A WORKING PAPER: THE CYBERSECURITY BUDGET BRIEF

January 2023

Centre for Communication Governance at National Law University Delhi

Published by
Centre for Communication Governance, NLUD

Patron: Professor (Dr.) Harpreet Kaur Vice Chancellor (I/c), NLUD
Faculty Advisor, CCG: Dr. Daniel Mathew
Executive Director, CCG: Jhalak M. Kakkar

Authored by Gunjan Chawla, Ananya Moncourt and Vagisha Srivastava

Reviewed and edited by Jhalak Kakkar, Sachin Dhawan and Sidharth Deb

Research Input by Sukanya Thapliyal, Tavishi Alhuwalia, Sharngan Aravindakshan and Rakesh Roshan

We thank Maansi Verma (*Maadhyam*) and Arun Sudarsan (*Civic Data Labs*) for their feedback on this paper

Suggested Citation: Gunjan Chawla, Ananya Moncourt and Vagisha Srivastava, Working Paper: *The Cybersecurity Budget Brief,* Centre for Communication Governance, National Law University Delhi_ January 2023.

(CC BY-NC-SA 4.0)

About the National Law University Delhi (NLUD)

The National Law University Delhi is one of the leading law universities in the capital city of India. Established in 2008 (by Act. No. 1 of 2009), the University is ranked second in the National Institutional Ranking Framework for the last five years. Dynamic in vision and robust in commitment, the University has shown terrific promise to become a world-class institution in a very short span of time. It follows a mandate to transform and redefine the process of legal education. The primary mission of the University is to create lawyers who will be professionally competent, technically sound and socially relevant, and will not only enter the Bar and the Bench but also be equipped to address the imperatives of the new millennium and uphold the constitutional values. The University aims to evolve and impart comprehensive and interdisciplinary legal education which will promote legal and ethical values, while fostering the rule of law. The University offers a five year integrated B.A., LL.B (Hons.) and one-year postgraduate masters in law (LL.M), along with professional programs, diploma and certificate courses for both lawyers and non-lawyers. The University has made tremendous contributions to public discourse on law through pedagogy and research. Over the last decade, the University has established many specialised research centres and this includes the Centre for Communication Governance (CCG), Centre for Innovation, Intellectual Property and Competition, Centre for Corporate Law and Governance, Centre for Criminology and Victimology, and Project 39A. The University has made submissions, recommendations, and worked in advisory/consultant capacities with government entities, universities in India and abroad, think tanks, private sector organisations, and international organisations. The University works in collaboration with other international universities on various projects and has established MoU's with several other academic institutions.

About the Centre for Communication Governance (CCG)

The Centre for Communication Governance at the National Law University Delhi (CCG) was established in 2013 to ensure that Indian legal education establishments engage more meaningfully with information technology law and policy and contribute to improved governance and policy making. CCG is the only academic research centre dedicated to undertaking rigorous academic research in India on information technology law and policy in India and in a short span of time has become a leading institution in Asia. Through its academic and policy research, CCG engages meaningfully with policy making in India by participating in public consultations, contributing to parliamentary committees and other consultation groups, and holding seminars, courses and workshops for capacity building of different stakeholders in the technology law and policy domain.

CCG has built an extensive network and works with a range of international academic institutions and policy organisations. These include the United Nations Development Programme, Law Commission of India, NITI Aayog, various Indian government ministries and regulators, International Telecommunications Union, UNGA WSIS, Paris Call, Berkman Klein Center for Internet and Society at Harvard University, the Center for Internet and Society at Stanford University, Columbia University's Global Freedom of Expression and Information Jurisprudence Project, the Hans Bredow Institute at the University of Hamburg, the Programme in Comparative Media Law and Policy at the University of Oxford, the Annenberg School for Communication at the University of Pennsylvania, the Singapore Management University's Centre for AI and Data Governance, and the Tech Policy Design Centre at the Australian National University.

The Centre has had multiple publications over the years including the Hate Speech Report, a book on Privacy and the Indian Supreme Court, and most recently an essay series on Democracy in the Shadow of Big and Emerging Tech. The Centre has launched freely accessible online databases - Privacy Law Library (PLL) and High

Court Tracker (HCT) to track privacy jurisprudence across the country and the globe in order to help researchers and other interested stakeholders learn more about privacy regulation and case law. CCG also has an online 'Teaching and Learning Resource' database for sharing research-oriented reading references on information technology law and policy. In recent times, the Centre has also offered courses on AI Law and Policy, Technology and Policy, and first principles of cybersecurity. These databases and courses are designed to help students, professionals, and academicians build capacity and ensure their nuanced engagement with the dynamic space of existing and emerging technology and cyberspace, their implications for the society, and their regulation. Additionally, CCG organises an annual International Summer School in collaboration with the Hans Bredow Institute and the Faculty of Law at the University of Hamburg in collaboration with the UNESCO Chair on Freedom of Communication at the University of Hamburg, Institute for Technology and Society of Rio de Janeiro (ITS Rio) and the Global Network of Internet and Society Research on contemporary issues of information law and policy.

Table of Contents

Executive Summary

The Cybersecurity Budget Brief provides a detailed overview of trends in cybersecurity budgeting, from publicly available data in the Union Budget, from financial year 2012-13 to 2022-23. As a guide to cybersecurity budgeting for parliamentarians and policy researchers, this brief covers basic concepts on cybersecurity and presents findings from an analysis of budget data to inform debates in the upcoming 2023 Budget Session of Parliament, as well as serve as a foundation for future analysis. With the increasing relevance of cybersecurity in both domestic and international contexts, this brief reflects on past trends to enable informed discussions for future fiscal and policy decisions on cybersecurity in India.

Part I introduces the components of cybersecurity and its relevance in today's digital landscape. Our increasing dependence on Information and Communications Technologies (ICT's) for economic activities and governance runs parallel to increasingly sophisticated cyberattacks and evolving threats that call for renewed emphasis on cybersecurity practices. As such, all relevant government ministries and departments that are currently driving cybersecurity policies and programmes in India are presented to advance a whole-of-government approach to cybersecurity.

Part II delves into the importance of budgeting for, and tracking the allocated and actual expenditures undertaken by the central government for cybersecurity and provides an introduction to the research methodology and analytical framework developed by the Centre for Communication Governance (CCG) to analyse budgeting and expenditure on cybersecurity. An overview of the trends in cybersecurity budgeting over the last ten financial years (FY 2012-13 to FY 2022-23) is also presented.

In Part III, we present trends in budgeted, revised and actual expenditures towards departments and schemes relevant for cybersecurity and identify discrete budget heads that are significant in this regard under the Ministry of Electronics and Information Technology (MeitY), Ministry of Home Affairs (MHA), Department of

Telecommunication (DoT) and other relevant departments.[1] A total of 47 budget heads have been examined in this analysis. Under the three ministries examined in this brief, four additional budget heads were introduced in the Union Budget 2022, and although relevant to cybersecurity generally, have not been included in this iteration of the report in order to maintain consistency in the budget heads being tracked. These are, namely, allocations under the Production Linked Incentive scheme to Ministry of Electronics and Information Technology and Department of Telecommunications, the Digital Intelligence Unit under Department of Telecommunications and Modernisation of Forensic Capabilities under Ministry of Home Affairs.

Part IV presents findings from analysis of a framework developed by CCG to track budgeting for cybersecurity. Budget heads under those government ministries that are relevant for cybersecurity are classified under six activities: (1) Cyber Incident Preparedness and Response (2) Technical Research and Capacity Development (3) Human Resource Development (4) International Cooperation and Investment Promotion (5) Standardisation, Testing and Quality Certification and (6) Digital Identity. Each of these activities form pillars of development for the country's cybersecurity resilience and this framework provides a systematic approach to assess the quantum of financial resources directed towards them over the last decade.

In conclusion, Part V presents the following key findings from our analysis:

- First, there have been overall positive increasing allocations towards cybersecurity in the Union Budget over the last decade. Since FY 2012-13 there has been a Compound Annual Growth Rate (CAGR) of 8.1% in the budgeted expenditure for cybersecurity over eleven years, from ₹6,612 crores in FY 2012-13 to ₹15,575 crores in FY 2022-23. Yet, variations in the exact quantum of resources being directed towards cybersecurity exist due to the lack of a

[1] Throughout this brief, 'other relevant departments' refers to four budget heads from different government ministries that are relevant for cybersecurity. These include, (1) Technical and Economic Co-operation with Other Countries under the Ministry of Finance's Department of Economic Affairs (2) UIDAI under MeitY (3) National Mission on Interdisciplinary Cyber Physical Systems under the Department of Science and Technology and (4) Corporate Data Management under the Ministry of Corporate Affairs

standardised framework and identified metrics that enable tracking of the cybersecurity budget.

- Second, approximately 0.1% of the total government budget has been dedicated to budgeted expenditures for cybersecurity annually since FY 2012-13. We observe fluctuating trendlines in budgeted expenditures (BE) across ministries through the years. Nevertheless, we observe that underutilisation of the cumulative cybersecurity budget in the earlier years diminishes and in FY 2018-19, actual spending exceeds the allocated budget. Consistent positive increases in budgeted allocations for cybersecurity post FY 2017-18 are also evident. There is an 8% decrease in FY 2019-20 and a 7% increase in FY 2020-21, in total actual expenditures for cybersecurity.

- Third, despite inconsistencies and underutilisation of allocations, the introduction of specialised programs such as the Digital India scheme under MeitY and Cyber Crime Prevention against Women and Children under MHA spur allocations towards cybersecurity. Budget heads under each ministry that have received consistent and/ or increasing allocations make it possible to identify key priorities for cybersecurity budgeting.

- Fourth, 'Technical Research and Capacity Development' and 'Cyber Incident Preparedness and Response' have received most importance via consistent and/or increasing allocations across ministries. Relatively, 'Human Resource Development' has been a low priority area and renewed attention can increase technical capacity that is currently lacking.[2]

[2] "The Curious Case of India's Cybersecurity Skills Gap and Prevailing Opportunities" (*Dataquest)* April 23, 2020 <https://www.dqindia.com/the-curious-case-of-indias-cybersecurity-skills-gap-and-prevailing-opportunities/>
"Cybersecurity Skill Demand in India Triples in Last One Year" (*CISO MAG | Cyber Security Magazine)* June 19, 2018 https://cisomag.eccouncil.org/cybersecurity-skill-demand-india-triples-last-one-year/
Singh A, "Amid Rising Cyber Security Threats, Indian Firms Facing Shortage of Skilled Professionals" (*The Week)* June 16, 2021 <https://www.theweek.in/news/biz-tech/2021/06/16/amid-rising-cyber-security-threats-indian-firms-facing-shortage-of-skilled-professionals.html>

- Finally, we note that gaps in the publicly available data, that tracks utilisation of allocations, limits and skews analysis for cybersecurity budgeting. Incomplete datasets further blur the lines between cases of underutilisation of funds and challenges of presentation of data in the Union Budget.

The Cybersecurity Budget Brief presents trends in cybersecurity expenditures over the last decade and highlights various aspects about the landscape of cybersecurity for parliamentarians to consider and debate. It also offers avenues for further research and analysis on cybersecurity, towards the growth and development of a secure and resilient cyber ecosystem in India.

Limitations of Analysis in the Cybersecurity Budget Brief

1. Expenditure figures in this brief are estimations of the total cybersecurity budget that are indicative of the entire pool of resources available for cybersecurity. These figures must be viewed as the pool of financial resources available to government to strengthen the state of cyber security and various aspects of internet governance related thereto at the national level, including the security of e-governance initiatives to facilitate the online delivery of public services to citizens, and not actual direct spending on cybersecurity. This is due to the fact that entire budgeted allocations for all the programmes and schemes in our analysis are not utilised exclusively for cybersecurity and its related activities. The current format of the Demands for Grants does not allow for inference of the precise share of budgeted allocations that are actually used for activities directly related to cybersecurity. All budget heads included in our analysis therefore fall on a spectrum of high significance to low significance with respect to percentage share of their budgeted allocations being utilised for cybersecurity. For certain budget heads, it is likely that a greater share of the allocation is directed towards cybersecurity related activities. For example, it is likely that for Cybersecurity projects under the Digital India scheme and CERT-In, both under the Ministry of Electronics and Information Technology, the entire allocation is directly relevant for cybersecurity. On the other hand, for budget heads

such as the Prime Minister's Office under Ministry of Home Affairs, only a specific percentage of the total allocated budget is likely to be directed towards cybersecurity activities. However, there exist no relevant mechanisms to establish what percentage of these allocations can be taken as relevant for cybersecurity activities, and thus the entire allocation has been included for such budget heads in our analysis.

2. This analysis does not include certain ministries that are of relevance to cybersecurity. There are budget heads under the Ministry of Defense, Ministry of External Affairs, Department of Telecommunication and Ministry of Home Affairs that can possibly be utilised for cybersecurity-related activities. However, their expenditure values are at best an estimate of the total funds available which may be utilised for cybersecurity-related functions. It is not possible to infer from the current format of the Demands for Grants the precise share of these allocations that are actually used for activities directly related to cybersecurity. While it is important to highlight these areas of potential for cybersecurity – as supporting allocations – including them in our analysis would inflate allocations for cybersecurity and skew findings.

3. Incomplete expenditure data under certain ministries' Demand for Grants limits the scope and applicability of the analysis in this brief. There are instances of unavailable expenditure data for budget heads under the Ministry of Electronics and Information Technology and the Department of Telecommunications over the last decade. In some cases, budget heads have allocated expenditures but data on revised and actual expenditures remains unavailable without articulations of the reasons for such gaps. Incomplete budget datasets limit the veracity of analysis due to the ambiguity between cases of underutilisation of funds and bottlenecks in presentation of data in the Union Budget.

4. Four new budget heads that were introduced in the Union Budget 2022 have not been included in our analysis. These have been identified under their relevant ministries and include, (1) Production Linked Incentive (PLI) for Large Scale Electronics and IT Hardware under Ministry of Electronics and Information

Technology (2) Digital Intelligence Unit Project under Department of Telecommunications (3) Production Linked Incentive (PLI) Scheme to Promote Telecom and Networking Products under Department of Telecommunications and (4) Modernisation of Forensic Capacities under Ministry of Home Affairs. These budget heads have not been included in our analysis of trends in Part III and Part IV in order to maintain consistency in budget heads tracked over the last decade. However, any future analysis of India's cybersecurity budget should include these budget heads as well, subject to continued allocations towards the same.

VOLUME - I

What is CCG's Cybersecurity Budget Brief?

CCG's Cybersecurity Budget Brief ("the Brief") is a unique resource that compiles analysis of publicly available information on the Government of India's ("GoI") allocated and actual expenditure of public funds on cybersecurity and related activities through its various departments and ministries.

The Brief aims to provide a useful, comprehensive and user-friendly framework to set the context for cybersecurity budgeting by providing a glimpse of trends and priorities for cybersecurity budgeting, and enable policy-makers to engage critically with the topic. It provides an original analytical framework to assess the GoI's Union Budget with a view to identifying and analysing government expenditure that contributes to enhanced cybersecurity at the national level.

In CCG's Comments on the National Cyber Security Strategy 2020-2025 submitted to the National Security Council Secretariat in January 2019, CCG argued for the need to think strategically about the state of India's cybersecurity.

> *"...strategic thinking demands that we bear in mind internal and external constraints operating to restrict our security choices, and make efforts to economise and encourage the judicious use of available resources and actively guard against cybersecurity becoming a bottomless pit for public funds and resources being used inefficiently to produce uncertain outcomes".*[3]

Such a strategic approach can be strengthened by an understanding of trends in financial resources that are made available and utilised for cybersecurity over time, in

[3] Gunjan Chawla, SharnganAravindakshan and Vagisha Srivastava, CCG's Comments to the National Security Council Secretariat on the National Cyber Security Strategy 2020, Centre for communication Governance at National Law University Delhi, 10 January 2019, at pp, iii-iv <https://ccgdelhi.org/wp-content/uploads/2020/03/CCG-NLU-Comments-to-the-National-Security-Council-Secretariat-on-NCSS-2020.pdf>

terms of the budgeted allocations for cybersecurity by the government. This Brief is an updated version of an earlier piece published by CCG,[4] in a modest attempt to document and measure the quantum of funds available for, and dedicated to the enhancement of the state of India's cybersecurity. It is intended as a guiding resource to track and inform debates on budgetary allocations towards cybersecurity related activities undertaken by the Government of India.

Who should read CCG's Cybersecurity Budget Brief?

This document is designed for use as a ready reference by policy makers and policy researchers interested in cybersecurity policy. The Brief intends to inform, enable and support discussions on crucial questions that are relevant to assess the state of cybersecurity in India. This includes matters regarding public funds dedicated to investments and expenditure incurred in building and maintaining India's cyber infrastructure, capabilities as well as governance structures and processes.

We present this framework and analysis for policymakers to highlight the need for cybersecurity budget analysis, and to aid the debate around cybersecurity in the Parliament in the Budget Session 2023. There is a need to allocate funding and other public resources towards strengthening India's cybersecurity. We hope that this analysis will help bring this discussion, of tracking India's cybersecurity budgeting in a structured manner, into focus for lawmakers and policy researchers.

