vulnerabilities; -obtaining latest software and hardware products; -conducting joint cyber drills; -building staff capacity. The Strategy also notes that Sri Lanka has ratified the Budapest Convention.	P. 18 (Para 6.8)
Relationship between the public and private sector	The Strategy notes the need for – -Partnering with businesses to promote security in products and services; -nurturing start-ups; -Promoting cooperation with industry sector (in the context of sharing information)	P. 19 (Para 6.10, 6.13) P. 18 (Para 6.6)
Preventive measures for cyber crime	The Strategy also fleshes out the following measures – -information and cyber security risk assessment to be carried out, particularly in CNI; -Security policies for government digital infrastructure and establish a Digital Government Infrastructure Protection Unit; No other specific measures in the Strategy.	P. 12 P. 13
Investigation of and punitive measures for cyber crime	The Strategy states that the Budapest Convention will be implemented.	P. 18
Status of Data Protection Laws	The Strategy notes the lack of an adequate legislative framework for data protection in Sri Lanka and promises to enact suitable legislations.	P. 9 (Para 2.2)
Skilling and Capacity Building for Cybersecurity Personnel	The Strategy places emphasis on skilling and capacity, evident from Pillar 3- Development of a Competent Workforce. The salient features in this portion include – -Assessing supply & demand for professionals; -introduce a “Competency Framework” that outlines	P. 10-11

	the core competencies that both the govt and the private sector should possess; -up-skilling and re-skilling opportunities for public sector staff; -establish training infrastructure across the country;	
Economic Growth of the ICT sector generally.	Same as Relationship between the public and private sector.	
Approach to foreign investment	Not specified.	
Supply chain risk management	The Strategy espouses a Security-by-design approach for government infrastructure.	P.14 (Para 4.6)
Government initiatives, campaigns and programmes for cyber space	Not specified.	
Other relevant strategies or policy documents	Not specified.	

UNITED KINGDOM

Country- United Kingdom

Document Title- National Cyber Security Strategy 2016-2021[15]

Date- 2016

Prepared By- Cabinet Office (otherwise not specified)

PARAMETERS	CONTENTS/DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	Vision for 2021 is that the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.	Para 1.4
Basic Pillars	No pillars identified. But the objectives identified are (1) Defend, (2) Deter and (3) Develop. Cyber-strategy based on the following assessments – • the scale and dynamic nature of cyber threats, and our vulnerability and dependency, mean that maintaining the current approach will not in itself be sufficient to keep us safe; • a market based approach to the promotion of cyber hygiene has not produced the required pace and scale of change; therefore, Government has to lead the way and intervene more directly by bringing its influence and resources to bear to address cyber threats; • the Government alone cannot provide for all aspects of the nation's cyber security. An embedded	Para 1.5 Para 2.7

[15] Accessible at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

	and sustainable approach is needed where citizens, industry and other partners in society and government, play their full part in securing our networks, services and data; • the UK needs a vibrant cyber security sector and supporting skills base that can keep pace with and get ahead of the changing threat.	
Identified Threats / Challenges	Broadly identifies categories of cyber-threat actors as – (i) Cyber criminals (ii) States and State Sponsored Threats (iii) Terrorists (iv) Hacktivists (v) Script Kiddies	Paras 3.2-3.6 Paras 3.7-3.10 Para 3.11-3.12 Para 3.13 Para 3.14
Approach specified (if any)	Multi-stakeholder Model is explicitly acknowledged and adopted.	Page 63
Definitions of Key Concepts	The Strategy defines “cyber security” as – “the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.”	Para 2.11
Period of Validity	2016-2021	
Allocated Budgetary Resources (If any)	£1.9 billion over 5 years generally “a proportion” of £165m Defence and Cyber Innovation Fund to support innovative procurement in defence and security.	Para 1.14, Page 10 Para .13, Page 10

First responders in Cyber Incident Management and Response	The Strategy identifies the following organizations in relation to incident response- -CERT-UK (by its very nature) -National Cyber Security Centre has been mooted as a "centralized incident reporting and response mechanism" but it appears that the NCSC has been conceived of as more of a capacity builder rather than a first responder itself.	 P. 73 Para 5.6.9 and P. 29
Institutions (Civilian)	1. National Cyber Security Centre [replaces the Communications-Electronic Security Group (CESG) 2. National Cyber Crime Unit in the National Crime Agency 3. Cyber-crime units in the Regional Organized Crime Units (regional level cyber specialist capabilities, supporting the NCCU and local forces) 4. Action Fraud (for cyber-crime or cyber-enabled fraud reporting)	Para 6.2.3, P. 48; Para 6.2.6, P. 49
Institutions (Military)	Not specified.	
Role of Intelligence Agencies	No exhaustive list provided. But the Strategy does mention that the National Cyber Security Centre has absorbed the CESG (Communications Electronic Security Group-information security arm of the GCHQ), the Centre for the Protection of National Infrastructure (CPNI), CERT-UK (Computer Emergency Response Team) and the Centre for Cyber Assessment (CCA), which is expected to simplify the overall intelligence agency structure.	
Offensive Cyber Capabilities	"Enhancing Sovereign Capabilities- Offensive Cyber" is a goal under the "Deter" prong of the cyber strategy. This portion specifies the dedicated National Offensive Cyber Programme in existence to build capacity for offensive operations. It also lists the objective as ensuring that the UK has "*appropriate offensive cyber capabilities that can be*	Para 6.5 Para 6.5.2

	deployed at a time and place of our choosing, for both deterrence and operational purposes", with the caveat that it will be in accordance with national and international law. Para 6.5.3 lists out how this will be achieved- • invest in our NOCP – the partnership between the Ministry of Defence and GCHQ that is harnessing the skills and talents of both organisations to deliver the tools, techniques and tradecraft required; • develop our ability to use offensive cyber tools; and • develop the ability of our Armed Forces to deploy offensive cyber capabilities as an integrated part of operations, thereby enhancing the overall impact we can achieve through military action.	
Declared stance on international norms for responsible State behaviour in cyberspace	UK notes existing work on cybernorm-making – "*there has been agreement that international law applies in cyberspace; that human rights apply online as they do offline; and a broad consensus that the multi-stakeholder approach is the best way to manage the complexities of governing the Internet.*" UK's approach will include- • strengthen and embed a common understanding of responsible state behaviour in cyberspace; • build on agreement that international law applies in cyberspace; • continue to promote the agreement of voluntary, non-binding, norms of responsible state behaviour; • support the development and implementation of confidence-building measures; • increase our ability to disrupt and prosecute cyber criminals based abroad, especially in hard-to-reach jurisdictions; • help foster an environment which allows our law enforcement agencies to work together to ensure fewer places exist where cyber criminals can act without fear of investigation and prosecution;	Para 8.2 Para 8.4

	• promote the resilience of cyberspace by shaping the technical standards governing emerging technologies internationally (including encryption), making cyberspace more 'secure by design' and promoting best practice; • work to build common approaches amongst like-minded countries for capabilities such as strong encryption, which have cross-border implications; • build the capacity of others to tackle threats to the UK, and our interests overseas; • continue to help our partners develop their own cyber security – since we share a single cyberspace, we collectively become stronger when each country improves its own defences; • ensure that NATO is prepared for the conflicts of the 21st century, which will play out in cyberspace as well as on the battlefield; • work with our allies to enable NATO to operate as effectively in cyberspace as it does on land, air and sea; and • ensure that the 'London Process' of Global Conferences on Cyberspace continues to promote global consensus towards a free, open, peaceful and secure cyberspace. The Strategy declares that it will publicly attribute cyber attacks from the following - "To reduce the cyber threat from hostile foreign actors, we will attribute specific cyber identities publicly when we judge it in the national interest to do so."	Para 6.3.3
Declared stance on free and open nature of the internet	The Strategy notes that the UK seeks to "*ensure the continuation of a free, open, peaceful and secure cyberspace that delivers these benefits*" [benefits being economic benefits and social well-being] The Strategy further notes that the UK will continue to – -champion the multi-stakeholder model of internet governance; -oppose data localisation; -and work to build the capacity of our partners to improve their own cyber security.	Para 8.1 Para 8.3

International Cooperation and Information Sharing Mechanisms	The Strategy notes that while countering hostile foreign actors, the UK will use "existing networks and relationships with our key international partners to share information about current and nascent threats, adding value to existing thought and expertise." Apart from this, the following is identified as a step the Government will take to bring about cyber security- • *Expanded intelligence and law enforcement focus on the threat*. The intelligence agencies, the Ministry of Defence, the police and the National Crime Agency, in coordination with international partner agencies, will expand their efforts to identify, anticipate and disrupt hostile cyber activities by foreign actors, cyber criminals and terrorists. This will improve their intelligence collection and exploitation, with the aim of obtaining pre-emptive intelligence on the intent and capabilities of our adversaries. A member of the Budapest Convention.	Para 6.3.3 Para 4.16
Relationship between the public and private sector	Although the Strategy states that the private sector will be given boosts and recognizes the Government's role in ensuring cyber security, it also places emphasis on the private sector's own role in protecting themselves – "*the Government will meet its responsibilities and lead the national response, but businesses, organisations and individual citizens have a responsibility to take reasonable steps to protect themselves online and ensure they are resilient and able to continue operating in the event of an incident*." In fact, it is suggested that the government will "*not accept significant risk being posed to the public and the country as a whole as a result of businesses and*	Para 4.5 Para 4.5

	organisations failing to take the steps needed to manage cyber threats." In the context of the role of businesses and organizations, the cyber-strategy states "*But with this technological transformation comes the responsibility* *to safeguard the assets which they hold…..<u>Businesses and organisations must also understand that, if they are the victim of a cyber attack, they are liable for the consequences.</u>"* The Strategy also highlights the use of regulation and incentives to make the private sector cyber-secure- "*For businesses, we will work through organisations such as insurers, regulators and investors which can exert influence over companies to ensure they manage cyber risk. In doing so, we will highlight the clear business benefits and the pricing of cyber risk by market influencers.*"	Para 4.8 Para 5.5.4
Preventive measures for cyber crime	Categorizes cybercrimes as "cyber-enabled" and "cyber-dependent". Preventive Measures- (i) Promotes "Active Cyber Defence (ACD)" as a way of making systems more robust against attack. ACD is defined as *cyber security analysts developing an understanding of the threats to their networks, and then devising and implementing measures to proactively combat, or defend, against those threats*. (ii) Plans to achieve ACD by- • work with industry, especially Communications Service Providers (CSPs), to make it significantly harder to attack UK internet services, including securing UK's telecommunications and internet routing infrastructure. • Increase capabilities of GCHQ, Ministry of Defence and National Cybercrime Agency (NCA). • better protect government systems and	Para 3.2 Para 5.1.1 Para 5.1.3

	networks, help industry build greater security into the CNI supply chain, make the software ecosystem in the UK more secure, and provide automated protections for government online services to the citizen. • work with finance sector to make it hostile to those seeking to monetise stolen credentials. Specific Governmental activities – • working with CSPs to block malware attacks by blocking specific websites, domains (DNS blocking / filtering) • deploying email verification / filtering systems on government networks to stop phishing. • Promoting best practices in multi-stakeholder forums such as ICANN, IETF, IGF, RIPE. • Securing routing of internet traffic for government depts. • Adopt "secure by default" standard for products, requiring the consumer to actively disable the setting for it to become insecure. • The Government Digital Service (GDS), the Crown Commercial Service (CCS) and the NCSC will ensure that all new digital services built or procured by government are also 'secure by default'. Awareness spreading efforts – • Cyber Aware Campaign (Targeted messaging delivered through social media, advertising and in partnership with the business promotes, eg. Using three random passwords, latest software downloads) • Cyber Essentials (The Cyber Essentials scheme was developed to show organisations how to protect themselves against low-level "commodity threat" – lists five technical controls that organizations should have- (i) access control; (ii) boundary firewalls and internet gateways; (iii) malware protection; (iv) patch management; (v)n secure configuration.	Para 6.2.5 Para 5.1.5 Para 5.2.4, 5.2.5 Para 5.3.3 Page 43
Investigation of and punitive measures for	No punitive measures specified, other than the general deterrent of prosecuting cyber criminals.	Para 6.2.5

cyber crime	As regards investigation, the strategy lays out capacity-strengthening measures among cyber-intelligence / investigatory authorities – (i) build a better understanding of the cyber crime business model, so we know where to target interventions in order to have the most disruptive effect on criminal activity. (ii) tackle cyber crime upstream, adding friction to the criminal business model by dismantling their infrastructure and financial networks (iii) Provide industry with proactive intelligence and encourage industry to share upstream intelligence so as to disrupt upstream activities. (iv) Develop 24/7 reporting and triage capability in Action Fraud, NCSC, NCA's National Cyber Crime Unit and wider law enforcement.	Para 6.2.5
Status of Data Protection Laws	The Strategy does not go into any detail. However, the Strategy fleshes out how the Government will "*make use of all available levers, including the forthcoming General Data Protection Regulation (GDPR), to drive up standards of cyber security across the economy, including, if required, through regulation*." The Strategy reiterates this in the context of "Changing Public and Business Behaviours" in that it states that the Government will also make sure it has the "*right regulatory framework in place to manage those cyber risks the market fails to address. As part of this, we will seek to use levers, such as the GDPR, to drive up standards of cyber security and protect citizens*."	Para 4.16 Para 5.5.4
Skilling and Capacity Building for Cybersecurity Personnel	The Strategy recognizes this "requires action for the next twenty years, not just the next five". The measures intended to be taken by the	Para 7.1.4

	Government are then listed out – • establishing a schools programme to create a step change in specialist cyber security education and training for talented 14-18 year olds (involving classroom-based activities, after-school sessions with expert mentors, challenging projects and summer schools); • creating higher and degree-level apprenticeships within the energy, finance and transport sectors to address skills gaps in essential areas; • establishing a fund to retrain candidates already in the workforce who show a high potential for the cyber security profession; • identifying and supporting quality cyber graduate and post graduate education, and identifying and filling any specialist skills gaps – acknowledging the key role that universities play in skills development; • supporting the accreditation of teacher professional development in cyber security. This work will help teachers, and others supporting learning, to understand cyber security education and provide a method of externally accrediting such individuals; • developing the cyber security profession, including through achieving Royal Chartered status by 2020, reinforcing the recognised body of cyber security excellence within the industry and providing a focal point which can advise, shape and inform national policy; • developing a Defence Cyber Academy as a centre of excellence for cyber training and exercise across the Ministry of Defence and wider Government, addressing specialist skills and wider education; • developing opportunities for collaboration in training and education between government, the Armed Forces, industry and academia, together with facilities to maintain and exercise skills; and • we will work with industry to expand the CyberFirst programme to identify and nurture the diverse young talent pool to defend our national security; and • embedding cyber security and digital skills as an integral an integral part of relevant courses within the education system, from primary to postgraduate levels, setting standards, improving quality and providing a firm foundation for onwards progression into the field.	Para 7.1.9