We welcome comments, suggestions and proposals for further research in this domain from institutions engaged in academic research, public policy think tanks as well as other organisations engaged in the management or monitoring of public funds. The

[4] Gunjan Chawla, Sharngan Aravindakshan, Vagisha Srivastava, 'India's Cybersecurity Budget FY 2013-14 to FY 2020-21: Analysis of Budgetary Allocations for Cybersecurity and Related Activities',30 January 2020,<https://ccgnludelhi.wordpress.com/2020/01/30/indias-cybersecurity-budget-analysis-of-budgetary-allocations-for-cybersecurity-and-related-activities-fy-2013-14-to-fy-2019-20/>

original dataset which forms the basis of our analyses will be made available to interested persons and/or organisations on request.[5]

Purpose, Scope and Structure

The analyses presented in this Brief are aimed at formulating and raising pertinent questions about efforts undertaken at the national level to improve the state of India's cybersecurity as well as about financial resources allocated to departments and programmes geared towards achieving this objective.

Our analysis draws on insights from '*CCG's Cybersecurity Budget Dataset*', which has been created using publicly available data on Union Budgets from FY 2012-13 to FY 2022-23. The release of India's first National Cyber Security Policy in 2013 forms an important marker for tracking the commencement of cybersecurity budgeting in the country.

Even though the allocation of financial, technical and human resources from the private sector are an important component that will determine India's national posturing on cybersecurity and related issues, the quantum of resources made available in and through the private sector are beyond the scope of this analysis.[6]

This Brief is presented in two volumes.

Volume I is divided into five main parts – Part I provides a brief introduction to the meaning and importance of cyber security. It seeks to support Parliamentarians as policy makers engage with this issue. Part II delves into the importance of budgeting for, and tracking the allocated and actual expenditures undertaken by the Central

[5] Requests may be directed to ccg@nludelhi.ac.in
[6] For researchers interested in tracking the private sector, NASSCOM-DSCI's report on India Cybersecurity Services Landscape: A Global Hub in the Making published on 21 May 2020 may be a useful (paywalled) resource, available at https://www.dsci.in/content/India-Cybersecurity-Services-Landscape.

Government towards cybersecurity. It provides a brief introduction to the research methodology and analytical framework developed by CCG to analyse trends in cybersecurity budgeting over the last decade. Part III and IV present the trends from our data analysis and Part V offers certain conclusions and insights by identifying (a) issues that would be useful for Parliament to consider and (b) avenues for further research and analysis.

Volume II provides a detailed exposition of (1) the relevance of each budget head examined to cybersecurity at large (2) the methodology of data collection and classification adopted to develop the analysis in Volume I, (3) the methodology for data analysis, and (4) interpretation guidance for readers.

Limitations of Analysis in the Cybersecurity Budget Brief

1. Expenditure figures in this brief are estimations of the total cybersecurity budget that are indicative of the entire pool of resources available for cybersecurity. These figures must be viewed as the pool of financial resources available to government to strengthen the state of cyber security and various aspects of internet governance related thereto at the national level, including the security of e-governance initiatives to facilitate the online delivery of public services to citizens, and not actual direct spending on cybersecurity. This is due to the fact that entire budgeted allocations for all the programmes and schemes in our analysis are not utilised exclusively for cybersecurity and its related activities. The current format of the Demands for Grants does not allow for inference of the precise share of budgeted allocations that are actually used for activities directly related to cybersecurity. All budget heads included in our analysis therefore fall on a spectrum of high significance to low significance with respect to percentage share of their budgeted allocations being utilised for cybersecurity. For certain budget heads, it is likely that a greater share of the allocation is directed towards cybersecurity related activities. For example, it is likely that for Cybersecurity projects under the Digital India scheme and CERT-In, both under the Ministry of Electronics and Information Technology, the entire allocation is directly

relevant for cybersecurity. On the other hand, for budget heads such as the Prime Minister's Office under Ministry of Home Affairs, only a specific percentage of the total allocated budget is likely to be directed towards cybersecurity activities. However, there exist no relevant mechanisms to establish what percentage of these allocations can be taken as relevant for cybersecurity activities, and thus the entire allocation has been included for such budget heads in our analysis.

2. This analysis does not include certain ministries that are of relevance to cybersecurity. There are budget heads under the Ministry of Defense, Ministry of External Affairs, Department of Telecommunication and Ministry of Home Affairs that can possibly be utilised for cybersecurity-related activities. However, their expenditure values are at best an estimate of the total funds available which may be utilised for cybersecurity-related functions. It is not possible to infer from the current format of the Demands for Grants the precise share of these allocations that are actually used for activities directly related to cybersecurity. While it is important to highlight these areas of potential for cybersecurity – as supporting allocations – including them in our analysis would inflate allocations for cybersecurity and skew findings.

3. Incomplete expenditure data under certain ministries' Demand for Grants limits the scope and applicability of the analysis in this brief. There are instances of unavailable expenditure data for budget heads under the Ministry of Electronics and Information Technology and the Department of Telecommunications over the last decade. In some cases, budget heads have allocated expenditures but data on revised and actual expenditures remains unavailable without articulations of the reasons for such gaps. Incomplete budget datasets limit the veracity of analysis due to the ambiguity between cases of underutilisation of funds and bottlenecks in presentation of data in the Union Budget.

4. Four new budget heads that were introduced in the Union Budget FY 2022-23 have not been included in our analysis. These have been identified under their relevant

ministries and include, (1) Production Linked Incentive (PLI) for Large Scale Electronics and IT Hardware under Ministry of Electronics and Information Technology (2) Digital Intelligence Unit Project under Department of Telecommunications (3) Production Linked Incentive (PLI) Scheme to Promote Telecom and Networking Products under Department of Telecommunications and (4) Modernisation of Forensic Capacities under Ministry of Home Affairs. These budget heads have not been included in our analysis of trends in Part III and Part IV in order to maintain consistency in budget heads tracked over the last decade. However, any future analysis of India's cybersecurity budget should include these budget heads as well, subject to continued allocations towards the same.

PART I: Introduction

What is cybersecurity?

According to the Information Technology Act, 2000 'cyber security' means '*protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification and destruction*'.[7] According to the Ministry of Electronics and Information Technology (MeitY), this activity can be viewed as one component of the broader field of internet governance.[8] 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. the internet protocols such as TCP/IP protocol) and (3) the content layer (e.g. websites, posts on social media, etc.).[9]

Indeed, cyberspace is a complex environment consisting of interactions between people, software and services supported by the worldwide distribution of information and communication technology (ICT) devices and networks.[10] Moreover, the challenges of cybersecurity encompass multiple governance, policy, operational, technical and legal aspects.[11] For instance, mere acquisition of cybersecurity products like, say, firewalls would not ensure cybersecurity in the absence of an enabling legal framework or skilled human resources to properly utilise the product. Similarly, the formulation of a cybersecurity policy without allocation of adequate resources to administer and execute actions required under said policy will not necessarily improve upon the status quo. To improve the state of cybersecurity in India — i.e., to protect

[7] Section 2(nb), Information Technology Act, 2000.
[8] Internet Governance and Proliferation (Ministry of Electronics and Information Technology)< https://meity.gov.in/content/internet-proliferation-governance>
[9] Ibid,
[10] National Cybersecurity Policy 2013, para. 1, <https://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf>
[11] Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity (International Telecommunication Union, 2018)< https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf>

computer resources from unauthorised access, use, disruption, etc. — people, processes and technologies need to be deployed in tandem with each other.

Accordingly, a 2018 notification by the Ministry of Electronics and Information Technology[12] defines 'cybersecurity products' as — *a product or appliance or software manufactured/produced for the purpose of protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction*. Such products (and services) may cater to one or more components of cyber security at large.

These components include, but are not limited to:

1. **Network security:** Protecting computer networks from intrusion and malwares, including remote access to endpoints such as organisations and individual systems.
2. **Application security:** Protecting end-user and middleware applications[13] from threats and attacks.
3. **Information security:** Protecting the integrity of data and privacy of users whether in storage or transit.
4. **Database and infrastructure security:** Protecting the databases and data centres are crucial for information security. Moreover, it is important to protect critical information infrastructure from attacks and security risks as well.
5. **Cloud security:** Cloud security is a part of information security which involves protecting data and interfaces in a completely online environment.
6. **End-point or mobile security:** Protecting cell phones and tablets includes all types of security challenges from the end-user perspective.

[12] Ministry of Electronics and Information Technology Notification No. 1(10)/2017-CLES dated 2nd July 2018.
[13] Middleware is software that provides common services and capabilities to applications outside of what's offered by the operating system. Data management, application services, messaging, authentication, and API management are all commonly handled by middleware. < https://www.redhat.com/en/topics/middleware/what-is-middleware#:~:text=Middleware%20is%20software%20that%20provides,all%20commonly%20handled%20by%20middleware>

7. **Disaster recovery:** Protecting the system not only from attacks, threats and hacking attempts but also from natural calamities is an important aspect of cybersecurity.
8. **End-user education:** This addresses the most unpredictable cybersecurity factor – the people. Digital literacy for end-users can reduce and prevent several cyber attacks.

Accordingly, a defence-in-depth approach to cybersecurity would be cognisant of, and would cater to each of the above-mentioned components. Defence-in-depth is an approach to cybersecurity in which a series of defensive mechanisms are thoughtfully layered throughout the computer network[14] in order to protect valuable data or information.[15] A layered approach to security can be applied to all levels of IT systems,[16] to slow down the advance of attempts by bad actors to acquire access to unauthorised information. As such, each layer offers protection and if one layer of security is breached, a subsequent layer is in place to mitigate threats. While no individual mitigation can stop all cyber threats, together they provide mitigations against a wide variety of threats while incorporating redundancy in the event one mechanism fails.[17] Such an approach can be represented as depicted in Figure 1.

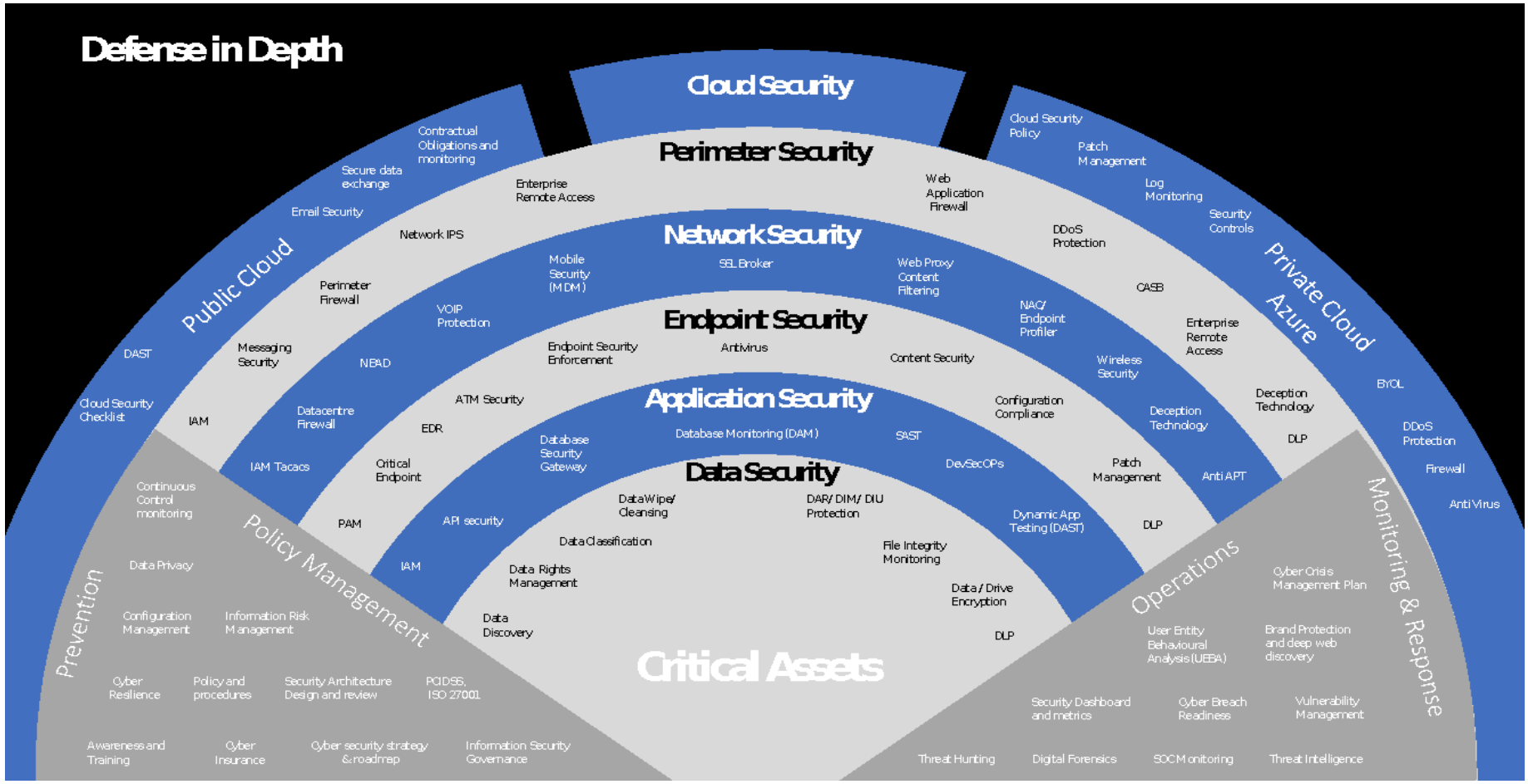
[14] Centre for Internet Security, Cybersecurity Spotlight – Defense-in-Depth, https://www.cisecurity.org/spotlight/cybersecurity-spotlight-defense-in-depth-did/#:~:text=Defense%20in%20Depth%20(DiD)%20refers,network%20and%20the%20data%20within

[15] What is Defense in Depth?, Forcepoint, <https://www.forcepoint.com/cyber-edu/defense-depth>.

[16] Ibid.

[17] Centre for Internet Security, Cybersecurity Spotlight – Defense-in-Depth, https://www.cisecurity.org/spotlight/cybersecurity-spotlight-defense-in-depth-did/#:~:text=Defense%20in%20Depth%20(DiD)%20refers,network%20and%20the%20data%20within

***Figure 1: Defence-in-Depth*[18]**



[18] Pritam Hazarika, Presentation on Cybersecurity Technologies at the Cybersecurity Training-cum-certificate course organized by the Confederation of Indian Industry-Tata Communications Centre for Digital Transformation Cybersecurity (CII-CDT) on 13 March 2020. Image reproduced with permission of the presenter.

Why is cybersecurity important?

Cyberspace has shaped up to be a critical strategic sector and therefore, cybersecurity has a significant impact on national security choices for the country. Owing to the growth of the digital economy and development dependence of governments on digital technologies, as e-governance and social welfare programmes migrate online in Digital India, the state of our cybersecurity must be attentively monitored. Its importance will only increase as the emphasis on 5G, IoT, AI and smart cities/urbanisation increases. Government, military, corporate, financial, and medical organisations deal with massive amounts of data, which is often sensitive and personal. With the ever-increasing volume of data and an exponential growth in sophisticated cyberattacks, the negative consequences of failed security are immense, and not always foreseeable with absolute certainty.

Increasing dependence on digital technologies for private communications, businesses and industry as well as e-governance and civil society, demands greater public investments in the creation and maintenance of digital infrastructure. Investments in technological infrastructure, capabilities and processes to ensure the security of this cyber infrastructure and protecting the privacy of communications are crucial to operationalising good governance in the digital age. The increasing global connectivity and combined efforts towards Digital India also come with unintended consequences such as cyber insecurity. In the digital domain, such insecurity "*has the potential to strain economic growth and sustainable development, and hinder the full enjoyment of human rights and fundamental freedoms*".[19] There is thus a need to carefully plan towards building a more robust and resilient cyberspace by catering to the requirements of cybersecurity.

[19] 'Final Substantive Report of the UN Open Ended Working Group on developments in the field of information and telecommunications in the context of international security, 10 March 2021, at p.1 para 3, <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>.

Existing and Emerging Threats

In light of the pandemic which illustrated our increased reliance on digital technologies, there was a massive surge in cyber attacks globally[20] as well as in India. Table 1 below displays statistics as per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) on cyber security incidents.[21]

Table 1: Number of "Cybersecurity Incidents" since 2015

Year	Number of 'Cyber Security Incidents' Reported by CERT-IN
2015	49,455
2016	50,362
2017	53,117
2018	2,08,456
2019	3,94,499
2020	11,58,208
2021	14,02,809
2022*	6,74,021

Source: CERT-In Annual Reports
(*until June 2022)

These statistics can be contrasted with the findings of leading cybersecurity firm Kaspersky, which reports a significantly higher number of cyber attacks (3,60,00,000) being detected in India from January through November in 2020 alone.[22] While none

[20] Press Trust of India, "Cyber Attacks Surge amid Covid-Driven Digitalisation: World Economic Forum Study" (*NDTV.com*January 18, 2022) <https://www.ndtv.com/world-news/cyber-attacks-surge-amid-covid-driven-digitalisation-world-economic-forum-study-2715400>

[21] Government of India, Ministry of Electronics and Information Technology, Response to Lok Sabha Unstarred Question no. 1782, answered on 21.09.2020, accessible at < http://164.100.24.220/loksabhaquestions/annex/174/AU1782.pdf>.
Government of India, Ministry of Electronics and Information Technology, Response to Lok Sabha Unstarred Question no. 541, answered on 20.07.2022, accessible at <http://164.100.24.220/loksabhaquestions/annex/179/AU541.pdf>.

[22] Hackers Continue Targeting remote Employees in India, 36mn attacks reported till Nov, The Hindustan Times, 20 December 2020, <https://tech.hindustantimes.com/tech/news/hackers-

of these attacks are known to have in fact caused physical damage, the gravity and scale of their potential economic impact necessitates that we explore the topic more critically beyond their cursory media coverage.

Due to a lack of consensus on the use of terminology around cyber attacks, different media organisations cover cyber threats differently. This becomes problematic when the statistics reported in the media show a much higher margin than those reported by CERT-In, India's Computer Emergency Response Team.[23] The difference however, is understandable. As discussed above, not all attacks are consequential; moreover, a widely agreed upon definition for cyber 'attacks' does not exist.

Data released by India's CERT-In reveals a substantial increase in incidents like network scanning and probing between 2017 and 2018 alone[24] — from 9,359 incidents in 2017, to 1,27,481 incidents in 2018. Separate from malicious cyber activity tracked by CERT-In, increasing cyber crimes too, are a cause for cyber insecurity. The National Crime Records Bureau (NCRB) reported a doubling of ICT-enabled crimes under the Indian Penal Code between 2016 and 2017.[25] According to the NCRB, more than half of the reported cyber-crime in India is economically motivated, and causes great financial losses to citizens, perpetuating economic insecurity.[26]

However, these statistics on malicious cyber activity and cyber crime against Indian targets do not indicate whether their origins can be attributed to another state, or non-state actors or individuals, who may be foreign or domestic. Because of numerous technological, strategic and legal barriers to decisive attribution of cyber attacks and

---

continue-targeting-remote-employees-in-india-36mn-attacks-reported-till-nov-71608453968390.html>.

[23] For a compilation of statistics released by CERT-In on malicious cyber activity in India since 2013, see Gunjan Chawla, SharnganAravindakshan and Vagisha Srivastava, CCG's Comments to the National Security Council Secretariat on the National Cyber Security Strategy 2020, Centre for communication Governance at National Law University Delhi, 10 January 2019, at pp. 6-9, < https://ccgdelhi.org/2020/01/30/ccgs-comments-to-the-national-security-council-secretariat-on-the-national-cyber-security-strategy-2020/>

[24] Gunjan Chawla, SharnganAravindakshan and Vagisha Srivastava, CCG's Comments to the National Security Council Secretariat on the National Cyber Security Strategy 2020, Centre for communication Governance at National Law University Delhi, 10 January 2019, at pp. 6-8, available at https://ccgdelhi.org/2020/01/30/ccgs-comments-to-the-national-security-council-secretariat-on-the-national-cyber-security-strategy-2020/.

[25] Ibid at pp. 15-16.

[26] Ibid.

incidents, India is faced with a kind of 'Schrödinger's cyberwar'.[27] The State is defending itself against adversaries whose legal status, and consequently, rights and obligations remain unclear in law, often due to technological obfuscation.[28] These threats could be executed by various means - some trivial and some very sophisticated ones. These include, but are not limited to malwares - like trojans, viruses, adwares, spywares, - botnets, SQL injections, phishing attacks, Denial of Service attacks, man in the middle attacks, etc.

Additionally, the covid health crisis underscored the fundamental benefits of ICTs and our reliance upon them, including for provision of vital government services, communicating essential public safety messages, innovative solutions to ensure business continuity, accelerating research, and the possibility to maintain social cohesion through virtual means. Underscoring the lack of awareness and adequate capacities to detect, resist or respond to malicious activities constitutes a threat in and of itself as all countries are increasingly reliant on digital technologies.[29]

While cyber threat and anticipation of loss is different for different organisations and individuals, the risk of a cyber attack exists for every person and organisation with a digital presence. Owing to rapid digitisation, government security could also be severely compromised if not secured by proper means. This brings us to the point that cybersecurity is important for companies, individuals and governments alike. Of course, the scope and gravity of threats as well as their adverse effects will differ on a case-by-case basis.

[27] Gunjan Chawla, The Legal Contours of India's 'Sovereign Cyberspace', The Seminar, July 2020, available at https://www.india-seminar.com/2020/731/731_gunjan_chawla.htm. Image: "Arms Race" by Khahn Tran is licensed under CC BY 4.0

[28] Ibid.

[29] Zero Draft' of the report of the UN OEWG on developments in the field of information and telecommunications in the context of international security, 19 January 2021, para 23, <t https://front.un-arm.org/wp-content/uploads/2021/01/OEWG-Zero-Draft-19-01-2021.pdf>

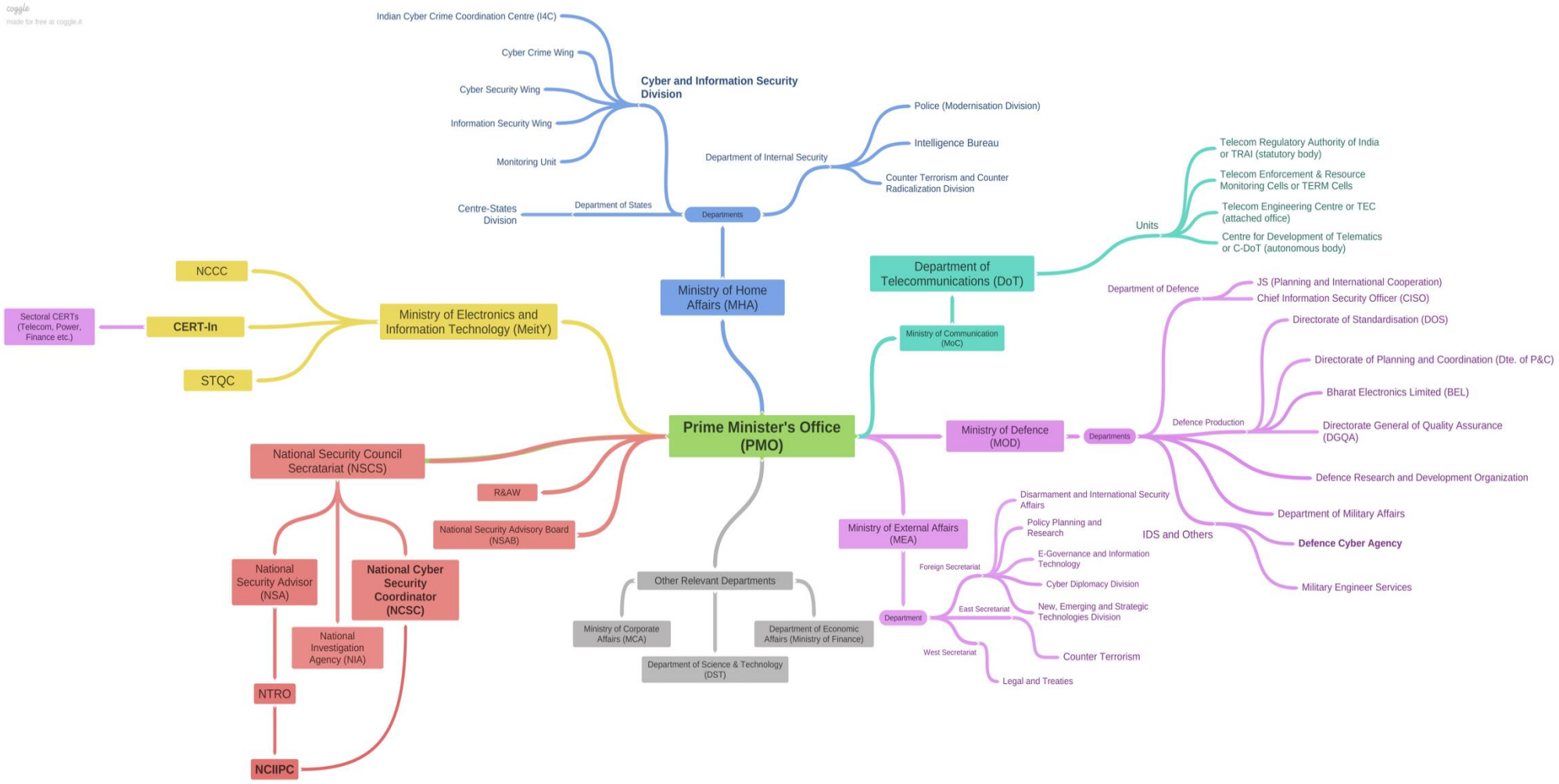
Mapping Government Institutions

Thus, it is apparent that cybersecurity is a shared concern for all who are digitally connected. As the economy as well as governance institutions of the nation transition from being digitally-enabled to becoming digitally-dependent, every government department and agency bears its own responsibility to ensure their cybersecurity.[30]

However, certain ministries and departments have specified roles to play and responsibilities to discharge in accordance with the rule of law. The institutions and departments charged with leading the formulation and execution of cybersecurity policies and measures can thus be depicted as an inter-ministerial or inter-departmental ecosystem (Figure 2). While the map presented below includes those ministries and departments of government that are driving cybersecurity initiatives, it is an indicative rather than an exhaustive presentation of the architecture of cybersecurity institutions in the country. A more holistic, whole-of-government approach to cybersecurity envisions the presence of extensive processes, mechanisms and collaboration across all levels of government.

[30] "Rising Digital Dependence during Pandemic Heightening Cyber Threats: WEF Survey" (*The Times of India*) Jan 11 2022 <https://timesofindia.indiatimes.com/business/india-business/rising-digital-dependence-during-pandemic-heightening-cyber-threats-wef-survey/articleshow/88838621.cms>

Figure 2: The Architecture of Cybersecurity Institutions in the Government of India



Source: Chawla Gunjan, "The Architecture of Cybersecurity Institutions in India" (*The CCG Blog* February 7, 2020) <https://ccgnludelhi.wordpress.com/tag/national-security-council-secretariat/>

PART II: Budgeting for Cybersecurity

Why is it important to budget for cybersecurity?

The COVID-19 pandemic has led to a 'new normal' that is characterised by accelerating digitisation across all industries and levels of government. In a report released by the Ministry of Electronics and Information Technology (MeitY), India's digital economy is estimated to be $200 billion in 2019 and projected to increase fivefold to $1 trillion by 2025.[31] The government's flagship 'Digital India' initiative is also seeking to drive digital inclusion efforts, development of network infrastructure[32] and collaborative technology solutions to enhance service delivery.[33] While such efforts will lead to growth of the country's cyberspace in the coming future, the restructuring of network and security systems that the pandemic necessitated in the private sector has increased vulnerabilities to cyberattacks and breaches.[34] In 2021 for instance, a global survey conducted by cybersecurity firm Sophos found that 67% of Indian organisations had to pay a ransom to retrieve their data compromised from ransomware attacks, a two-fold increase from the previous year.[35] It is clear that with digitisation and growth of the cyber realm, the attack surfaces or opportunities for malicious actors also increase manifold.

---

[31] "India's Trillion-Dollar Digital Opportunity: Ministry of Electronics and Information Technology, Government of India" (Ministry of Electronics and Information Technology, Government of India) <https://www.meity.gov.in/content/india%E2%80%99s-trillion-dollar-digital-opportunity>

[32] Infrastructure: Digital India Programme: Ministry of Electronics & Information Technology (MeitY) Government of India" (Infrastructure | Digital India Programme | Ministry of Electronics & Information Technology (MeitY) Government of India) <https://www.digitalindia.gov.in/infrastructure>

[33] Aryan A, "It Ministry Plan: One Digital ID That Links, Can Access Other Ids" (The Indian Express January 30, 2022) <https://indianexpress.com/article/india/it-ministry-plan-one-digital-id-that-links-7747828/>

[34] "Infrastructure: Digital India Programme: Ministry of Electronics and Information Technology (Meity) Government of India" (Infrastructure | Digital India Programme | Ministry of Electronics and Information Technology (MeitY) Government of India) <https://www.digitalindia.gov.in/infrastructure>

[35]'India tops ransomware attacks globally with 68% entities impacted: Sophos' (The Business Standard 1 June 2021) < https://www.business-standard.com/article/technology/india-tops-ransomware-attacks-globally-with-68-entities-impacted-sophos-121060100982_1.html>

There is thus a pressing need for various entities of government to understand and budget for cybersecurity needs, be prepared to respond to cyber incidents and develop skilled expertise and allocate appropriate resources that will help develop the overall cyber resilience of the country. While needs are likely to vary across ministries, the formulation of normative benchmarks that dedicate specific budgetary allocations towards cybersecurity at the ministerial, departmental and state levels will ensure adaptability and preparedness of the government as-a-whole. The Haryana State Cyber Security Policy Framework (2017)[36] is a good example of efforts at the state level to enumerate cybersecurity objectives and lay out a framework for policies, processes and programs towards this end. Significantly, the policy recommends that 10% of the IT budgets of all departments, agencies and organisations should be earmarked towards implementation of plans laid out for cybersecurity.[37]

Budgeting priorities for cybersecurity are also indicative of the balance struck by a country between offensive and defensive cyber capabilities and shape preparedness for response to threats in cyberspace. According to the Stockholm International Peace Research Institute (SIPRI), India ranks third in terms of defense expenditure only after the US and China.[38] The US has allocated $18 billion for cybersecurity related activities in the President's budget for FY 2021. This cybersecurity allocation forms 0.26% of the total $6.8 trillion budget of the U.S. Government's in FY 2021.[39] Statistics on China's cybersecurity budget allocations are not available in the public domain.[40] However, it is evident that both the US and China are actively investing in advancing their cyber capabilities. In light of recent developments at the India-China border,[41]

[36] Cyber Security Policy 2017, Electronics and Information Technology Department, Government of Haryana <https://cdnbbsr.s3waas.gov.in/s35352696a9ca3397beb79f116f3a33991/uploads/2020/07/2020071457.pdf>

[37] Ibid p. 18

[38] Ankit Panda, China and India Top Asian Military Spending, Figure in World Top 3 With US,(The Diplomat, 28 April 2020), <https://thediplomat.com/2020/04/china-and-india-top-asian-military-spending-figure-in-world-top-3-with-us/#:~:text=The%20two%20countries%20were%20the,military%20spenders%20in%20SIPRI's%20database>.

[39] "Budget of the United States Government" (govinfo.gov March 17, 2021) <https://www.govinfo.gov/help/budget>

[40] "U.S. Government to Spend over $18 Billion on Cybersecurity - HS Today" (*Homeland Security Today* June 23, 2020) <https://www.hstoday.us/subject-matter-areas/cybersecurity/u-s-government-to-spend-over-18-billion-on-cybersecurity/>

[41] India-China dispute: The border row explained in 400 words' (BBC News 25 January 2021) <https://www.bbc.com/news/world-asia-

and rising concerns around China's cyber capabilities,[42] it is essential for India to enhance and further develop its own cyber capabilities.

The complexity of the technical architecture required for a layered defense of the nation's assets in cyberspace is illustrated in Figure 1 (Defense in Depth). Certainly, such an elaborate system may not always be feasible, or even necessary in all use cases. Therefore, it is imperative for the government to identify and prioritise which of its functions (e-governance, border security, internal security, law and order, welfare, etc.) and assets (infrastructural or informational) require higher degree of protection from cyber threats and therefore, may be in need of greater allocation of resources (financial, technical or human).

Finally, in order to align with international best practices, we need to actively invest in and allocate expenditure towards cybersecurity in the national budget. According to the framework defined by the United States' National Institute of Standards and Technology ("NIST Framework"), a meaningful cybersecurity strategy would identify, protect, detect, respond to and recover from any and all threats in cyberspace.[43] In doing so, it is important to consider the internal and external constraints operating to restrict our security choices in order to economise and encourage the judicious use of available resources towards cybersecurity.

The International Telecommunications Union ("ITU") also proposes allocation of a dedicated budget and resources towards a cybersecurity strategy such that resources can even be allocated by tasks, objectives or departments and ministries.[44] According to the proposal, "*resources should be defined in terms of money, people, material, as well as the relationships and partnerships along with continued political*

53062484#:~:text=In%20August%2C%20India%20accused%20China,of%20firing%20into%20the%20air>

[42] Jr Ng, 'China Broadens Cyber Options' (Asian Military Review 15 January 2020) <https://asianmilitaryreview.com/2020/01/china-broadens-cyber-options/>

[43] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, 16 April 2018, at pp. 7-8, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

[44] Ibid at p. 38

commitment for successful execution [of the strategy]."[45] Such assessment and classification of resources is especially important for the Government of India, which is currently in the process of reviewing and revising its National Cyber Security Strategy.