Economic Growth of the ICT sector generally.	The Strategy recognizes growth issues in the private cybersecurity sector and "funding gaps that prevent SMEs from growing and expanding into new markets and territories." The Strategy lists the following measures to stimulate growth in the sector – • commercialise innovation in academia, providing training and mentoring to academics; • establish two innovation centres, to drive the development of cutting-edge cyber products and dynamic new cyber security companies, which will sit at the heart of a programme of initiatives to give start-ups the support they need to get their first customers and attract further investment; • allocate a proportion of the £165m Defence and Cyber Innovation Fund to support innovative procurement in defence and security; • provide testing facilities for companies to develop their products, together with a fast-track form of assessment for the next generation of cyber security products and services as they emerge, enabling customers to be confident in their use; • draw on the collective expertise of the industry-government Cyber Growth Partnership to help shape and focus further growth and innovation interventions; • help companies of all sizes scale-up and access international markets; and • promote agreed international standards that support access to the UK market.	Para 7.2.1 Para 7.2.3
Approach to foreign investment	Not specified	
Supply chain risk management	No dedicated portion in the Strategy document.	

	But the Strategy recognizes the importance of better protecting government systems and networks and helping industry build greater security into the CNI supply chain. The Strategy also proposes the use of the "secure by default" initiative by the government which lists out the following to-dos – • continue to encourage hardware and software providers to sell products with security settings activated as default, requiring the user to actively disable these settings to make them insecure. Some vendors are already doing this, but some are not yet taking these necessary steps; • continue to develop an Internet Protocol (IP) reputation service to protect government digital services (this would allow online services to get information about an IP address connecting to them, helping the service make more informed risk management decisions in real time); • seek to install products on government networks that will provide assurance that software is running correctly, and not being maliciously interfered with; • look to expand beyond the GOV.UK domain into other digital services measures that notify users who are running out-of-date browsers; and • invest in technologies like Trusted Platform Modules (TPM) and emerging industry standards such as Fast Identity Online (FIDO), which do not rely on passwords for user authentication, but use the machine and other devices in the user's possession to authenticate. The Government will test innovative authentication mechanisms to demonstrate what they can offer, both in terms of security and overall user experience.	Para 5.1.3, 5.2.2 and 5.4.4 Para 5.2.5
Government initiatives, campaigns and programmes for cyber space	Cyber Aware campaign and Cyber Essentials	

Other relevant strategies or policy documents	2013 Serious and Organized Crime Strategy (sets out the UK's strategic response to cyber-crime)	

UNITED STATES OF AMERICA

Country- United States

Document Title- National Cyber Strategy of the United States of America[16]

Date- September 2018

Prepared By- White House

PARAMETERS	CONTENTS/DESCRIPTION	REFERENCE
Declared Objectives/Vision of the Strategy/Policy Document	The objectives identified in the Strategy are – 1) Defend the homeland by protecting networks, systems, functions, and data; (2) Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) preserve peace and security by strengthening the United States' ability — in concert with allies and partners — to deter and if necessary punish those who use cyber tools for malicious purposes; and (4) expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.	P. 3
Basic Pillars	i) Pillar 1- Protect the American People, Homeland and the American Way of Life (ii) Pillar 2- Promote American Prosperity (iii) Pillar 3- Preserve Peace through Strength (iv) Pillar 4- Advance American Influence	P. 3
Identified Threats / Challenges	**Threats / Areas of Concern** (i) National Security- Protect the Confidentiality, Integrity and Availability of US telecommunication networks and prevent them from being compromised by a foreign adversary.	Page 16

[16] Accessible at https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

	(ii) Human Rights Violations **<u>Adversaries / Actors-</u>** (i) State Actors / State Interests- Russia, Iran, China and North Korea (ii) Non-State Actors / Non-State Interests- Russian, Iranian, North Korean and Chinese groups (iii) Transnational Criminal Organizations	Page 24 Page 2 Pages 1 and 2 Page 11
Approach specified (if any)	Explicitly Multi-stakeholder Model.	P. 25
Definitions of Key Concepts	None specified.	
Period of Validity	None specified.	
Allocated Budgetary Resources (If any)	Not specified.	
First responders in Cyber Incident Management and Response	Not specified.	
Institutions (Civilian)	Department of Homeland Security to be given the mandate of securing Federal department and agency networks (excepting DoD, IC and national security networks). Departmental Chief Information Officers to be given powers and held accountable for standardizing government wide-cybersecurity architecture.	Page 6
Institutions (Military)	Not specified.	
Role of Intelligence Agencies	Not specified.	
Offensive Cyber Capabilities	Not specified.	
Declared stance on international norms for responsible State	**<u>Stated Goal:-</u>** US to promote a framework of responsible state behaviour in cyberspace built upon international law,	Page 20

behaviour in cyberspace	adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime, and the consideration of practical confidence building measures to reduce the risk of conflict stemming from malicious cyber activity. **<u>Action to be taken (*Priority Action*):-</u>** Encourage universal adherence to Cyber-Norms. Will do this by:- -Encouraging other nations to publicly affirm these principles and views through enhanced outreach and engagement in multilateral fora. -Increased public affirmation by the United States and other governments will lead to accepted expectations of state behavior and thus contribute to greater predictability and stability in cyberspace. Further, in the Strategy, public attribution is described as an instrument of "national power" to "prevent malicious cyber activity against the United States" and "public statements of support for responsive actions taken" are identified as cyber deterrents.	Page 20 Page 21
Declared stance on free and open nature of the internet	**<u>Stated Goal</u>**:- Promote an Open, Interoperable, Reliable, and Secure Internet. **<u>Action to be taken (*Priority Action*):-</u>** -Protect and promote internet freedom -Work with like-minded countries, industry, academia and civil society. -Promote a multi-stakeholder model of internet governance (as opposed to state centric) -Promote interoperable and reliable communications infrastructure and internet connectivity -Promote and maintain markets for United States ingenuity worldwide	P. 24-25
International Cooperation and Information Sharing	**1. <u>Stated Goal:-</u>** - Combat cyber-crime and improve incident reporting.	P. 10

Mechanisms	**2. <u>Priority Action (Action to be Taken)</u>** **a. Improve apprehension of criminals located abroad-** - USG to "increase diplomatic and other efforts with countries to promote cooperation with legitimate extradition requests." - USG to "push other nations to expedite their assistance in investigations and to comply with any bilateral or multilateral agreements or obligations." **b. <u>Strengthen Partner Nations' Law Enforcement Capacity to Combat Cyber-criminal Activity:-</u>** - US to "aid willing partner nations to build their capacity to address cyber-criminal activity." - Acknowledges "interest of the US national security to continue building cybercrime-fighting capacity that facilitates stronger international law enforcement cooperation." - US to "improve inter- national cooperation in investigating malicious cyber activity, including developing solutions to potential barriers to gathering and sharing evidence. - US to utilize tools such as United Nations Convention Against Trans- national Organized Crime, the G7 24/7 Network Points of Contact and the Budapest Convention. A member of the Budapest Convention.	P. 11
Relationship between the public and private sector	**1A. <u>Stated Goal:-</u>** Secure Federal Networks and Information **1B. <u>Priority Action (Action to be Taken)</u>** a. <u>Strengthen Federal Contractor Cybersecurity</u> - the Federal Government will be able to assess the security of its data by reviewing contractor risk management practices and adequately testing, hunting, sensoring, and responding to incidents on contractor systems. -Contracts to include provisions for cyber-security and authorize Federal oversight. -Key targets- contractors within the defense industrial base responsible for researching and	P. 7