Why is it important to keep track of budgeting for cybersecurity?

The following section attempts to deduce the quantum of financial resources made available by the Indian government vis-à-vis cybersecurity by analysing publicly available data on budgetary allocations to relevant ministries and departments since FY 2012-13 in support of their role and functions to ensure and improve the state of cybersecurity in India. Tracking of the budget will provide an evidence-based understanding of the country's cybersecurity priorities. This will foreground insights into what domains, if any, are being overlooked thereby enabling focus on a more proactive and adaptive approach to developing a secure cyber ecosystem. In this regard, a continuous monitoring approach to India's cybersecurity budget would be more fruitful than the current model of action as a response to an attack.

Tracking of the budget is also essential to ensuring accountability for allocations toward cybersecurity and assessing state capacity to implement programs and schemes that have been allotted funds.

An important case in point is the FY 2020-21 Union Budget's proposal for a ₹8,000 crore allocation towards Quantum Computing over a period of five years.[46] Close scrutiny of the Demands for Grants for FY 2020-21, FY 2021-22 and FY 2022-23 indicate that no such allocation towards a 'National Mission on Quantum Computing' has been made to departments within the Department of Science and Technology (DST), Ministry of Electronics and Information Technology (MeitY), Department of Telecommunications (DoT) or the Ministry of Home Affairs (MHA).

[45] International Telecommunication Union, Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity, 2018, at p. 14, <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf>

[46] Government of India, Union Budget 2020-21, Speech by the Finance Minister Ms. Nirmala Seetharaman in the Lok Sabha on 1 February 2020.

An Office Memorandum of the DST indicates that an Apex Committee was constituted in October 2018 to consider a Quantum Information Science and Technology cluster proposal[47] under the Interdisciplinary Cyber Physical Systems Division (ICPS). Indeed, the figure of ₹8,000 crore can be spotted as the estimated cost of such a mission over five years in a Draft Concept note by the Department of Science and Technology (DST) on a 'National Mission on Quantum Technology and Its Applications',[48] which also mentions plans to set up a national Centre for Development of Quantum Technology or 'C-DoQ'

However, it is imperative to highlight that the total budget allocated to the National Mission on Interdisciplinary Cyber Physical Systems for is merely ₹270 crores for FY 2020 - 21 and ₹350 crores for FY 2022-23. As on date, C-DoQ or any mention of a National Mission on Quantum Technology cannot be found in the Ministry's Demands for Grants in the Union Budget presented before Parliament. According to a leading news report, as of January 2021, the National Mission on Quantum Technologies and its Applications was still awaiting clearance from the Union Cabinet.[49] Although the website of the Office of the Principal Scientific Advisor (PSA) appears to reference that an allocation of ₹204 crores to a quantum technologies research program was made in 2018,[50] this figure or budget head does not seem to be available in the DST's expenditure budget for the year mentioned. It is also relevant to note that the PSA's total budgeted expenditure for FY 2018-19 was ₹53.18 crores only. On August 19th 2022, the PSA stated publicly that the Department of Science and Technology is leading the work of multiple government ministries towards the imminent launch of

[47] Department of Science and Technology, OM No. DST/ICPS/QuSt dated 18 October 2018, <https://tifac.org.in//images/nmqta/OM_apex_committee.pdf. More relevant documents can be accessed at https://tifac.org.in/index.php/17-announcement/909-national-mission-on-quantum-technologies-applications-nmqta>

[48] Technology Information, Forecasting and Assessment Council (TIFAC), Department of Science and Technology, National Mission on Quantum Technologies and Applications, Draft Concept Note on National Mission for Quantum Technologies and its Applications (NM-QTA), <https://tifac.org.in//images/nmqta/concept_note12.06.19.pdf>

[49] Chethan Kumar, Rs. 8000 crore quantum mission a step away from cabinet, RRI scientist hailed, The Times of India, 21 January 2021, < https://timesofindia.indiatimes.com/india/rs-8000-crore-national-quantum-mission-one-step-away-from-cabinet/articleshow/80372320.cms>.

[50] Office of the Principal Scientific Advisor to the Government of India, Quantum Technologies, <https://www.psa.gov.in/technology-frontiers/quantum-technologies/346>

the scheme.[51] However, there has been no publicly available information on relevant developments up until January 2023.

Further, we find that there is a lack of clarity on the exact quantum of funds dedicated to and used for cybersecurity-related activities by various departments and ministries. An inherent limitation for analysis arises due to the existing format in which the Union Budget is presented. This can lead to variations in the identification of funds that are being dedicated to cybersecurity as a whole, and present a challenge for the analysis of broader trends in the budget over time. For instance, on 28th July 2021, the total funds allocated by MeitY for strengthening cybersecurity between 2015 and 2022 was presented as ₹1,333.48 crores in Parliament in response to Starred Question No. 139.[52]

However, this figure does not capture the emphasis placed on adopting a whole-of-society *and* whole-of-government approach to ensuring and improving cybersecurity by the National Security Council Secretariat (NSCS), in its call for comments on the National Cyber Security Strategy. CCG's comments, in response to this call, asserted that the principle of "common but differentiated responsibility" can be used to operationalise both these approaches. Necessarily, this implies that the responsibility for the country's cybersecurity at the government level does not rest exclusively upon MeitY. Our analysis demonstrates that this figure is the summation of two specific budget heads under MeitY's Expenditure Budget that are overtly relevant to cybersecurity, i.e., cybersecurity functions performed by CERT-In and the National Cyber Coordination Centre (NCCC).

Due to a narrow understanding of 'cybersecurity' adopted by the government for responding to the above mentioned question, the data gathered and presented in this report does not align with the government's response to Starred Question No. 139 during the Monsoon session in 2021. We posit that total allocations towards

[51] "National Quantum Mission to Be Launched 'Very Soon', Says PSA Ajay Sood" (*The Economic Times* November 30, 2022) <https://economictimes.indiatimes.com/news/science/national-quantum-mission-to-be-launched-very-soon-says-psa-ajay-sood/articleshow/95891074.cms?from=mdr> Choudhary S, "Exclusive: India's 'Quantum Leap' in Computing Soon, Work in Advanced Stage: PSA Sood" (*News18* August 19, 2022) <https://www.news18.com/news/tech/exclusive-india-to-take-quantum-leap-in-computing-soon-work-in-advanced-stage-psa-sood-tells-news18-5778547.html>

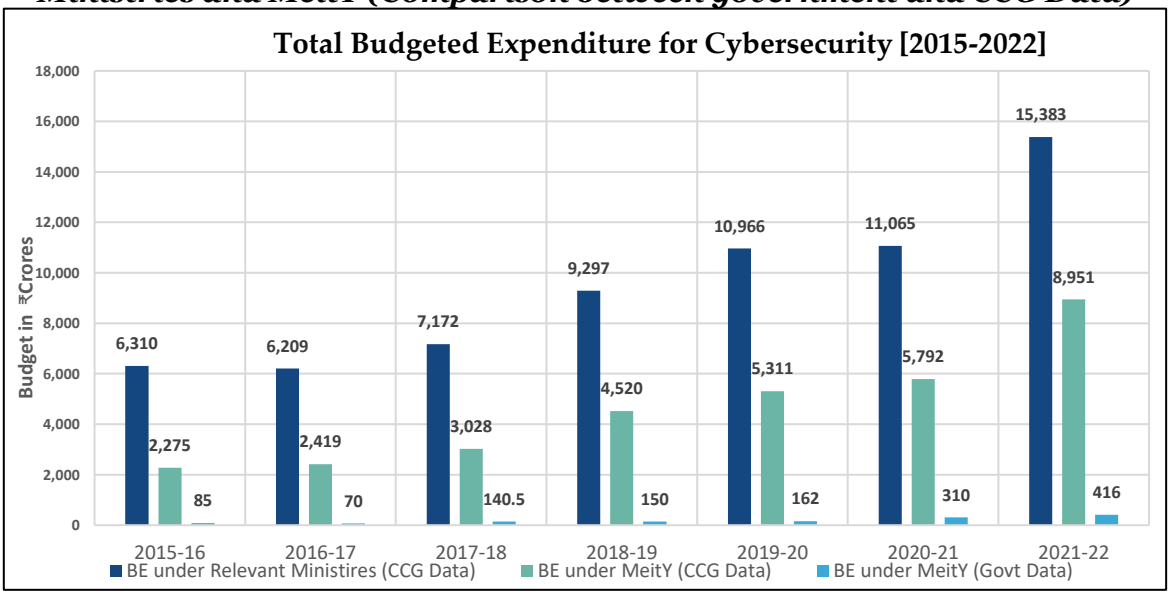
[52] Starred Question No. 139, Questions, Lok Sabha House of the People, Parliament of India <http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=25631&lsno=17>

strengthening cybersecurity over the seven-year period from FY 2015-16 to FY 2021-22 is ₹32,297 crores under MeitY, and ₹66,402 crores across all relevant ministries identified in this report, and that allocations should be much higher than what was reported in this particular response. It is important to note here that cybersecurity allocations reported in this brief are estimations of the total cybersecurity budget, indicative of the entire pool of resources available for cybersecurity. These figures must be viewed as the pool of financial resources available to government to strengthen the state of cyber security and various aspects of internet governance related thereto at the national level, including the security of e-governance initiatives to facilitate the online delivery of public services to citizens.

This is because firstly, there are several other departments and budget heads, such as the Digital India programme to name but one, within MeitY's Demands for Grants that are highly relevant to paint a full, more comprehensive picture of the resources required and available for utilisation towards better cybersecurity within governmental institutions and beyond. Secondly, a whole-of-government approach to cybersecurity demands that each department and ministry play an active role in ensuring their own cybersecurity, under the guidance of national nodal institutions like CERT-In and National Critical Information Infrastructure Protection Centre (NCIIPC).[53] Accordingly, we have identified a total of 47 budget heads that are directly relevant to the nation's cybersecurity under various ministries. Chart 1 presents the gap in budgetary allocations toward cybersecurity between government data and the data on cumulative and ministry-wise cybersecurity budgets as presented in this report.[54]

[54] Refer pages 18 & 21 of this report.

Chart 1: Total Budgeted Expenditure for Cybersecurity under Relevant Ministries and MeitY (Comparison between government and CCG Data)



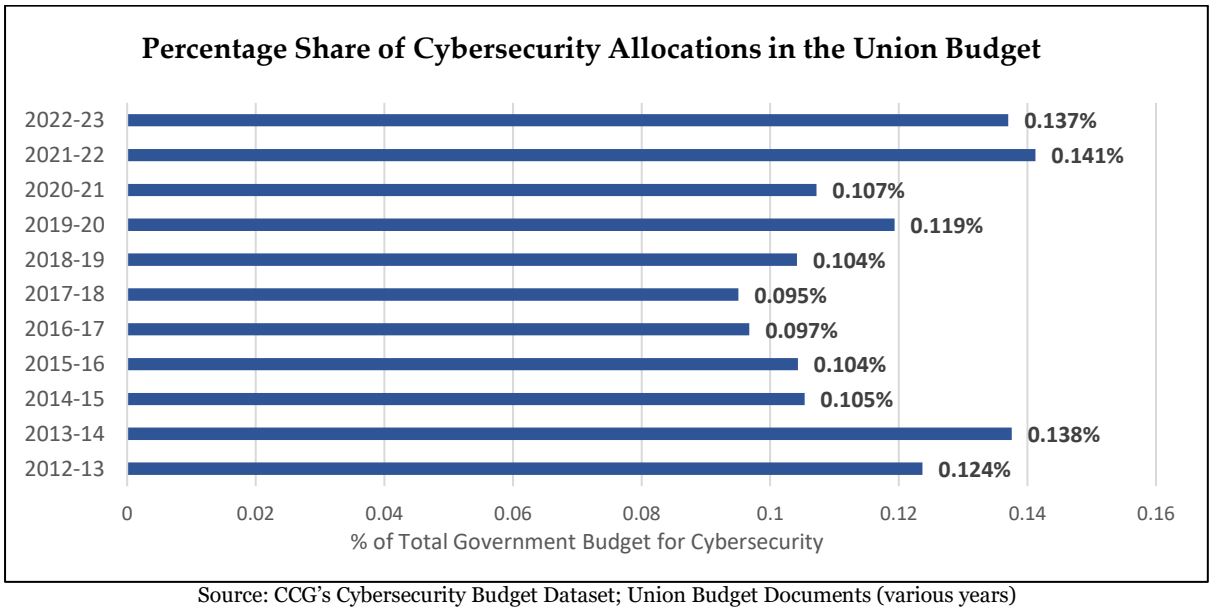
Source: For "CCG Data" – CCG's Cybersecurity Budget Dataset, and for "Govt Data" - Starred Question No. 139 from Lok Sabha's Monsoon Session in 2021

The lens used to approach analysis of budgetary allocations toward cybersecurity is crucial in terms of what activities can and cannot be classified as being directly related to cybersecurity. CCG's 'Cybersecurity Budget Dataset' includes those budget heads that are demonstrably linked to cybersecurity and have a role to play in the growth and development of the country's cyber resilience. Volume II Annexure I (Research Methodology and Interpretation Guidance) appended to this report contains the rationale for classification of each specific budget head and its relevance for cybersecurity.

In order to provide a frame of reference for the varying estimates of the cybersecurity budget presented in Chart 1, we use the total government budget (as presented in the Demand for Grants Summary for each year) to identify what percentage of it has been allocated for cybersecurity since FY 2012-13. Here, the 'Cybersecurity Budget' is taken to be the budgeted expenditure for cybersecurity under all the identified relevant ministries as presented in this report. Chart 2 depicts the percentage of the total government budget being directed towards cybersecurity. It is evident that on average, the Indian government allocates 0.1% of its total budget to cybersecurity related activities annually. In FY 2020-21, we note that cybersecurity has received the highest percentage share of the total government's budget yet, with 0.141% of it being directed

towards cybersecurity. The release of the National Cyber Security Policy in 2013 coincides with the second highest share of total government budget for cybersecurity at 0.138% in FY 2013-14.

Chart 2: Percentage Share of Cybersecurity in Total Union Govt Budget



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Further, placing the total cybersecurity budget in the context of allocations for the Ministry of Defense. can serve as a benchmark for tracking the cybersecurity budget. In FY 2021-22 the allocation to the Ministry of Defense is the highest among all ministries of central government, at 14% of the Union Budget.[55]

While such references can provide indicative inferences about India's cybersecurity allocations, building standardised benchmarks to better gauge the quality and quantity of public expenditure on cybersecurity will significantly benefit the policy making process and aid the efforts of researchers.

[55] "Demand for Grants 2021-22 Analysis: Defence" (PRS Legislative Research January 23, 2022) <https://prsindia.org/budgets/parliament/demand-for-grants-2021-22-analysis-defence>

While certain other budget heads under the Ministry of Defense,[56] Ministry of External Affairs,[57] Department of Telecommunication[58] and Ministry of Home Affairs[59] can possibly be used for cybersecurity-related activities, their expenditure values are at best an estimate of the total funds available which *may* be utilised for cybersecurity-related functions. It is not possible to infer from the current format of the Demands for Grants the precise share of these allocations that are actually used for activities directly related to cybersecurity. While it is important to highlight these areas of potential for cybersecurity – as supporting allocations - including them in our analysis would only inflate allocations for cybersecurity and skew findings. The next section explores our dataset curated with a balanced approach to include those budget heads that are demonstrably linked to cybersecurity. In adopting this methodology,[60] we avoid extreme representations of budgetary allocations towards cybersecurity.

How do we analyse the budget for cybersecurity?

The dataset compiled for this analysis collates expenditures incurred on government programs and activities relevant to cybersecurity since FY 2012-13, one year prior to the promulgation of India's first National Cybersecurity Policy in 2013. Data was gathered 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 those ministries and their respective departments, from FY 2012-13 to FY 2022-23, that are related to cybersecurity.

[56] Under **Ministry of Defence,** we consider the Navy/Joint Staff (Capital), Ordnance Factories R&D (Revenue), Research and Development including the Research and Development component of R&D head (Revenue), Capital Outlay on R&D (Capital) and Technology Development and Assistance for Prototype Development under Make Procedure (Capital) to contribute towards the larger security and governance framework in cyberspace.
[57] Under **Ministry of External Affairs,** we consider the following heads to be important for cybersecurity: Special Diplomatic Expenditure, Expenditure for International Cooperation, Expenditure for Technical and Economic Cooperation with other Countries, and Other Expenditure of Ministry.
[58] Under **Department of Telecommunication** Defence Spectrum/Network for Defence Services, Capital Outlay on Telecommunication and Electronic Industries, Capital Outlay on Other Communication Services and Universal Service Obligation Fund (USOF) are most relevant for cybersecurity.
[59] Under **Ministry of Home Affairs,** departments that are involved with defence and intelligence along with law enforcement are crucial to be considered for cybersecurity. The allocations for Intelligence Bureau, Delhi Police, and Capital Outlay on Police are relevant here.
[60] Refer Volume II Annexure I appended to this report

The budget data has been grouped into two primary buckets for analysis relevant to departments' ministry-wise allocations and activity-wise allocations. The classification of **'relevant departments'** includes budget heads from those departments under each ministry which are either directly related to cybersecurity and/or support the functioning of the security aspects of internet governance at large. We analyse cybersecurity budgets under the Ministry of Electronics and Information Technology (MeitY), Ministry of Home Affairs (MHA), Department of Telecommunications (DoT) and Other Relevant Departments.

Under **'activity wise allocations'**, we have classified the listed expenditures from the 'relevant departments' bucket under six categories. These include (1) Cyber Incident Preparedness and Response, (2) Technical Research and Capacity Development, (3) Human Resource Development, (4) International Co-operation and Investment Promotion, (5) Standardisation, Testing and Quality Certification and (6) Digital Identity. Each of these categories align with a constituent element of the Three Pillars of the National Cyber Security Strategy – Secure, Strengthen and Synergise.[61] The rationale for classification of each budget head under a certain activity can also be found in Volume II Annexure I (Research Methodology and Interpretation Guidance), appended to this brief.

Limitations of analysis in the cybersecurity budget brief

The analysis in this brief is subject to limitation, such that estimations of the total cybersecurity budget presented are indicative of the entire pool of resources available for cybersecurity. This is due to the fact that entire budgeted allocations for all the programmes and schemes in our analysis are not utilised exclusively for cybersecurity and its related activities. The current format of the Demands for Grants does not allow for inference of the precise share of budgeted allocations that are actually used for activities directly related to cybersecurity. All budget heads included in our analysis therefore fall on a spectrum of high significance to low significance with respect to percentage share of their budgeted allocations being utilised for cybersecurity. For

[61] These three "Pillars of Strategy", namely, Secure, Strengthen and Synergise were identified by the National Security Council Secretariat as such in the call for comments on the National Cyber Security Strategy 2020-25.

certain budget heads, it is likely that a greater share of the allocation is directed towards cybersecurity related activities. For example, it is likely that for Cybersecurity projects under the Digital India scheme and CERT-In, both under MeitY, the entire allocation is directly relevant for cybersecurity. On the other hand, for budget heads such as the Prime Minister's Office under MHA, only a specific percentage of the total allocated budget is likely to be directed towards cybersecurity activities. However, there exist no relevant mechanisms to establish what percentage of these allocations can be taken as relevant for cybersecurity activities, and thus the entire allocation has been included for such budget heads in our analysis.

An overview of the cybersecurity budget

An overview of the broad trends in budgeting for cybersecurity will help contextualise our analysis in the next two parts of this report. Table 2 displays a clear trend of increasing allocations for cybersecurity since FY 2012-13, that have more than doubled by FY 2021-22. Budgeted expenditure for cybersecurity was ₹6,612 crores in FY 2012-13 and is ₹15,575 crores in FY 2022-23. The compound annual growth rate (CAGR) for budgeted allocations towards cybersecurity is 8.10% in FY 2022-23, over a period of eleven years since FY 2012-13.

Additionally, we note that revised expenditures for cybersecurity have been consistently lower by 9% of the budgeted allocations in the last three years from FY 2019-20 to FY 2021-22.

Table 2: Budgeted, Revised and Actual Expenditures for Cybersecurity (CCG Data)*

Financial Year	Budgeted Expenditure (in ₹ crores)	Revised Expenditure (in ₹ crores)	Actual Expenditure (in ₹ crores)	Budgeted vs Revised%	Budgeted vs Actual%
2012-13	6,612	3,920	3,898	-41%	-41%
2013-14	7,923	5,519	5,483	-30%	-31%
2014-15	6,221	5,225	5,917	-16%	-5%
2015-16	6,310	6,402	5,890	1%	-7%

2016-17	6,210	5,102	6,037	-18%	-3%
2017-18	7,172	6,870	6,577	-4%	-8%
2018-19	9,297	10,790	10,583	16%	14%
2019-20	10,967	10,017	10,036	-9%	-8%
2020-21	11,065	10,071	11,826	-9%	7%
2021-22	17,519	15,864	-	-9%	-
2022-23	15,575	-			
CAGR	**8.10%**	**15%**	**13.12%**		

*Actual expenditure for FY 2021-2022 and Revised Expenditure for FY 2022-23 will only be available in 2023-24.

Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

The total budgeted expenditure in FY 2022-23 is ₹15,575 crores, that marks a 13% decrease in total allocations for cybersecurity from the previous year. However, this figure does not include the four relevant budget heads for cybersecurity across ministries that were introduced in the Union Budget 2022-23 to maintain consistency in the budget heads being tracked in our analysis.[62] Including the four newly introduced budget heads results in a total budgeted expenditure of ₹21,713 crores in FY 2022-23. The outcomes of these new allocations can only be tracked and included in our framework of analysis once the revised and actual expenditures for the schemes are made available in FY 2023-24.

Its further worth highlighting that up until FY 2015-16, gaps between budgeted, revised and actual expenditures were significant such that revised and actual expenditures were substantially lower than budgeted allocations. This underutilisation of the cumulative cybersecurity budget diminishes in subsequent years and in FY 2018-19, actual spending exceeds the allocated budget by 14%. Consistent positive increases in budgeted allocations post FY 2017-18 are also evident. This trend may reflect the increasing priority of efforts toward cybersecurity and aligns with India's ranking in ITU's Global Cybersecurity Index,[63] that improved dramatically in 2020, as it moved up 37 places to rank 10th just below France.

[62] These budget heads are, namely, Production Linked Incentive (PLI) scheme allocation to MeitY, PLI allocation to DoT, Digital intelligence Unit project under DoT and Modernisation of Forensics under MHA.

[63] ITU, "Global Cybersecurity Index 2020"<https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF E.pdf>

In the next two parts of this Brief, we break down the cumulative figures presented above to provide insights from our data analysis under two classifications - Relevant Departments' Ministry-wise classification (Part III) and Activity-wise classification (Part IV).

PART III: Relevant Departments' Ministry Wise Analysis

In this section of our analysis, those departments that are directly concerned with expenditures for cybersecurity are analysed. Select expenditures under the Ministry of Electronics and Information Technology (MeitY), Department of Telecommunications (DoT), Ministry of Home Affairs (MHA) and three other relevant departments are accounted for here. Under 'other relevant departments', four budget heads from different government ministries that are relevant for cybersecurity are included. These are: (1) Technical and Economic Co-operation with Other Countries under the Ministry of Finance's Department of Economic Affairs (2) Unique Identification Authority of India (UIDAI) under MeitY (3) National Mission on Interdisciplinary Cyber Physical Systems under the Department of Science and Technology and (4) Corporate Data Management under the Ministry of Corporate Affairs. A detailed explanation for the relevance of each of the 47 budget heads included in this section of our analysis can be found in Volume II Annexure I appended to this brief.

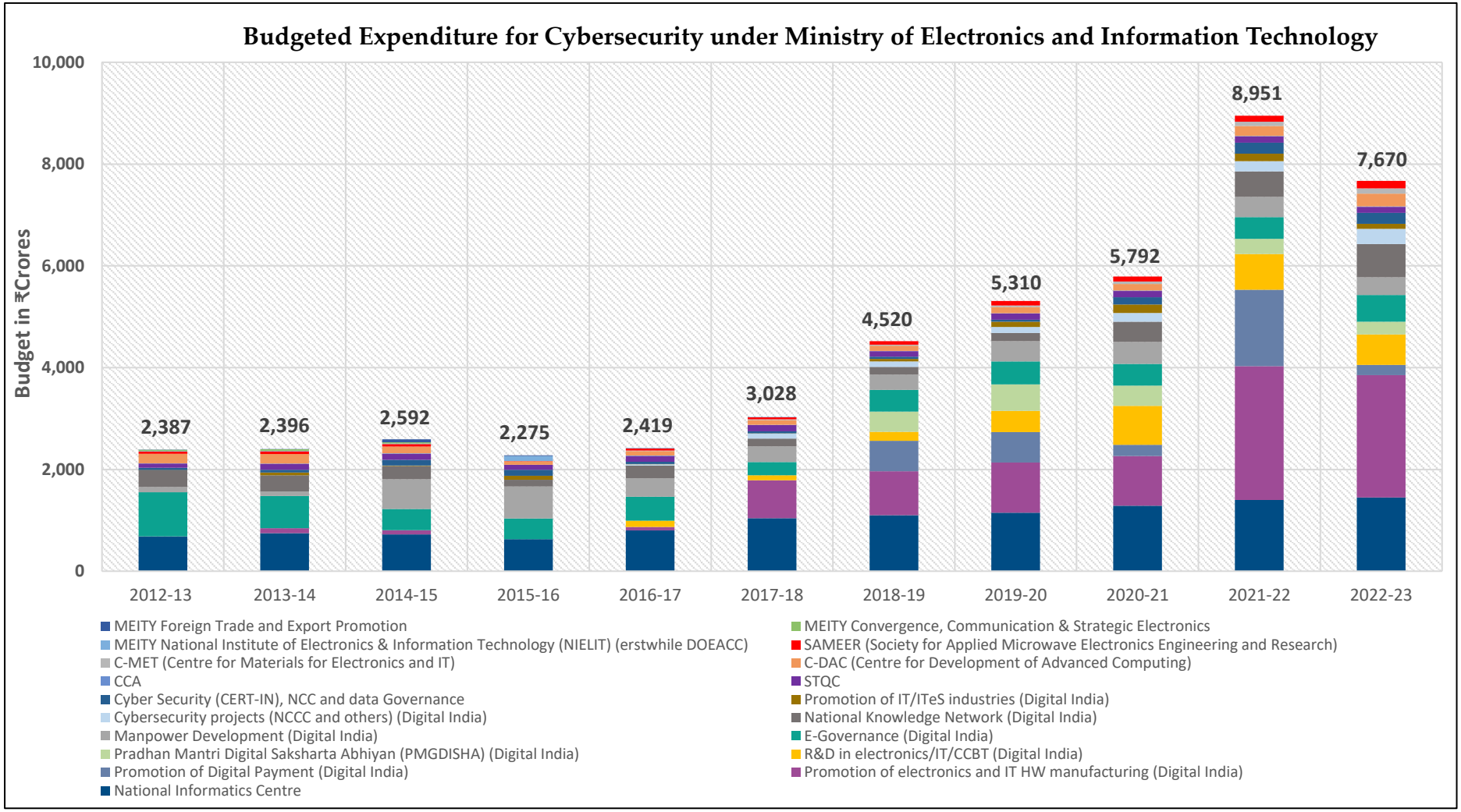
In this part of the brief, an overview of the distribution of allocations among discrete budget heads and trends in budgeting over the last decade is presented for each ministry. Visualisations from CCG's Cybersecurity Budget Dataset summarise the trends in actual, revised and budgeted expenditures at the ministry level.

This is followed by a granular descriptive assessment of how budgeted allocations are revised during the year and the actual expenditures incurred are assessed. We further examine year-on-year changes to present the rate at which budgeted and actual expenditures vary through the years.

(i) Ministry of Electronics and Information Technology (MeitY)

The trends in budgeted expenditure over the last decade for cybersecurity under MeitY have been presented in Chart 3. The distribution of MeitY's budget among relevant budget heads for cybersecurity is also presented in Table 3.

Chart 3: Budgeted Expenditure for Cybersecurity under Ministry of Electronics and Information Technology



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Table 3: Budgeted Expenditure (in ₹ crores) for Relevant Budget Heads under MeitY from FY 2012-13 to FY 2022-23

Relevant Budget Heads for Cybersecurity Under MeitY	FY 2012-13	FY 2013-14	FY 2014-15	FY 2015-16	FY 2016-17	FY 2017-18	FY 2018-19	FY 2019-20	FY 2020-21	FY 2021-22	FY 2022-23
National Institute of Electronics & Information Technology or NIELIT (erstwhile DOEACC)	12	12	11	98	6	-	-	-	-	-	-
Convergence, Communication & Strategic Electronics	23	28	23	-	-	-	-	-	-	-	-
Foreign Trade and Export Promotion	3	3	60	14	3	3	-	-	-	-	-
National Informatics Centre	679	747	720	630	800	1,040	1,100	1,150	1,285	1,400	1,450
Cyber Security (CERT-IN), NCC and Data Governance	42	53	116	115	45	41	40	42	140	216	215
C-DAC (Centre for Development of Advanced Computing)	185	187	133	68	87	92	100	120	127	200	250
STQC (Standardisation, Testing and Quality Certification)	83	117	117	100	112	120	110	120	125	120	120
SAMEER (Society for Applied Microwave Electronics Engineering and Research)	44	51	49	3	39	42	70	90	98	120	150
C-MET (Centre for Materials for Electronics and IT)	-	-	-	-	13	14	20	30	50	80	100
CCA (Controller of Certifying Authorities)	6	6	8	-	8	7	7	8	9	9	9
Digital India Programme											
Promotion of Electronics and IT Hardware Manufacturing	5	100	85	-	70	745	864	986	980	2,631	2,403
Promotion of Digital Payment	-	-	-	-	-	-	596	600	220	1,500	200
R&D in Electronics /IT /Communications, Convergence & Broadband Technologies (CCBT)	-	-	-	-	122	101	178	416	763	700	598
National Knowledge Network	335	320	261	135	250	150	150	160	400	500	650
E-Governance	867	630	415	407	470	261	425	450	425	425	525
Manpower Development	101	90	584	625	365	307	300	401	430	400	350
Pradhan Mantri Digital Saksharta Abhiyan (PMGDISHA)	-	-	-	-	-	-	400	518	400	300	250
Cybersecurity Projects (NCCC and others)	-	-	-	-	25	100	110	120	170	200	300
Promotion of IT/ IT Enabled Services (ITeS) Industries	3	53	10	80	5	6	50	100	170	150	100
Total Budgeted Expenditure for Cybersecurity under MeitY	**2,387**	**2,396**	**2,592**	**2,275**	**2,419**	**3,028**	**4,520**	**5,310**	**5,792**	**8,951**	**7,670**
PLI for Large Scale Electronics and IT Hardware	*Introduced in FY 2022-23*										5,300

Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Budgetary allocations for cybersecurity under MeitY have remained consistent till FY 2016-17, after which there is a significant increase in allocations and introduction of new programs such as Cybersecurity Projects under Digital India, Centre for Materials for Electronics and IT (C-MET) and R&D in Electronics, IT & CCBT (Table 3). Certain developments in this context of increasing allocations in FY 2016-17 are important. In July 2016, the Department of Electronics and Information under the Ministry of Communications was bifurcated and made a full-fledged ministry of its own as MeitY to deal specifically with all matters related to promotion of internet, bridging the digital divide and issuing Aadhaar numbers to all Indian citizens.[64] Additionally, the launch of the Digital India scheme in 2015 is reflected in introduction of several new programs in FY 2016-17 that result in increased total budgeted allocations for MeitY. Of the 19 budget heads classified as relevant for cybersecurity under MeitY, 9 fall under the Digital India scheme.

The following are insights from our analysis of the cybersecurity budget under MeitY:

- Consistent and increasing budgeted allocations towards the Promotion of IT Hardware Manufacturing, R&D in Electronics, IT & Communications, Convergence & Broadband Technologies (CCBT), National Informatics Centre (NIC), SAMEER (Society for Applied Microwave Electronics Engineering and Research) and C-MET (Centre for Materials for Electronics and IT) show the significance of these programs.

- Particularly, we note that **actual expenditures under National Informatics Centre (NIC) have consistently exceeded budgeted allocations** every financial year over the last decade. In FY 2020-21 for instance, the budgeted expenditure for NIC at ₹1,285cr translates to actual spending of ₹1,308cr. The only exception to this trend is FY 2013-14 where actuals decrease by 0.4% from the budgeted allocation. Despite this trend in

[64] The Hindu Business Line, "*Centre Bifurcates Communication Ministry; New Ministry for Information & Technology Formed*", The Hindu Business Line, July 20, 2016 <https://www.thehindubusinessline.com/info-tech/centre-bifurcates-communication-ministry/article8876031.ece>

actual spending, there presently exist manpower shortages and issues of basic infrastructure within NIC.[65] Examining the direction and utilisation of allocations towards NIC could help address such current issues.

- Under the Digital India scheme, Cyber Security Projects, Pradhan Mantri Digital Saksharta Abhiyan (PMGDISHA), Promotion of IT/ ITeS Industries and Promotion of Electronics and IT Hardware Manufacturing receive significant allocations post FY 2018-19.