	developing key systems fielded by the DOD. **1A. <u>Stated Goal</u>**:- Secure Critical Infrastructure 1B. **<u>Priority Action (Action to be Taken)</u>** a. Prioritize Action according to Identified Risks- - USG to work with the private sector to protect critical infrastructure - Identified as seven key areas- national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation. b. <u>Leverage Information and Communications Technology Providers as Cybersecurity Enablers-</u> - USG to "work with ICT providers to improve ICT security and resilience in a targeted manner and efficient manner while protecting privacy and civil liberties." - USG to "strengthen efforts to share information" with ICT providers, including "classified threat and vulnerability information with cleared ICT operators" - USG to encourage "industry-driven certification regimes" that ensure solutions can adapt in a rapidly evolving market and threat landscape. **2A. <u>Stated Goal</u>:-** Foster and Protect United States Ingenuity 2B. **<u>Priority Action (Action to be Taken)</u>** a. <u>Protect the confidentiality and integrity of American ideas</u> **-**USG to "work against the illicit appropriation of public and private sector technology and technical knowledge by foreign competitors, while maintaining an investor-friendly climate."	P. 9
Preventive measures for cyber crime	**<u>1A. Stated Goal:-</u>** - Combat cyber-crime and improve incident reporting. **<u>1B. Priority Action (Action to be Taken)</u>** **a. Improve apprehension of criminals**	Page 10

	located abroad- - USG to "increase diplomatic and other efforts with countries to promote cooperation with legitimate extradition requests." - USG to "push other nations to expedite their assistance in investigations and to comply with any bilateral or multilateral agreements or obligations." **b. <u>Strengthen Partner Nations' Law Enforcement Capacity to Combat Cyber-criminal Activity:-</u>** - US to "aid willing partner nations to build their capacity to address cyber-criminal activity." - Acknowledges "interest of the US national security to continue building cybercrime-fighting capacity that facilitates stronger international law enforcement cooperation." - US to "improve inter- national cooperation in investigating malicious cyber activity, including developing solutions to potential barriers to gathering and sharing evidence. - US to utilize tools such as United Nations Convention Against Trans- national Organized Crime, the G7 24/7 Network Points of Contact and the Budapest Convention.	Page 11
Investigation of and punitive measures for cyber crime	Same as above. No specific punitive measures specified other than the following: a. "imposing costs", "prosecutions and economic sanctions" as means of deterring malicious cyber-actors. b. "apprehend and prosecute offenders, disable criminal infrastructure, limit the spread and use of nefarious cyber capabilities, prevent cyber criminals and their state sponsors from profiting from their illicit activity, and seize their assets" by Federal law enforcement in combating cyber-crime c. "disrupt criminal infrastructure through civil injunctions, and impose appropriate consequences upon malicious cyber actors"	P. 8 P. 10 P. 11

Status of Data Protection Laws	Not specified / dealt with. But the Strategy does mention the following in the context of roping in ICT providers in enhancing cyber-security- "the Federal Government must work with these providers to improve ICT security and resilience in a targeted and efficient manner while protecting privacy and civil liberties."	P. 9
Skilling and Capacity Building for Cybersecurity Personnel	**1A. <u>Stated Goal</u>:-** Develop a Superior Cybersecurity Workforce **1B. <u>Priority Action (Action to be Taken)</u>** a. Build and Sustain Talent Pipeline - USG to focus on talent building from primary to secondary education. b. Expand re-skilling and educational opportunities for America's workers - USG to expand federal recruitment, re-skill people from different backgrounds, to re-train them into cybersecurity careers. c. Enhance Federal Cybersecurity workforce – USG to use the National Initiative for Cybersecurity Education (NICE) Framework for a standardized approach for hiring. d. Use Executive Authority to Highlight and Reward Talent **2A. <u>Stated Goal:-</u>** Build International Capacity (as part of the "Advance American Influence" objective) **2B. <u>Priority Action (Action to be Taken)</u>** a. Enhance cyber-capacity building efforts – -USG to help allies strengthen cyber-capacity -USG to "aggressively expand efforts to share	P. 17 P. 26

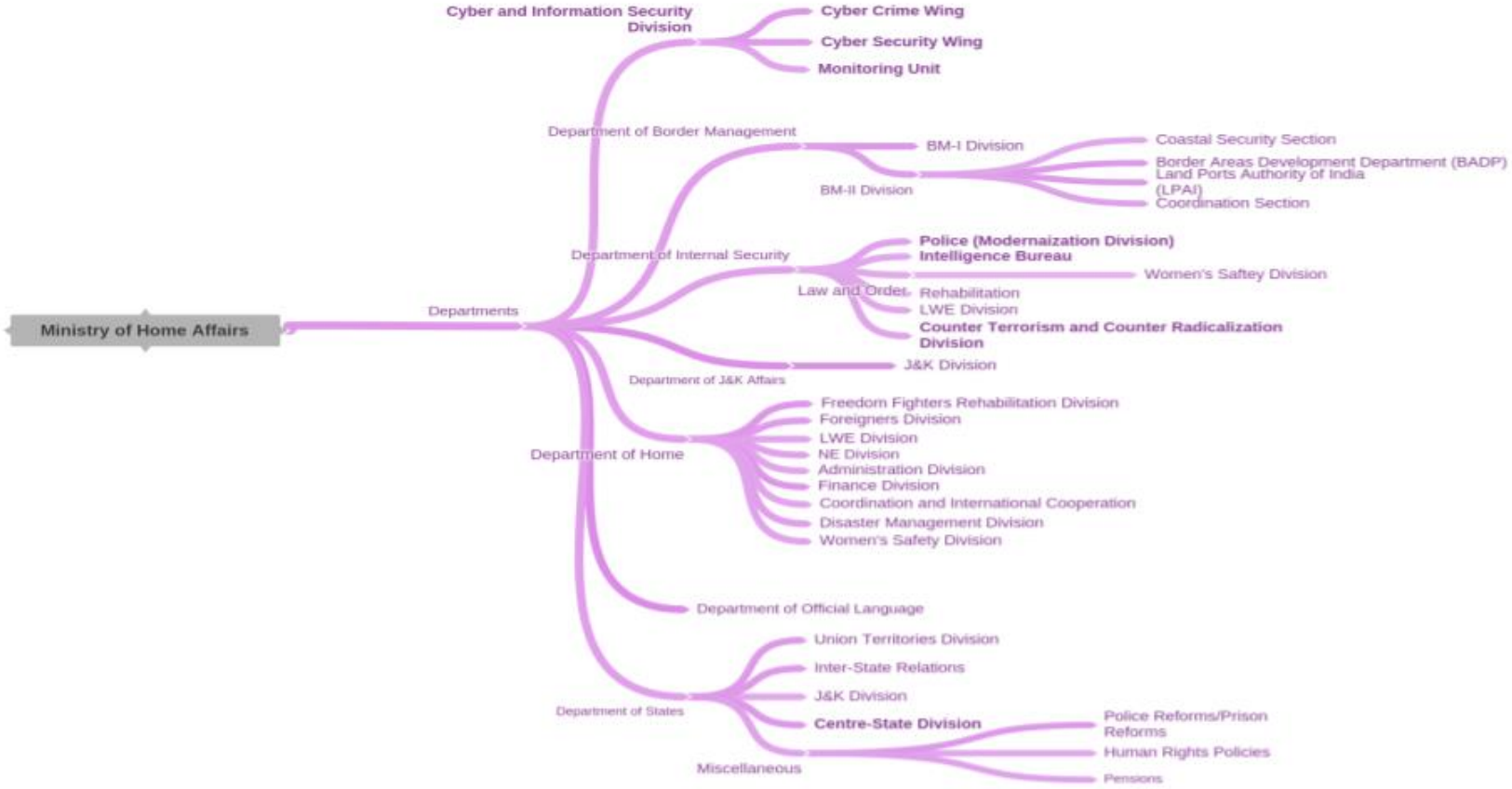
	automated and actionable cyber threat information, enhance cybersecurity coordination, and promote analytical and technical exchanges."	
Economic Growth of the ICT sector generally.	Under Pillar II (Promote American Prosperity), the Strategy outlines the plan for promoting the digital economy. The prime focus is to "*Preserve United States influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency.*" **1A**. **<u>Stated Goal</u>**:- Foster a Vibrant and Resilient Digital Economy **1B**. **<u>Priority Action</u>** a. Incentivize an adaptable and secure technology marketplace b. Prioritize Innovation c. Invest in Next Generation Infrastructure d. Promote the free flow of data across Borders e. Maintain US leadership in emerging technologies f. Promote full life cycle cybersecurity **2A**. **<u>Stated Goal</u>**:- Foster and Protect US Ingenuity **2B. <u>Priority Action</u>** a. Update mechanisms to review foreign investment and operation in the united states. Safeguard US telecommunication networks from being "used or compromised by a foreign adversary to harm the United States". b. Maintain a strong and balanced intellectual property protection system. c. Protect the confidentiality and integrity of American ideas.	P. 14 P. 14 P. 14-15 P. 16
Approach to foreign investment	The Strategy envisages a protective / nationalist approach to the cybersecurity sector – Under the goal "Foster and Protect United States Ingenuity", the Strategy states that the "United	P. 16