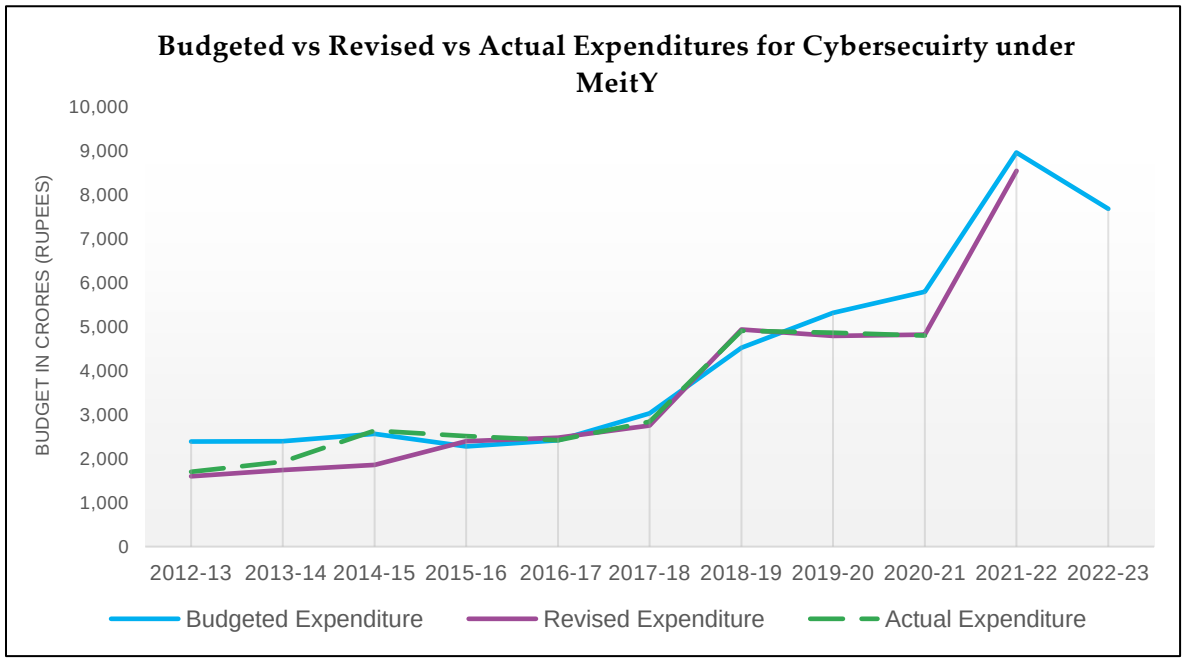
- **The most significant increase in budgeted allocations under MeitY in the last decade is for the Digital Payments scheme which receives a 581% increase from** ₹220cr **in FY 2020-21,** to ₹1,500cr **in FY 2021-22**. There was exponential growth in digital payments in 2016-17 (+74% YoY change)[66] and 2017-18 (+106% YoY change)[67]. FY 2018-19 saw the introduction of a relevant budget head with a BE of ₹595cr. While the revised estimate for FY 2021-22 remains the same as the budgeted allocation at ₹1,500 crores, we note a significant reduction in budgeted expenditure for Digital Payments in FY 2022-23 to ₹200cr – an 87% decrease in allocations from FY 2021-22.

  In the previous year i.e., FY 2020-21, actual spending for Digital Payments was ₹524cr, more than double its budgeted allocation of ₹220cr. Similarly, in FY 2018-19, the actual expenditure is ₹770cr which exceeds the allocated ₹596cr. The promotion of a "Faceless, Paperless, Cashless" economy has been accorded high priority by the government[68] and this is reflected in expenditures for its promotion under MeitY.

[65] "House Panel Calls for Manpower Push to Boost Cybersecurity" (*Hindustan Times*) March 20, 2022<https://www.hindustantimes.com/india-news/house-panel-calls-for-manpower-push-to-boost-cybersecurity-101647801730183.html>
[66] Annual Report 2018-19, Ministry of Electronics and Information Technology, Government of India, p 75 <https://www.meity.gov.in/writereaddata/files/MeiTY_AR_2018-19.pdf>
[67] Annual Report 2018-19, Ministry of Electronics and Information Technology, Government of India, p 75 <https://www.meity.gov.in/writereaddata/files/MeiTY_AR_2018-19.pdf>
[68] Digital Payment Division (DEDPD), Ministry of Electronics and Information Technology, Government of India" <https://www.meity.gov.in/digidhan#:~:text=%E2%80%9CFaceless%2C%20Paperless%2C%20Cashless%E2%80%9D,fold%20of%20digital%20payment%20services.&gt>

- Chart 4 indicates that MeitY's actual expenditures overlaps closely with budgeted allocations over the years. Allocations remain steady in the earlier half of the decade and increasing allocations are evident post FY 2016-17, after the launch of the Digital India scheme in 2015. The most significant increase in total allocations occurs in FY 2021-22 at ₹8,951cr - a 55% increase in allocations from the previous year (Chart 5). This boost is followed by a 14% reduction in total allocations in FY 2022-23. In FY 2014-15, prior to the introduction of the Digital India Scheme, significant cuts from budgeted to revised expenditures occurred across budget heads. These include the National Informatics Centre, e-governance, Manpower Development, Indian Computer Emergency Response Team (CERT-IN), Promotion of IT/ITeS Industries and Standardisation, Testing and Quality Certification (STQC). Despite these lower revised estemitaes, actual spending is infact higher than both budgeted and revised expenditures in FY 2014-15.

Chart 4: Budgeted vs Revised vs Actual Expenditures by MeitY

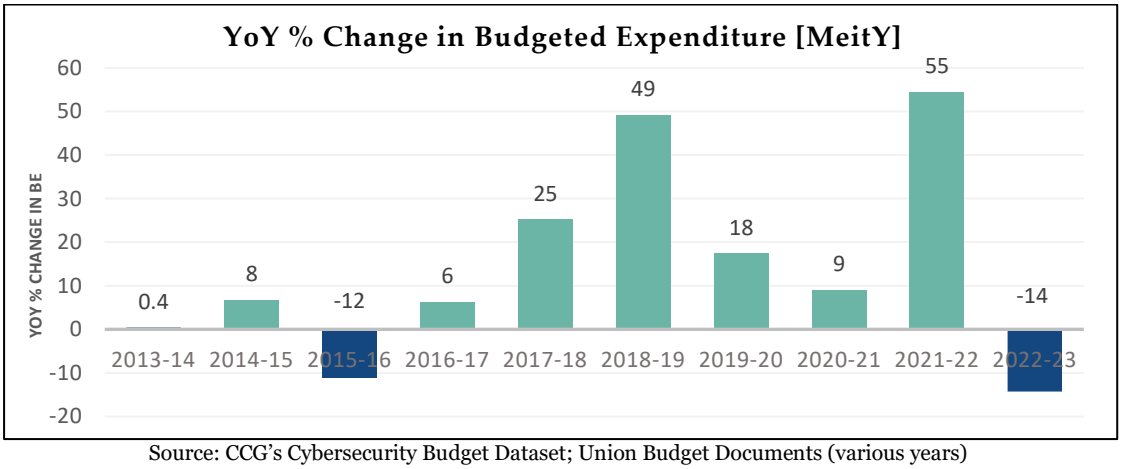


Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

- **After the introduction of the Digital India Scheme in 2015, there appears to be a reconfiguration of spending priorities towards more specialised programs**. Some budget heads see decreased actual spending (in relation to previous years) during the time period between FY 2015-16 and FY

2017-18. These include Centre for Development of Advanced Computing (C-DAC), Cybersecurity (CERT-IN), NCCC and Data Governance and Convergence Communication & Strategic Electronics. On the other hand, significant increases in actual expenditures for R&D in electronics, STQC, Cybersecurity Projects under Digital India and the National Informatics Centre can be seen.

Chart 5: Year on Year Percentage Change in Budgeted Expenditures [MeitY]



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

- In FY 2018-19, it is possible to attribute the increased actual and revised expenditures beyond budgeted allocations to specific budget heads. These include - National Knowledge Network (BE ₹150cr to RE ₹320cr and AE ₹320cr), Digital Payments (BE ₹596cr to RE ₹692cr and AE ₹770cr) and SAMEER (BE ₹70cr to RE ₹97cr and AE ₹97cr).

- Other programs under MeitY that have overt significance for cybersecurity and receive increased budgeted allocations in FY 2020-21 include - Cybersecurity (CERT-IN), NCCC and Data Governance (BE ₹42cr in FY 2019-20 to BE ₹140cr in FY 2020-21) and Cybersecurity Projects under Digital India (BE ₹120cr in FY 2019-20 to BE ₹170cr in FY 2020-21). In FY 2022-23, budgeted allocations for the latter increase while that of the former are sustained.

- We note that **although Promotion of Electronics and IT Hardware Manufacturing has received increasing significance in terms of budgeted allocations, there has been a consistent trend of underutilisation** of funds in terms of actual expenditures through the years for this program. In FY 2013-

14, a BE of ₹100cr translates to an AE of ₹8cr; in FY 2016-17, a BE of ₹70cr sees an AE of ₹50cr and in FY 2019-20, a BE of ₹986cr manifests as an AE of ₹655cr. The only year in the last decade that IT Hardware Manufacturing has not seen lower actual expenditures from the allocations, is FY 2015-16, for which data on the budgeted allocation is unavailable.

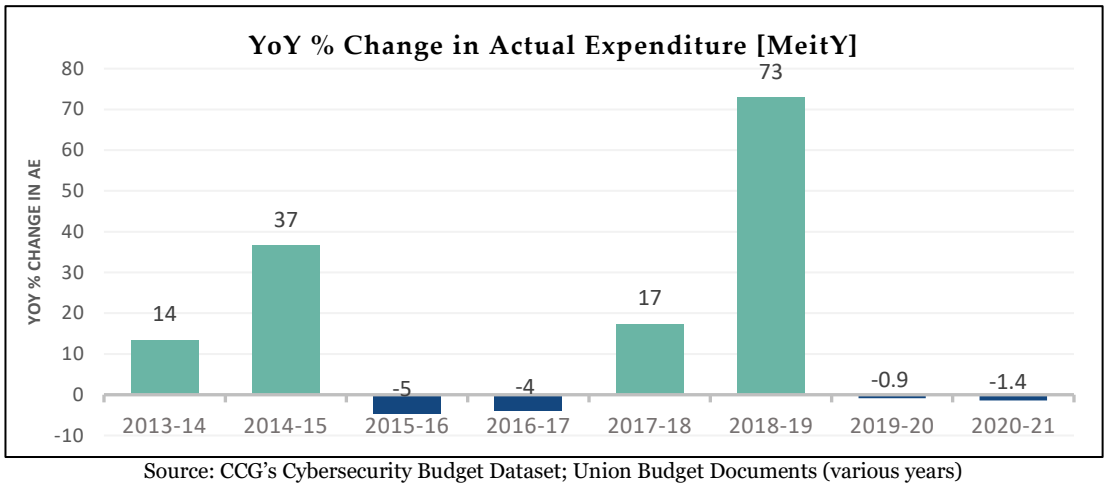
- We also observe that year-on-year changes in actual expenditures since FY 2013-14 for Promotion of Electronics and IT Hardware Manufacturing are characterised by two-year periods of increased actual spending that are followed by two-year periods of decreased spending. For example, in FY 2017-18 (823% increase in actual expenditure from FY 2016-17) and FY 2018-19 (58% increase in actual expenditure from FY 2017-18), we observe significant consecutive increases in actual spending from the previous year. This is followed by decreases in actual expenditure in FY 2019-20 (an 10% decrease from the previous year) and FY 2020-21 (a 27% decrease from the previous year). Such inconsistencies in spending for this component are particularly important in light of the significant allocations that will be made in this direction in subsequent years, via the Production Linked Incentive (PLI) scheme for large scale electronics manufacturing presented in the Union Budget 2022.[69]

- **A similar trend of underutilised funds can be seen for Cyber Security (CERT-IN), National Cyber Coordination Centre (NCCC) and Data Governance** such that actual spending has consistently been lower than revised and budgeted expenditures over the last decade. For instance, in FY 2013-14 (BE ₹53cr to RE ₹42cr to AE ₹41cr), FY 2016-17 (BE ₹45cr to RE ₹32cr to AE ₹19cr) and FY 2018-19 (BE ₹40cr to RE ₹32cr to AE ₹30cr), significant gaps between budgeted and revised expenditures exist. This trend of AE < RE < BE holds across all years over the last decade for Cyber Security (CERT-IN), NCCC and Data Governance. Yet, allocations have increased significantly

[69] "Govt Expects Rs 34,090-Crore Investment under PLI Scheme for Electronics Manufacturing" (*The Economic Times,* 4 February 2022) <https://economictimes.indiatimes.com/news/economy/policy/govt-expects-rs-34090-crore-investment-under-pli-scheme-for-electronics-manufacturing/articleshow/89352799.cms>

towards this budget head over the last three years –from BE ₹42cr in FY 2019-20 to BE ₹2,16cr in FY 2021-22.

Chart 6: Year on Year Percentage Change in Actual Expenditures [MeitY]



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

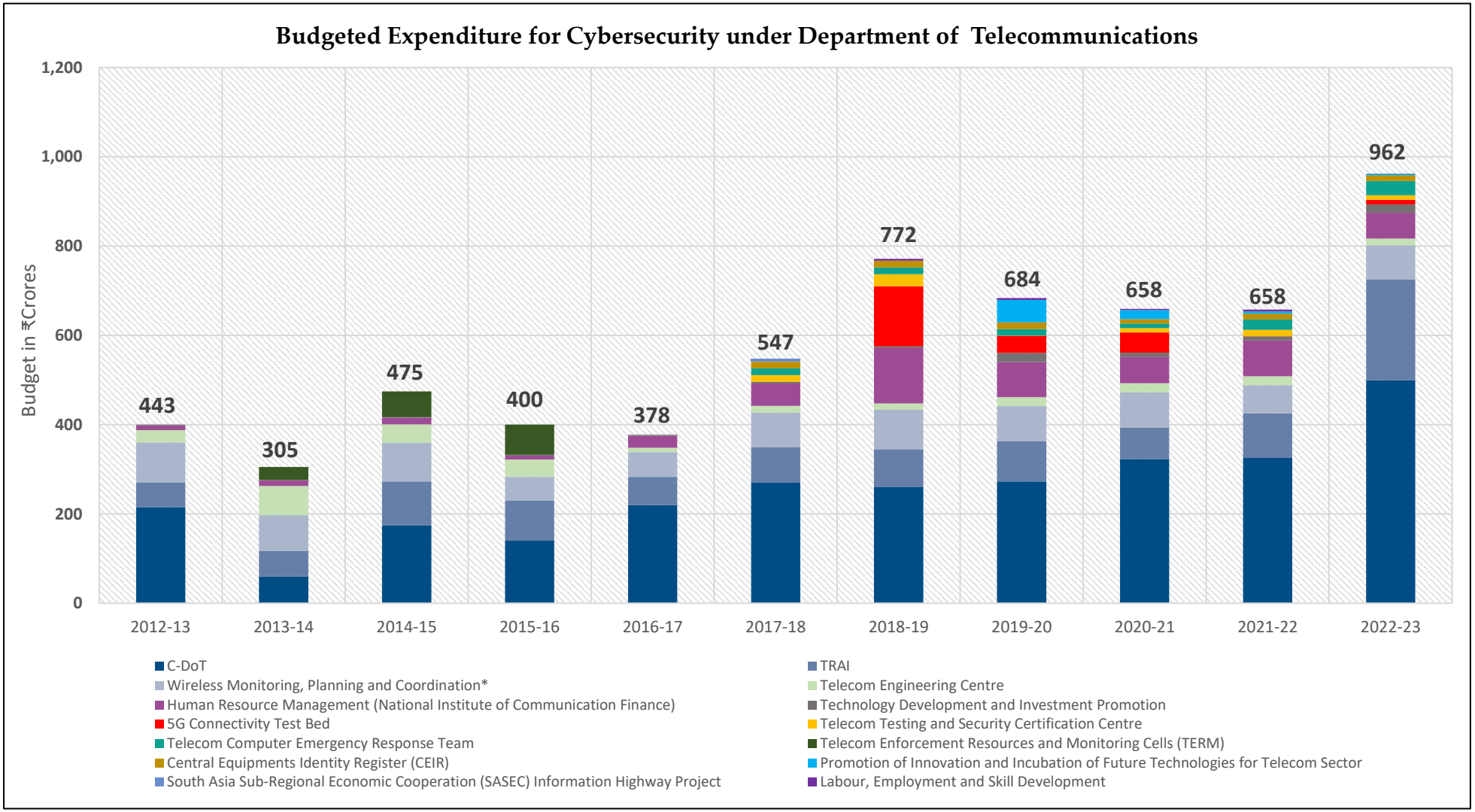
Overall, MeitY has seen increasing total budgeted expenditures for cybersecurity over the last decade, and diversification of spending with the introduction of the Digital India scheme. As the most significant ministry for cybersecurity spending, it is encouraging to note that budgeted allocations have seen continuous positive year-on-year changes (Chart 5). FY 2021-22 in particular has seen a 55% increase, the highest rate of change in past decade. National Informatics Centre, SAMEER, Digital Payments and Promotion of IT/ ITeS Industries have been clear priorities, in terms of quantum of and consistency in budgeted allocations.

However, trends of consistently underutilised funds allocated towards Cyber Security (CERT-In), NCCC and Data Governance and Promotion of Electronics and IT Hardware Manufacturing over the last decade requires examination. There are also instances of unavailable actual expenditure data for allocations that are made under MeitY. For example, in FY 2015-16, Promotion of IT/ITeS Industries receives a budgeted allocation of ₹80cr, a significant eight-fold increase from the previous year. While the revised estimate for this allocation is ₹150cr, data on the actual expenditure incurred is unavailable. Such incomplete records of the union budget limit analysis of trends across financial years and preclude transparency in public expenditures.

(ii) Department of Telecommunications (DoT)

The relevant budget heads under DoT and their changing composition in the total relevant budget for cybersecurity are displayed in Chart 7 and Table 4.

Chart 7: Budgeted Expenditure for Cybersecurity under Department of Telecommunications



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Table 4: Budgeted Expenditures (in ₹ crores) for Relevant Budget Heads under DoT from FY 2012-13 to FY 2022-23

Relevant Budget Heads for Cybersecurity under DoT	FY 2012-13	FY 2013-14	FY 2014-15	FY 2015-16	FY 2016-17	FY 2017-18	FY 2018-19	FY 2019-20	FY 2020-21	FY 2021-22	FY 2022-2023
Centre for Development of Telematics (C-DoT)	215	60	175	140	220	270	260	273	323	326	500
Telecom Regulatory Authority of India (TRAI)	55	57	98	90	63	80	85	90	70	100	226
Wireless Monitoring, Planning and Coordination*	90	80	86	53	56	77	89	79	80	63	76
Telecom Engineering Centre (TEC)	27	65	42	39	10	15	14	20	20	20	15
Human Resource Management (National Institute of Communication Finance)	11	12	15	9	27	50	124	79	59	80	58
Technology Development and Investment Promotion	2	2	1	2	2	4	4	20	10	9	19
5G Connectivity Test Bed	-	-	-	-	-	-	135	39	45	0.01	10
Telecom Testing and Security Certification Centre	-	-	-	-	-	15	27	0.1	10	15	10
Telecom Computer Emergency Response Team	-	-	-	-	-	15	15	15	10	23	32
Telecom Enforcement Resources and Monitoring Cells (TERM)	-	29	58	67	-	-	-	-	-	-	-
Central Equipment's Identity Register (CEIR)	-	-	-	-	-	15	15	15	10	13	13
Promotion of Innovation and Incubation of Future Technologies for Telecom Sector	-	-	-	-	-	-	-	50	20	5	4
South Asia Sub-Regional Economic Cooperation (SASEC) Information Highway Project	-	-	-	-	-	6	-	-	-	-	-
Labour, Employment and Skill Development	-	-	-	-	-	-	5	5	3	4	0.42
Total Budgeted Expenditure for Cybersecurity under DoT	**443**	**305**	**475**	**400**	**378**	**547**	**772**	**684**	**658**	**658**	**962**
Production Linked Incentive (PLI) Scheme to Promote Telecom and Networking Products Manufacturing in India	*Introduced in FY 2022-23*										528
Digital Intelligence Unit	*Introduced in FY 2022-23*										10

Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Minor variations in budgeted allocations from FY 2012-13 to FY 2015-16 are evident (Chart 7) in the cybersecurity allocations under DoT. The average total budgeted allocation during this period is ₹406cr. This is followed by a three-year period of significantly increasing allocations from ₹3,78cr in FY 2016-17 to ₹7,72cr in FY 2018-19. These increasing allocations can be placed in the context of the establishment of the Digital Communications Policy in 2018.[70] The increasing budgeted expenditures during this period are also driven by introduction of the 5G Connectivity scheme and increased allocations for Human Resource Management. The introduction of Telecom Testing and Security Certification Centre (TTSCC), Telecom Computer Emergency Response Team (Telecom CERT), Central Equipment's Identity Registry (CEIR) and South Asia Sub-Regional Economic Cooperation Information Highway Project (SASEC) in FY 2017-18 are also important during this period. From FY 2019-20, we note marginally decreasing total budgeted allocations until FY 2021-22. While MeitY and MHA both see reduced total budgeted allocations for cybersecurity in FY 2022-23 from the previous year, we note a significant 32% increase under DoT, from ₹6,58cr in FY 2021-22 to ₹9,62cr in FY 2022-23.

The following are insights from our analysis of the cybersecurity budget under DoT:

- Budgeting priorities for DoT over the last decade, in terms of quantum of allocations, can be located in allocations for C-DoT, Telecom Regulatory Authority of India (TRAI), Telecom Engineering Centre and Wireless Monitoring, Planning and Coordination (Table 4).

- The Telecom CERT, responsible for taking proactive measures against cyber breaches, has received steady allocations since they began in FY 2017-18. However, actual expenditures have been lower than allocations in FY 2017-18 (BE ₹15cr to AE ₹12.5cr) and FY 2020-21 (BE ₹10cr to AE ₹6.5cr). In FY 2021-22, we observe that the budgeted ₹23cr allocation is revised to ₹16cr. Most importantly, **there are instances of incomplete or unavailable budget data on expenditures for Telecom CERT** in FY 2016-17 (in which a revised expenditure of ₹0.5cr is presented without any actual or budgeted

[70] National Digital Communications Policy 2018 <https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf>.

expenditures) and in FY 2019-20 (in which a BE of ₹15cr is made but data on revised and actual expenditures is unavailable).

- **There are more instances of allocations for which data on actual spending is unavailable.** FY 2015-16 is a case in point where TERM (BE ₹67cr to unavailable AE)[71] and C-DoT (BE ₹140cr to unavailable AE)[72] both have significant budgeted expenditures but no data on actual expenditures under DoT's Demand for Grants. Further, in FY 2018-19, we note the absence of data on budgeted expenditures for TERM and SASEC. While budgeted expenditures for CEIR (₹15cr) exist in FY 2018-19, data for actual spending under this budget head is unavailable.

- **A steep decline in allocations for 5G connectivity testing since FY 2018-19** is noted. This may be due to the contested delays in commencement of trials,[73] that the government has attributed to the circumstances of the pandemic. However, a systemic factor that may be linked to the delays in roll-out and deployment of 5G services may be attributable to the challenging financial health of India's telecom sector.[74] Over the years, the poor health of the Indian telecom sector has manifested in extensive litigation on matters relating to the quantum of licensed service providers' dues to the Government

[71] Value unavailable in the DoT's Demand for Grants for FY 2015-16
[72] Value unavailable in the DoT's Demand for Grants for FY 2015-16
[73] 'Panel slams DoT for delay in 5G trials' (The Hindu, 8 February 2021) <https://www.thehindu.com/business/panel-slams-dot-for-delay-in-5g-trials/article33786016.ece>
[74] "Issues around Telecom Industry's Health Even More Relevant Now; Viability a Must: COAI" (*World News,* June 3, 2021) <https://article.wn.com/view/2021/06/03/Issues_around_telecom_industrys_health_even_more_relevant_no_p/>

of India,[75] enormous debt[76] and falling revenues for telecom service providers, that comes with consequential concerns about financial viability.[77] There have also been issues around the consolidation of firms within India's telecom sector,[78] and the government's approach to auctioning prices of spectrum for the roll-out of 5G services.[79] In FY 2021-22, the DoT finally commenced 5G trials between major telecom operators, trusted Original Equipment Manufacturers (OEM) and other solution providers.[80] These trials were scheduled for six months till November 26, 2021. However, after requests from

[75] *Union of India v Association of Unified Telecom Service Providers of India*, M.A. (D) No. 9887 OF 2020 In Civil Appeal Nos.6328-6399 OF 2015, Judgment dated 1st September 2020, <https://main.sci.gov.in/supremecourt/2020/9887/9887_2020_32_1501_23776_Judgement_01-Sep-2020.pdf> ; *Union of India v Association of Unified Telecom Service Providers of India and Ors*, M. A. No.83 of 2021 In M. A. (Diary) No.9887 of 2020 In Civil Appeal Nos. 6328-6399 of 2015, Order dated 23rd July 2021, <https://main.sci.gov.in/supremecourt/2021/5/5_2021_36_1501_28814_Judgement_23-Jul-2021.pdf>
"AGR Case of Telecom Majors: A Timeline" (*The Indian Express,* July 23, 2021) <https://indianexpress.com/article/business/agr-case-sc-to-pronounce-verdict-on-telcos-plea-seaking-modification-of-dues-soon-7416935/#:~:text=October%202019%3A%20SC%20upholds%20the,to%20clear%20their%20AGR%20dues>

[76] "Telcos' Debt to Rise to Rs 4.7 Lakh Crore by 2022 despite Tariff Hikes, Says ICRA" (*Business Today,* 21st December 2020) <https://www.businesstoday.in/industry/telecom/story/telecom-companies-debt-to-rise-by-march-2022-despite-tariff-hikes-says-icra-282110-2020-12-21>
Prasad GC, "Centre Rolls Out Lifeline for Debt-Ridden Telecom Sector" (Mint, September 16, 2021) <https://www.livemint.com/news/india/cabinet-clears-relief-package-for-stressed-telecom-sector-11631701994309.html>
Bloomberg AM, "Opinion: Vodafone Example of 'Most Painful Market in World' for Telecoms" (*NDTV,* July 30, 2021) <https://www.ndtv.com/opinion/opinion-vodafone-example-of-most-painful-market-in-world-for-telecoms-2498393>

[77] *Union of India v Association of Unified Telecom Service Providers of India*, M.A. (D) No. 9887 OF 2020 In Civil Appeal Nos.6328-6399 OF 2015, Judgment dated 1st September 2020, at para.32, p.41, <https://main.sci.gov.in/supremecourt/2020/9887/9887_2020_32_1501_23776_Judgement_01-Sep-2020.pdf>; CP Chandrasekhar Ghosh, "The Rising Spectre of a Telecom Monopoly" (*The Hindu Business Line,* August 23, 2021) <https://www.thehindubusinessline.com/opinion/columns/c-p-chandrasekhar/the-rising-spectre-of-a-telecom-monopoly/article36063279.ece>

[78] Competition Commission of India, "Market Study on the Telecom Sector in India", Para 8 <https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-Study-on-the-Telecom-Sector-In-India.pdf>; Pandey P, "A Year of Consolidation for Indian Telecom Industry" (*The Hindu* December 25, 2018) <https://www.thehindu.com/business/Industry/a-year-of-consolidation-for-indian-telecom-industry/article25821617.ece,>; Tele-Talk by Sonam Chandwani, "Resilience, Re-Consolidation and Reality of the Telecom Sector in India" (*ET Telecom*) https://telecom.economictimes.indiatimes.com/tele-talk/resilience-re-consolidation-and-reality-of-the-telecom-sector-in-india/4895.

[79] Aulakh G, "5G Spectrum Reserve Prices May Be Cut in Relief to Telcos" (*Mint* January 7, 2022) <https://www.livemint.com/industry/telecom/5g-spectrum-reserve-prices-may-be-cut-in-relief-to-telcos-11641570425324.html>

[80] "Airtel, VI, Jio, MTNL given Permission to Conduct 5G Trials: Govt" (*Business Today*) <https://www.businesstoday.in/industry/telecom/story/airtel-vi-jio-mtnl-given-permission-to-conduct-5g-trials-govt-321497-2022-02-04>

industry relating to a lack of *industry readiness*, the DoT granted a six-month extension till May 26, 2022.[81]

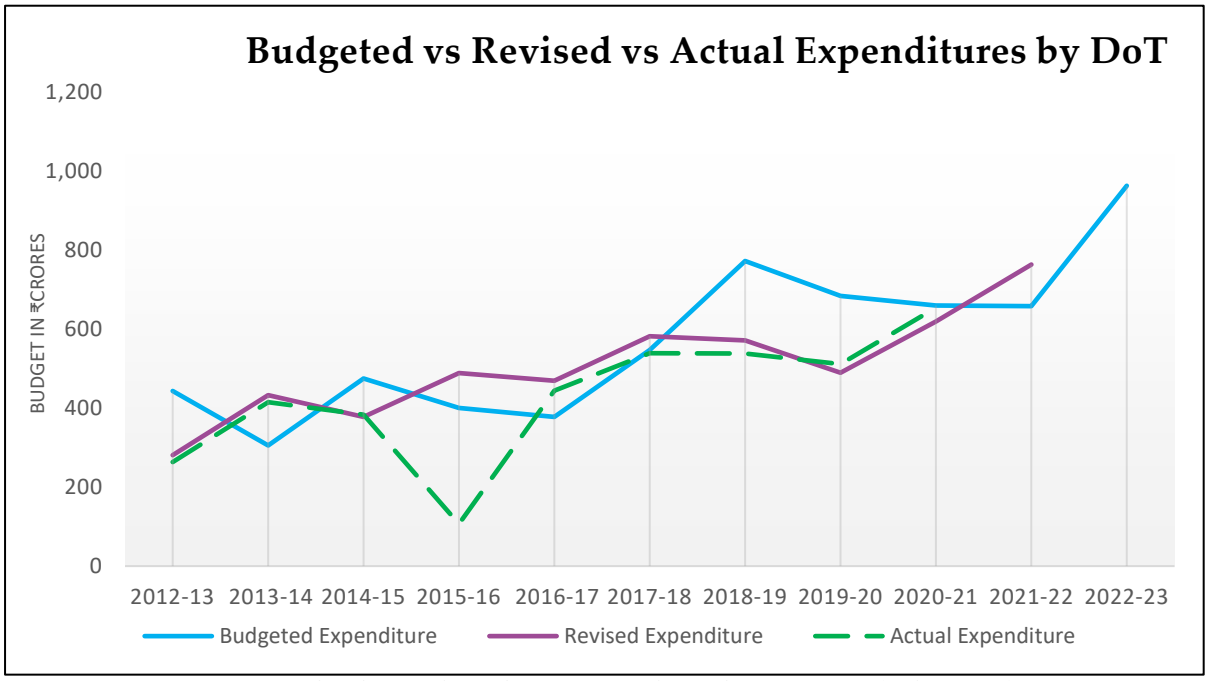
- **There is an absolute lack of allocations for the Telecom Testing and Security Certification Centre (TTSCC) in FY 2019-20 and decreasing allocations for the Incubation of Future Technologies since FY 2019-20**. In the FY 2022-23 Budget Speech, it is stated that the Government of India will conduct the auction for spectrum bands in 2022 to facilitate "roll-out" of 5G telecom services in 2022-23.[82] The Finance Minister's Speech also makes a reference to incentives within the Government of India's Production-linked Incentives (PLI) scheme in order to encourage design-led manufacturing of 5G infrastructure.[83] In August 2022, the government conducted a 5G spectrum auction with bids from industry worth Rs. 1,50,173cr for 71% of the total 5G airwaves.[84] As such, allocations to support testing, security certification and incubation of 5G technologies will be important in the future.

- A positive note is the larger average allocations for Human Resource Management since FY 2018-19 compared to all previous years.

- Budgeting priorities for DoT over the last decade, in terms of quantum of allocations, can also be located in allocations for C-DoT, Telecom Regulatory Authority of India (TRAI), Telecom Engineering Centre (TEC) and Wireless Monitoring, Planning and Coordination (Table 4).

[81] "Dot Gives a Six-Month Extension to Conduct 5G Trials" (*The Hindu Business Line* November 10, 2021) <https://www.thehindubusinessline.com/news/national/dot-gives-a-six-month-extension-to-conduct-5g-trials/article37418017.ece>
[82] "Budget 2022-2023", Para 82 <https://www.indiabudget.gov.in/doc/Budget_Speech.pdf>
[83] "Budget 2022-2023", Para 83 <https://www.indiabudget.gov.in/doc/Budget_Speech.pdf>
[84] Ians, "5G Spectrum Auction: Which Telco Got What, What Bands Were Sold the Most" (Business Standard News August 1, 2022) <https://www.business-standard.com/article/current-affairs/5g-spectrum-auction-which-telco-got-what-what-bands-were-sold-the-most-122080101662_1.html>

Chart 8: Budgeted vs Revised vs Actual Expenditures by Department of Telecommunications



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

- **Chart 8 indicates that on average, actual expenditures have been lower than revised and budgeted expenditures by DoT over the last few years**, especially in the time period between FY 2017-18 and FY 2019-20. The first exception to this trend is in FY 2016-17, where actual spending is greater than the budgeted allocation, in large part due to C-DoT (BE ₹220cr to AE ₹315cr). In FY 2013-14, despite reduced actual spending across other budget heads, the overshoot is due to C-DoT (BE ₹60cr to AE ₹224cr) and Telecom Enforcement Resources & Monitoring Cells or TERM (BE ₹29cr to AE ₹46cr). It is also noteworthy that the significant introduction of allocations for SASEC, TTSCC, Telecom CERT and CEIR in FY 2017-18 fall immediately in subsequent years where there is underutilisation of allocations. It is important for decision makers and researchers to analyse budgeting observations relating to expenditures by two institutions under the DoT– specifically, the TERM Cells and C-DOT.