	States government will counter predatory mergers and acquisitions and counter intellectual property theft." The Strategy also contemplates reviewing mechanisms to review foreign investment and operation in the United States (telecommunication licenses) to prevent telecommunication networks from being "compromised by foreign adversaries".	P. 16
Supply chain risk management	The Strategy recognizes the importance of standardizing federal cybersecurity with the objective being "*to manage cybersecurity risks to increase the security and resilience of the Nation's information and information systems.*" 1A. **<u>Stated Goal:-</u>** Secure Federal Networks and Information 1B. **<u>Priority Action</u>** a. Further centralize management and oversight of civilian cybersecurity- Federal agencies to transition to shared services and infrastructure. DHS to standardize federal security, except DoD and Intelligence Community (IC). b. Align risk management and information technology activities- -Chief Information Officers (CIO) in each department and agency to be held accountable for aligning cybersecurity risk management decisions and IT budgeting and procurement decisions. -CIOs have to ensure IT procurement takes into account cybersecurity. c. Improve federal supply chain risk management- -Supply chain risk management to be integrated into agency procurement and risk management processes to better ensure technology is secure. -Ensure better sharing of information among departments and agencies to improve awareness of	P. 6 P. 6 P. 7 P. 7

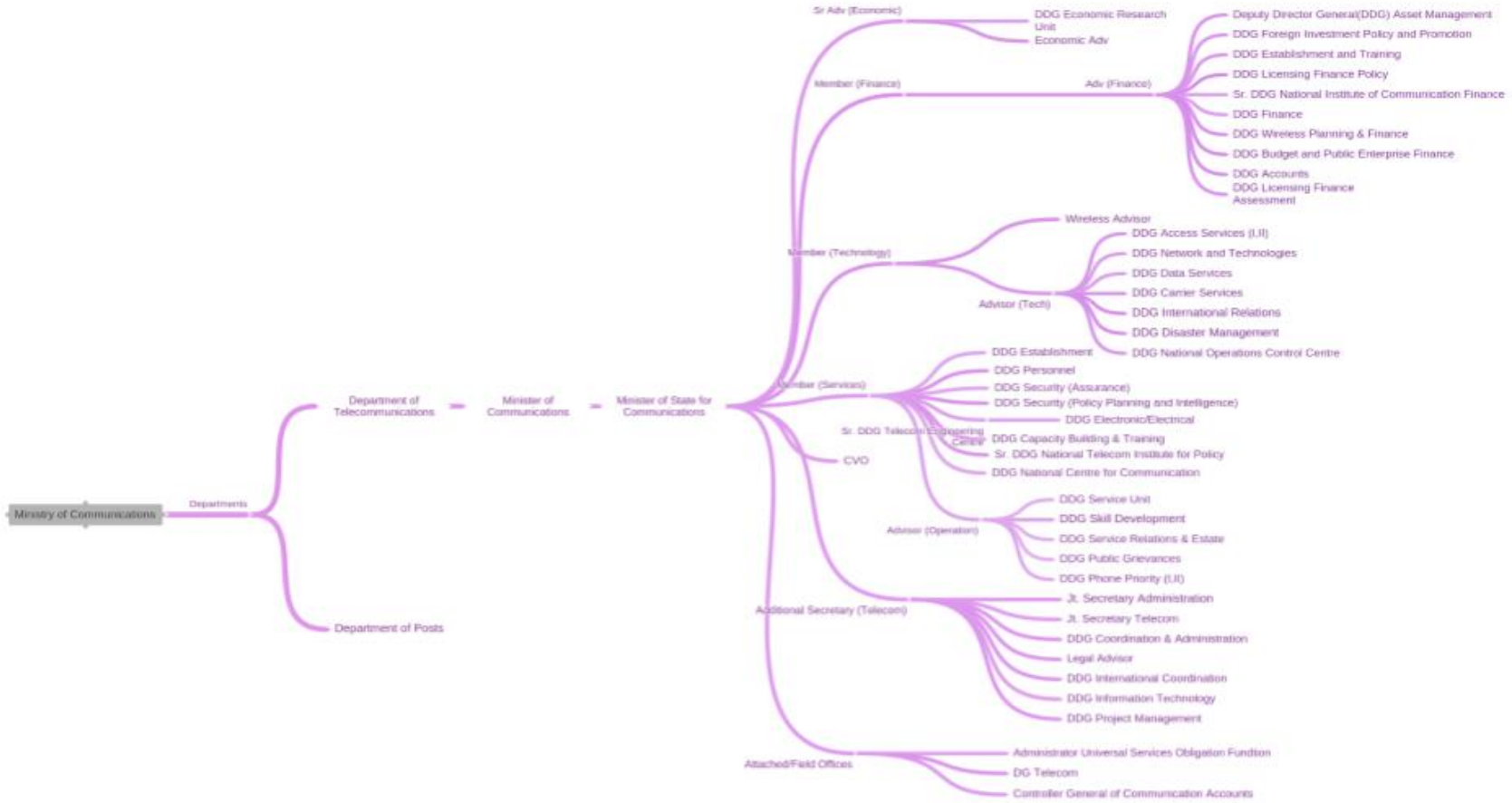
	supply chain threats and reduce duplicative supply chain activities within the United States Government, including by creating a supply chain risk assessment shared service. - Includes addressing deficiencies in the Federal acquisition system, such as providing more stream-lined authorities to exclude risky vendors, products, and services when justified. d. Strengthen federal contractor cyber-security- - the Federal Government will be able to assess the security of its data by reviewing contractor risk management practices and adequately testing, hunting, sensoring, and responding to incidents on contractor systems. -Contracts to include provisions for cyber-security and authorize Federal oversight. -Key targets- contractors within the defense industrial base responsible for researching and developing key systems fielded by the DOD.	P. 7
Government initiatives, campaigns and programmes for cyber space	None specified.	
Other relevant strategies or policy documents	• Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* • E.O. 13800 *Report to the President on Federal IT Modernization*	P. 1 P. 7

ANNEXURE ‘B’
ORGANOGRAMS OF RELEVANT MINISTRIES

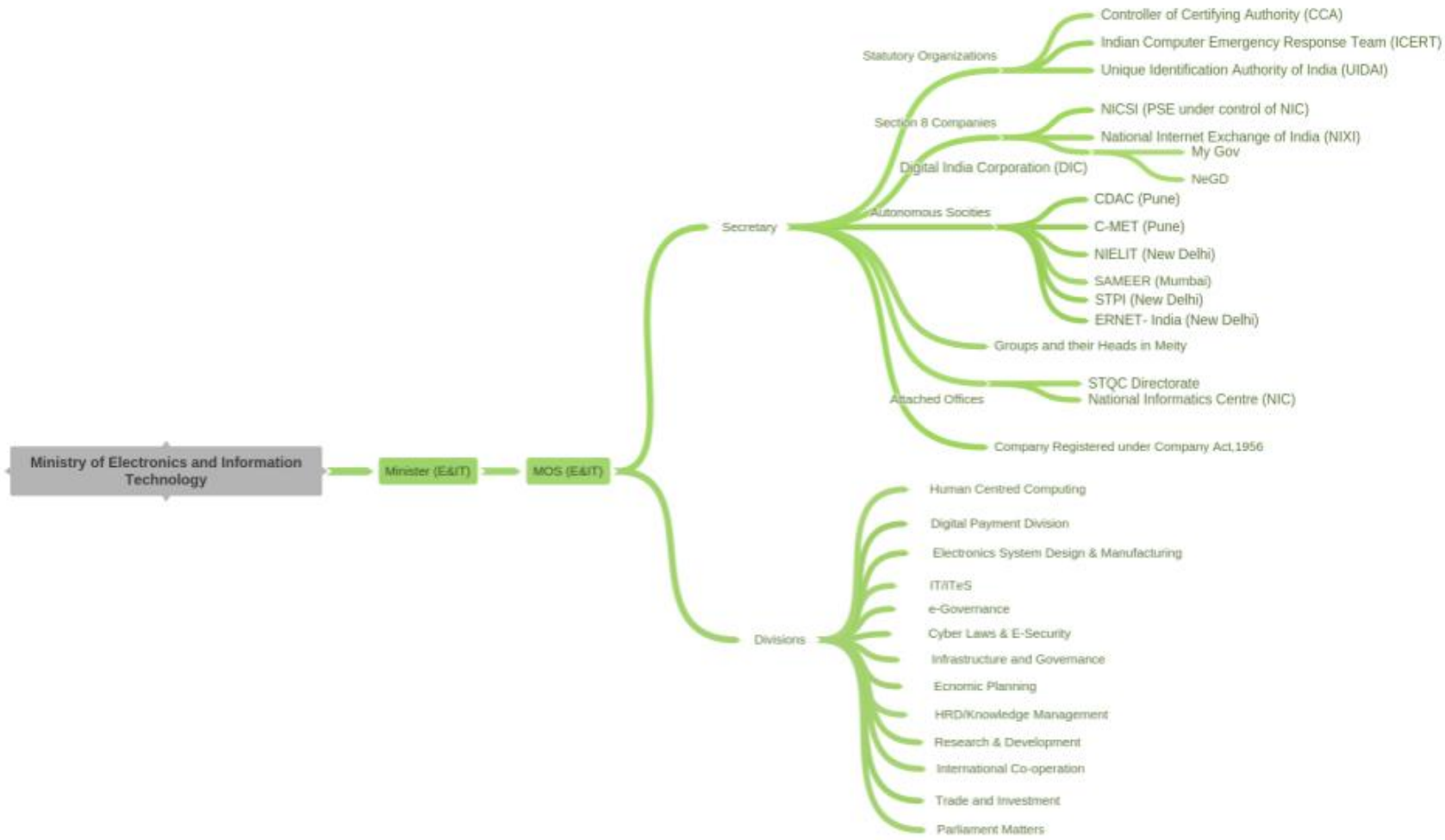
Ministry of Home Affairs



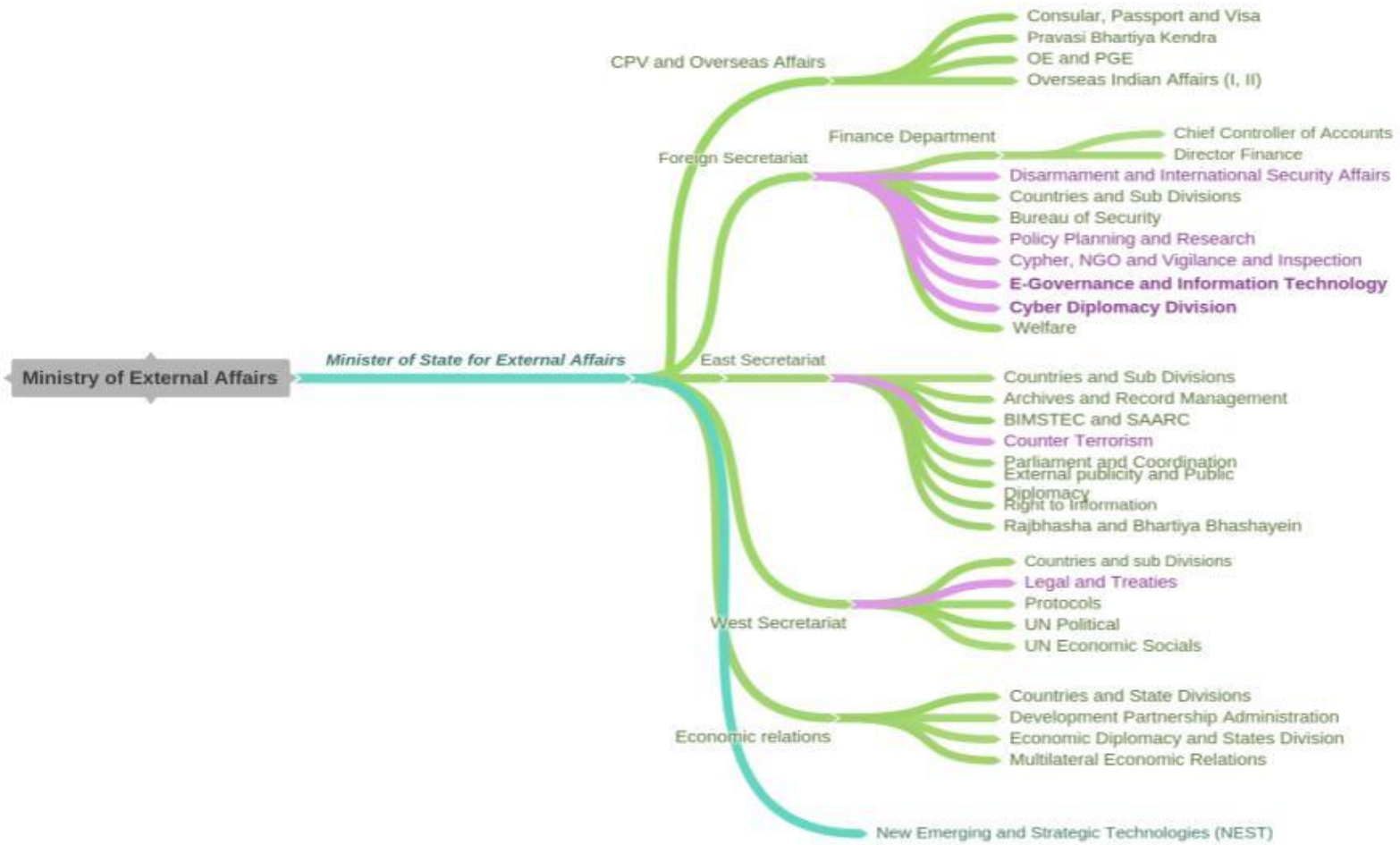
Ministry of Communications



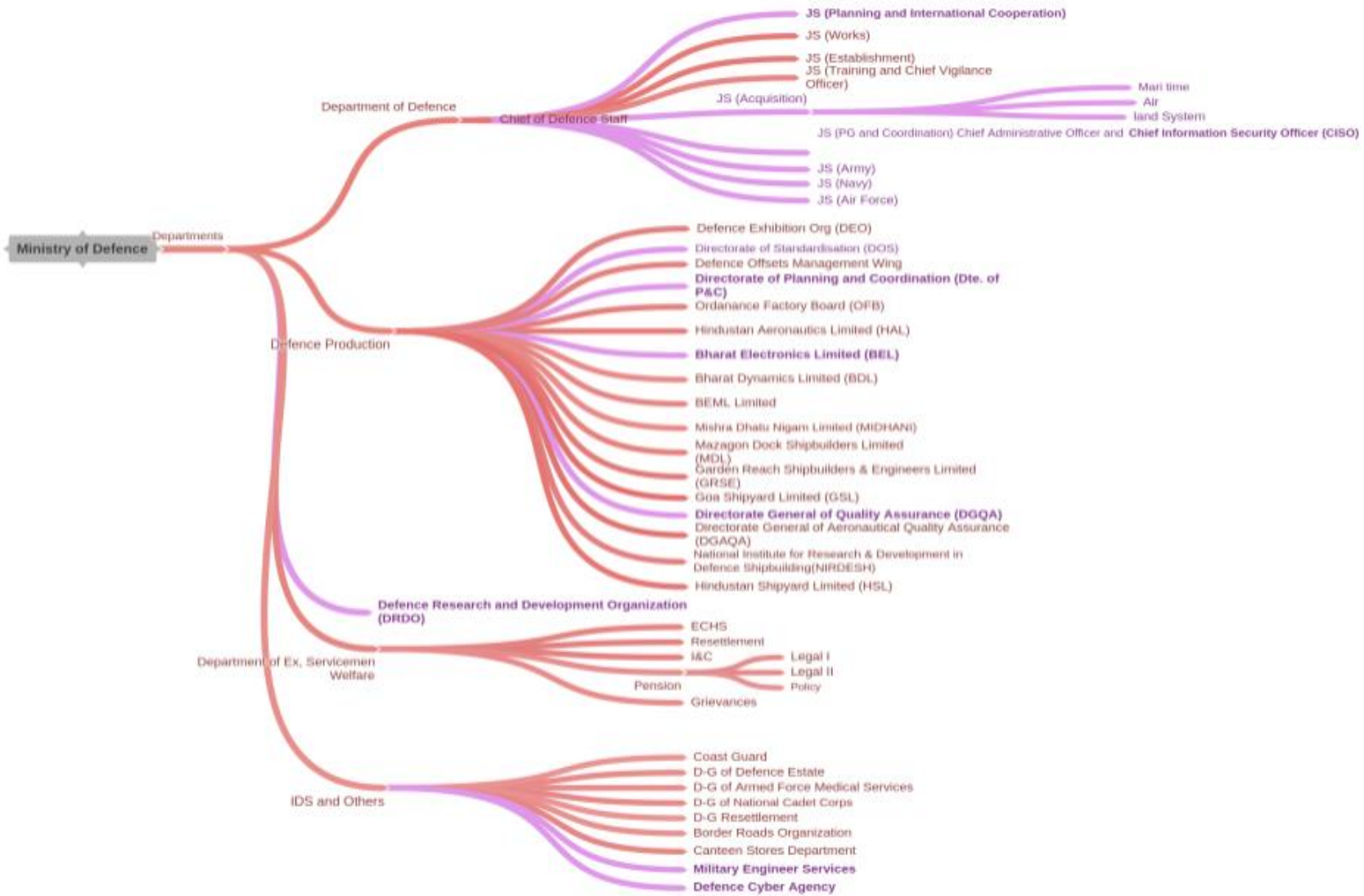
Ministry of Electronics and IT



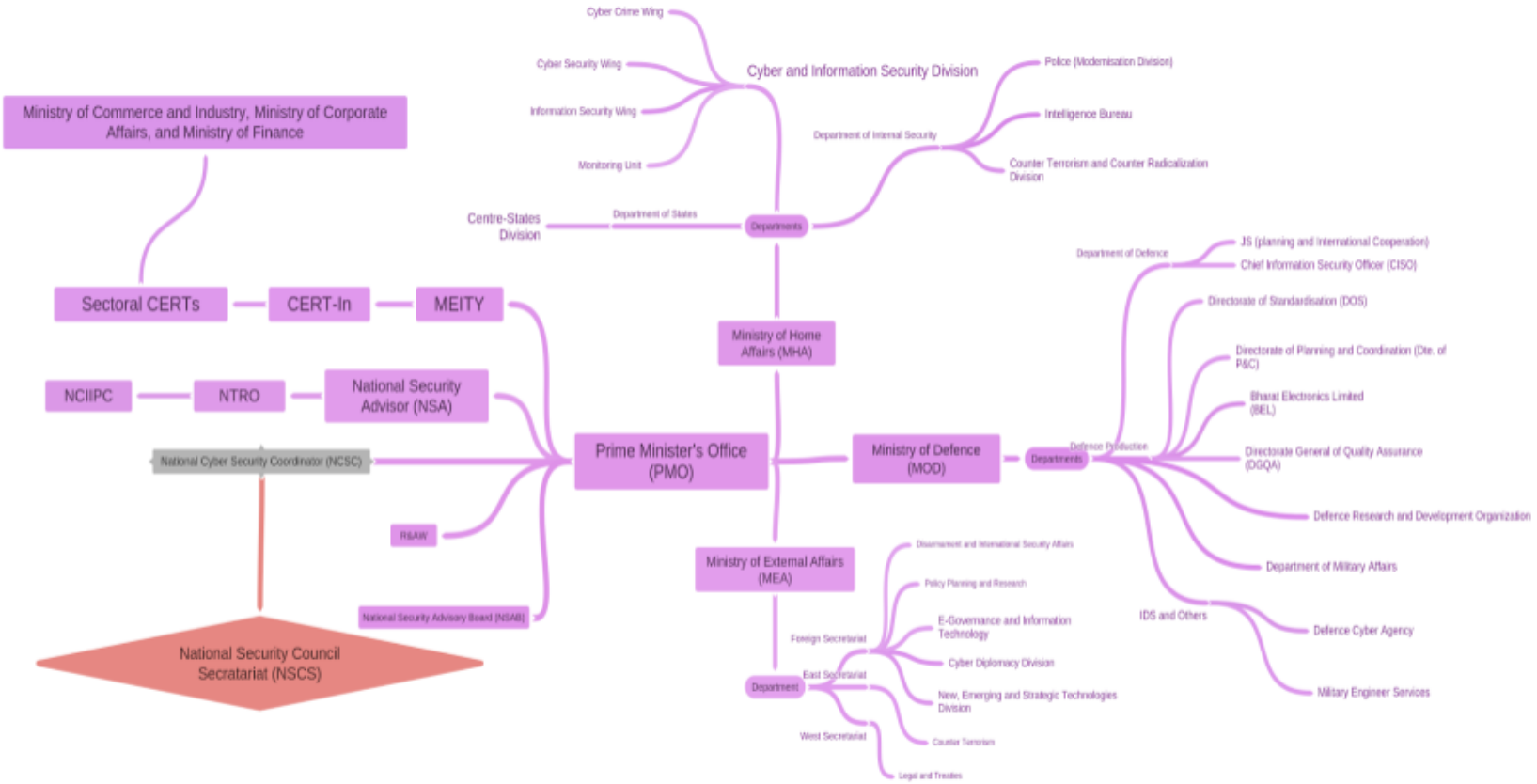
Ministry of External Affairs



Ministry of Defence



Composite Architecture of Relevant Departments and Ministries



Annexure 'C'
Note on Research Methodology for Union Budget Data Analysis

We have compiled the data on budgetary allocations (budget and revised) and actual expenditure from the Demands for Grants of Ministries as approved by Parliament and presented in the Annual Expenditure Budget of several ministries and their respective departments which are related to cybersecurity from the FY 2013-14 to FY 2019-20.

The departments have identified from publicly available information represented in the organograms presented as Annexure 'B'. We understand a 'relevant department' to mean those departments which are either directly related to cybersecurity and/or support the functioning of the security aspects of internet governance at large.

We have then identified those budget heads under the Union Budgets for FY 2013-14 through FY 2019-2020, which correspond most closely to the departments identified and highlighted in Annexure 'B' to calculate the total allocation to ministries for cybersecurity-related activities.

We then analyse this data in under four broad categories.

I. **Department Wise Allocation:** The departments that are directly related to the expenditure for cybersecurity are calculated under this heading. Various expenditures under Ministry of Electronics and Information Technology (MEITY), Department of Telecommunication (DoT), and Ministry of Home Affairs are tabulated for this.

   Under **MeitY**, we looked have included the budget heads for

   1. Computer Emergency Response Team (CERT-IN),
   2. Centre for Development of Advanced Computing (C-DAC),
   3. Centre for Materials for Electronics and IT (C-MET),
   4. Society for Applied Microwave Electronics Engineering and Research (SAMEER),
   5. Standardization Testing and Quality Certification (STQC),
   6. Controller of Certifying Authorities (CCA), and
   7. Foreign Trade and Export Promotion and
   8. Certain components of the Digital India Initiative, namely:
      a. Manpower Development,
      b. National Knowledge Network,
      c. Promotion of electronics and IT HW manufacturing,

d. Cybersecurity projects (which includes National Cyber Coordination centre and others),
e. Research and Development in Electronics/IT, Promotion of IT/ITeS industries,
f. Promotion of Digital Payment, and Pradhan Mantri Digital Saksharta Abhiyan (PMGDISHA).

Under **Ministry of Communication,** our focus was only on the Department of Telecommunication. We considered the budget allocated to the following, to come up with the total Department budget. These heads are –

1. Telecom Regulatory Authority of India (TRAI),
2. Human Resource Management under National Institute of Communication Finance,
3. Wireless Planning and Coordination, Telecom Engineering Centre,
4. Technology Development and Investment Promotion,
5. South Asia Sub-Regional Economic Cooperation (SASEC) under Information Highway Project,
6. Telecom Testing and Security Certification Centre,
7. Telecom Computer Emergency Response Team,
8. Central Equipments Identity Register (CEIR),
9. 5G Connectivity Test Bed,
10. Promotion of Innovation and Incubation of Future Technologies for Telecom Sector,
11. Centre for Development of Telematics (C-DoT), and
12. Labour, Employment and Skill Development.

Under **Ministry of Home Affairs,** the funds allocated for the following budget heads have been included:

1. Education, Training and Research purposes,
2. Criminology and Forensic Science,
3. Modernisation of Police Forces and Crime and Criminal Tracking Network and Systems (CCTNS),
4. Indian Cyber Crime Coordination Centre, and
5. Technical and Economic Cooperation with Other Countries.

All these budget heads were tabulated to come up with the total for department wise allocation. Along with departments mentioned under 'Supporting Departments', all these departments were again classified on the basis of their functions and activities, and analysed under (III).

II. **Supporting Department Wise Allocation:** While certain expenditures of the Ministry of Defence, Ministry of External Affairs, Department of Telecommunication, and Ministry of Home Affairs can potentially be used for cybersecurity-related activities, but it it is not possible to infer from the Demands for Grants, the share of cyber in the total allocation, we have treated them as 'allocations to supporting departments'. In this data, the total funds indicated may not be directly related to cybersecurity efforts, but they contribute towards the larger security and governance framework, which enables the creation of a secure ecosystem for cyber. These headings are tabulated under this section.

Under **Ministry of Defence,** the following heads were considered to contribute towards the larger security and governance framework in cyberspace:

1. Navy/Joint Staff,
2. Ordnance Factories R&D,
3. Research and Development, including the Research and Development component of R&D head,
4. Capital Outlay on R&D, and
5. Technology Development and Assistance for Prototype Development under Make Procedure.

Under **Ministry of External Affairs,** we considered the following heads as important contributors –

1. The Special Diplomatic Expenditure,
2. Expenditure for International Cooperation,
3. Expenditure for Technical and Economic Cooperation with other Countries, and
4. Other Expenditure of Ministry.

Under **Department of Telecommunication** again, there were several heads that we considered not to be directly related to cybersecurity, but they did significantly contribute towards it. These include allocations for

1. Defence Spectrum,
2. Capital Outlay on Telecommunication and Electronic Industries,
3. Capital Outlay on Other Communication Services, and
4. Universal Service Obligation Fund (USOF).

Under **Ministry of Home Affairs,** the departments that are involved with defence and intelligence along with law enforcement are important to be considered for cybersecurity. Thus we included the allocations for

1. Intelligence Bureau,

2. NATGRID,
3. Delhi Police, and
4. Capital Outlay on Police.

II. **Activity Wise Allocation:** For further analysis, we have categorized the expenditures mentioned in Department Wise Allocation into five categories, each of which have been identified as constituent elements of the three Pillars of Strategy namely -

1. Human Resource Development Component (Strengthen)
2. Technical Research & Development Component, Capacity Building (Strengthen/Synergize)
3. International Cooperation and Investment Promotion Component (Secure/Synergise)
4. Standardization, Quality Testing and Certification Component (Strengthen)
5. Active Cyber Incident Response/ Defence Operations and Security Component (Secure/Strengthen)

The total for these are calculated to identify if any trends or patterns emerge in expenditure by the ministries. Apart from the ministries covered in classifications (I) and (II), we have also included budgets of two other heads/departments. Namely, these are (i) the allocation towards corporate data management under the authority of the Ministry of Corporate Affairs, which has been included in category (5) indicated above and (ii) the allocation towards technical and economic cooperation with other countries for the Department of Economic Affairs under the Ministry of Finance, which has been included in category (3) indicated above.

III. **Ministries share over Financial Year:** The total value tabulated in Department wise allocation and supporting department wise allocation for the ministries is then used to calculate the share of budget allocated to Cyber Security and related activities with respect to the total budget allocation of ministries. The ministries taken into account, which contribute significantly to Cyber Security and related activities are

1. Department of Telecommunication (under the Ministry of Communications),
2. Ministry of Defence,
3. Ministry of External Affairs,
4. Ministry of Electronics and Information Technology,
5. Ministry of Home Affairs, and
6. Department of Science and Technology (under the Ministry of Science and Technology).