- While budgeted allocations for TERM Cells increase consistently between FY 2013-14 and FY 2015-16, there is no data available for any expenditures post

this period from FY 2016-17 to FY 2022-23. At a surface level, TERM Cells operate as DoT field offices which are entrusted with monitoring, security and vigilance on behalf of the DoT.[85] This includes ensuring that telecom operators comply with license conditions[86] and cooperating with law enforcement agencies in ensuring the prevention of illegal telecom exchanges using Indian telecom systems.[87] Moreover, according to multiple annual reports of the DoT, there are explicit references that DoT's field offices i.e. TERM Cells are responsible for the implementation of the Central Monitoring System (CMS).[88] CMS[89] is one of India's major technical infrastructures which central and state law enforcement are using/expected to use for automated interception and monitoring of telecommunications activities within the country.[90] CMS has been the subject of litigation and concerns about privacy concerns.[91] It is

[85] Annual Report 2008-2009, Department of Telecommunication, Ministry of Communications and Information Technology, Government of India< https://dot.gov.in/sites/default/files/AR_English_2008-09_0.pdf >.

[86] Annual Report 2020-2021, Department of Telecommunication, Ministry of Communications and Information Technology, Government of India, at p. 84, <https://dot.gov.in/sites/default/files/Annual%20Report%202020-21%20English%20Version.pdf>; PTI, 'Department of Telecom to telcos: Keep TERM cells informed about roaming pacts', (The Economic Times, June 4, 2012) <https://economictimes.indiatimes.com/industry/telecom/department-of-telecom-to-telcos-keep-term-cells-informed-about-roaming-pacts/articleshow/13826241.cms?from=mdr>

[87] Annual Report 2018-2019, Department of Telecommunication, Ministry of Communications and Information Technology, Government of India, at p. 89 <https://dot.gov.in/sites/default/files/Annual%20Report-2018-19%28English%29.pdf>.

[88] Annual Report 2012-2013, Department of Telecommunication, Ministry of Communications and Information Technology, Government of India, at p. 60; <https://dot.gov.in/sites/default/files/Telecom%20Annual%20Report-2012-13%20(English)%20_For%20web%20(1).pdf>; Annual Report 2020-2021, Department of Telecommunication, Ministry of Communications and Information Technology, Government of India, at p. 121 <https://dot.gov.in/sites/default/files/Annual%20Report-2019-20%28%20English%29.pdf>; Annual Report 2018-2019, Department of Telecommunication, Ministry of Communications and Information Technology, Government of India, at p. 103 <https://dot.gov.in/sites/default/files/Annual%20Report-2018-19%28English%29.pdf>.

[89] Government of India, Ministry of Communications a nd IT, Department of Telecommunications, 'Amendment to the Unified License agreement regarding Central Monitoring System, 11 October 2013, <https://dot.gov.in/sites/default/files/DOC231013.pdf?download=1>.

[90] Annual Report 2020-2021, Department of Telecommunication, Ministry of Communications and Information Technology, Government of India, at p. 86, <https://dot.gov.in/sites/default/files/Annual%20Report%202020-21%20English%20Version.pdf>.

[91] Singh SR, "No Blanket Permission given to Any Agency on Surveillance: Centre" (The Hindu February 5, 2021)<https://www.thehindu.com/news/national/no-blanket-permission-given-to-any-agency-on-surveillance-centre/article33762147.ece>
Software Freedom Law Centre, 'CPIL and Anr v. Union of India and Ors – Delhi High Court', <https://sflc.in/legal-challenge-cpil-and-sflcin-surveillance-projects-cms-natgrid-and-netra>,
Khadija Khan, Delhi High Court directs Centre for file detailed reply on procedure followed for monitoring, interception of phones, *Bar and Bench,* 31st August 2021,

notable that the budgeting details of its implementation and enforcement arm is unavailable for public scrutiny.

- **There is a clear importance for allocations towards the Centre for Development of Telematics (C-DoT) under DoT that is reflected in significantly increasing budgets since FY 2015-16.** C-DoT is the nodal technical agency which operates under the Department of Telecommunications and supports the development of next generation wireless 5G solutions and services (especially in concert with MTNL),[92] among other things. C-DoT is also expected to anchor R&D in next frontier wireless domains like 6G and Quantum Computing.[93] However, the consistent rise in funding for C-DoT may relate to its development and deployment work on security-related projects. Among other projects this vertical of C-DoT's work has anchored the development and country-wide deployment of the aforementioned Central Monitoring System.[94] C-DoT's most recent annual report (2020-21) reveals that the institution is currently in the midst of implementing the national roll out project of the CMS.[95] This includes the implementation of law enforcement monitoring facilities by institutions like field offices of the Central Board of Direct Taxes, state police departments, and support and enhancement of technical capabilities of the CMS systems.[96]

<https://www.barandbench.com/news/litigation/delhi-high-court-centre-reply-monitoring-interception-phones-surveillance>,

[92] 'MTNL to carry out 5G trials in Delhi as DoT allocates trial spectrum to govt telco, *India Today*, June 21, 2021, <https://www.indiatoday.in/technology/news/story/mtnl-to-carry-out-5g-trials-in-delhi-as-dot-allocates-trial-spectrum-to-govt-telco-1818776-2021-06-24>, Also see Centre for Development of Telematics (C-DoT), *Annual Report 2020-21* at p. 7, <https://www.cdot.in/cdotweb/assets/docs/annualReports/ANNUAL_REPORT_2020-21.pdf>.

[93] 'Telecom Secretary asks C-DoT to work on 6G, launches Quantum Computing Lab, (*The Economic Times*, October 10, 2021) <https://economictimes.indiatimes.com/industry/telecom/telecom-news/telecom-secretary-asks-c-dot-to-work-on-6g-launches-quantum-communication-lab/articleshow/86910729.cms?from=mdr>.

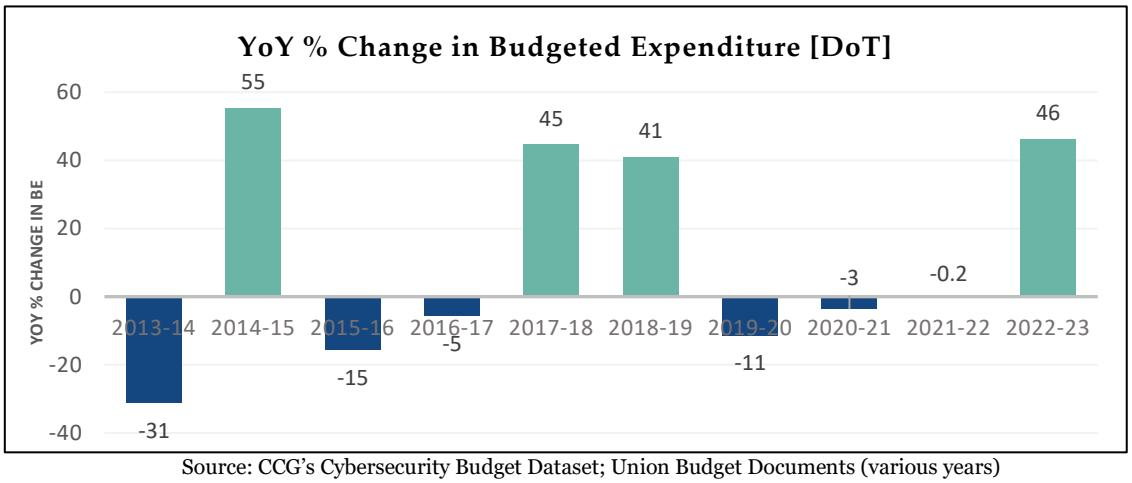
[94] Keerthana Sankaran, 'Big Brother is here: Amid snooping row, govt report says monitoring system 'practically complete'', (*The New Indian Express,* 24 December 2018) <https://www.newindianexpress.com/nation/2018/dec/24/big-brother-is-here-amid-snooping-row-govt-report-says-monitoring-system-practically-complete-1915866.html>.

[95] Centre for Development of Telematics (C-DoT), *Annual Report 2020-21* <https://www.cdot.in/cdotweb/assets/docs/annualReports/ANNUAL_REPORT_2020-21.pdf>.

[96] Centre for Development of Telematics (C-DoT), *Annual Report 2020-21* at p.5 <https://www.cdot.in/cdotweb/assets/docs/annualReports/ANNUAL_REPORT_2020-21.pdf>.

- Taken together, these observations on C-DoT and TERM indicate the need for ensuring availability of budget data and expenditure such as of the TERM Cells, while also highlighting the increase in expenditure to develop the operational capacity of C-DOT including for projects related to interception systems. Trends in expenditure for both these heads under DoT must continue to be mapped in the years to come.

Chart 9: Year on Year Percentage Change in Budgeted Expenditures [DoT]



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

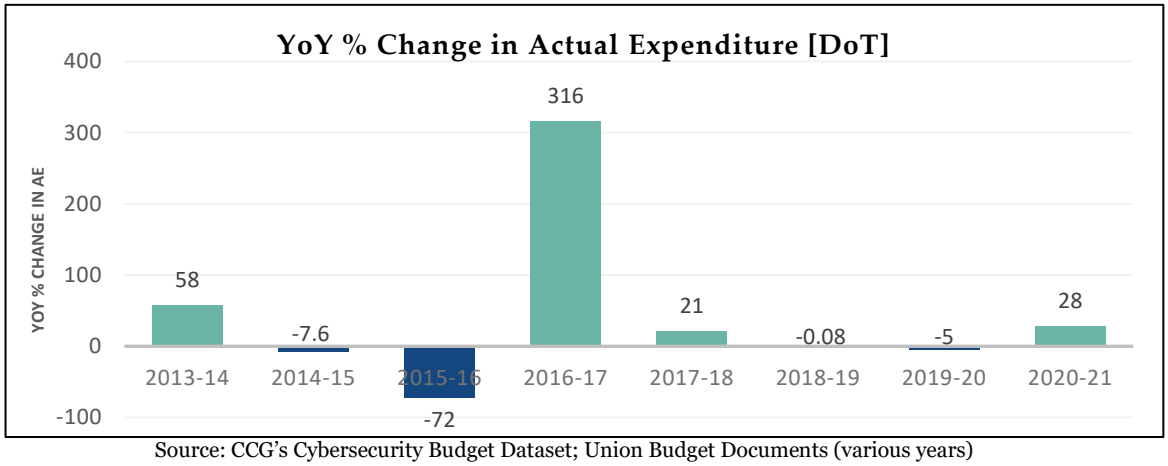
- **This underutilisation of total allocations under DoT can be traced to specific budget heads.** For instance, in FY 2018-19, one year after its introduction, 5G Connectivity Test Bed sees a significant BE of ₹134cr that translates into an AE of ₹59cr. Human Resources Management (BE ₹123cr to AE ₹27cr) and Telecom Engineering Centre (BE ₹14cr to AE ₹0.65cr) also see significant underutilisation of allocations in the same year.

- The year-on-year changes in budgeted expenditures (Chart 9) are further indicative of variability in total budgeted allocations for cybersecurity under DoT across financial years in the last decade. There have been alternating periods of significant increases - largely driven by C-DoT and TERM in FY 2014-15; the new budget heads introduced in FY 2017-18; and Human Resources Management and 5G Test Bed in FY 2018-19 - that are followed by periods of decreased allocations.

- **Wireless Monitoring, Planning and Coordination also has substantially lower actual expenditures from revised and budgeted expenditures in every year since FY 2012-13**. The underutilisation of funds for Wireless Monitoring, Planning & Coordination is most prominent in earlier years. For instance, in FY 2014-15, a BE of ₹86cr manifests in actual spending that is less than half this allocation at ₹37cr. The gaps between actual and budgeted expenditures reduce in later years. For instance, in FY 2019-20 a BE of ₹79cr sees an actual expenditure of ₹52cr. The activities carried out under this allocation currently include monitoring observations for radio frequency management and enforcement of national and international radio regulations under the Indian Telegraph Act (1885).

- The large percentage changes in actual expenditures for FY 2015-16 (-72%) and FY 2016-17 (316%) in Chart 10 are due to **high variations in spending by C-DoT.** Wireless Monitoring, Planning and Coordination has also been a budgeting priority for DoT but has seen average actual spending fall short of allocations since FY 2013-14.

Chart 10: Year on Year Percentage Change in Budgeted Expenditures [DoT]



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

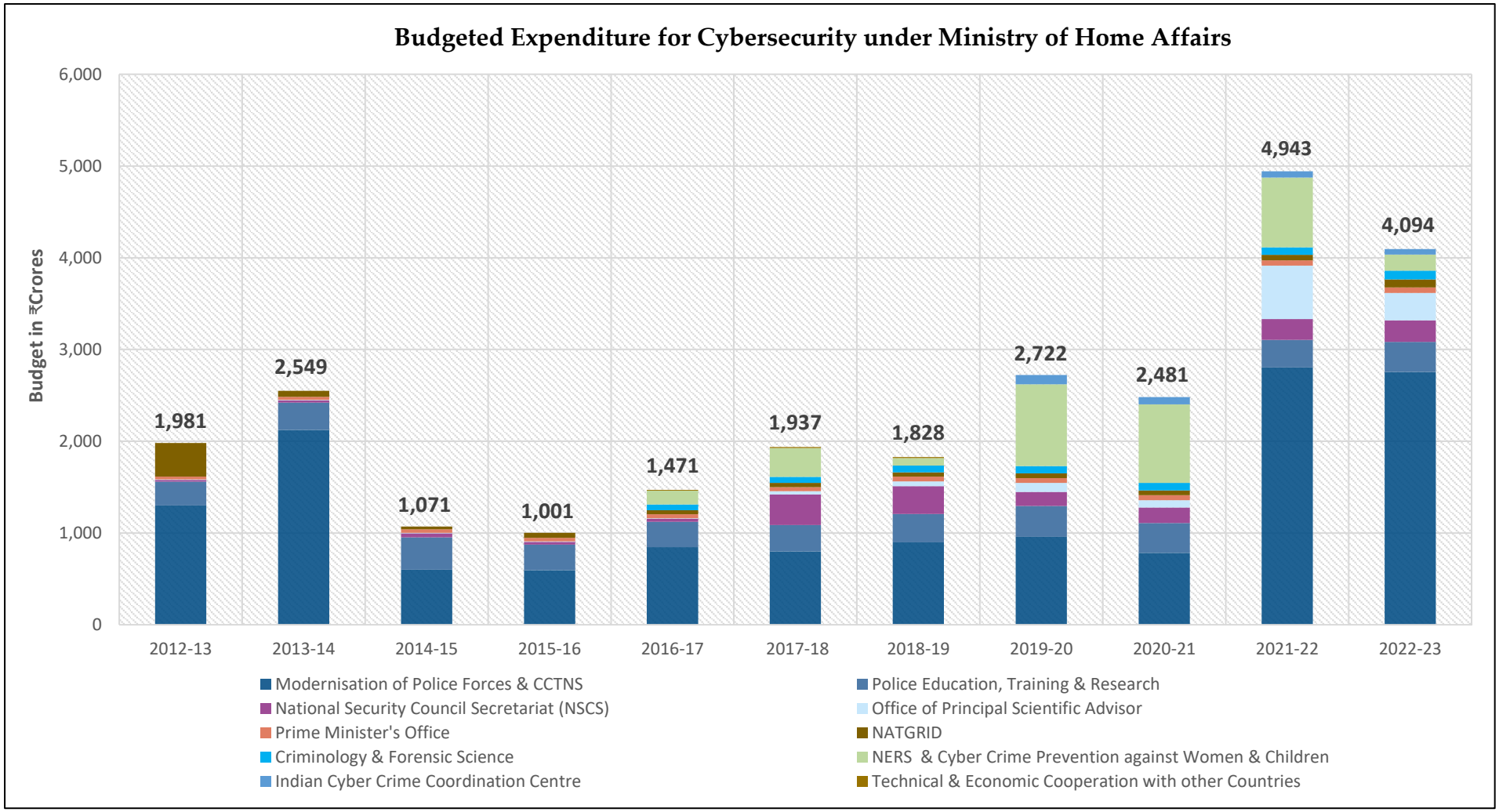
In sum, DoT has seen significant underutilisation of resources and variation in budgeting through the years, with particularly fluctuating spending under C-DoT. The lack of data that tracks budgeted allocations, their revised estimated and actual spending is also evident in the case of Telecom CERT, TERM, SASEC and CEIR. Such

cases of absent data blur the lines between underutilisation of funds and problems of monitoring and recording expenditures across schemes, programs and ministries.

(iii) Ministry of Home Affairs (MHA)

The total budgeted expenditures for cybersecurity under MHA over the last decade are displayed in Chart 11. The discrete budget heads that make up the total allocations toward cybersecurity under MHA are further presented in Table 5.

Chart 11: Budgeted Expenditure for Cybersecurity under Ministry of Home Affairs



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Table 5: Budgeted Expenditures (in ₹ crores) for Relevant Budget Heads under MHA from FY 2012-13 to FY 2022-23

Relevant Budget Heads for Cybersecurity under MHA	FY 2012-13	FY 2013-14	FY 2014-15	FY 2015-16	FY 2016-17	FY 2017-18	FY 2018-19	FY 2019-20	FY 2020-21	FY 2021-22	FY 2022-23
National Emergency Response System (NERS) & Cyber Crime Prevention against Women and Children (CCPWC)	-	-	-	-	150	313	82	891	855	760	176
Modernisation of Police Forces & Crime and Criminal Tracking Network Systems (CCTNS)	1,300	2,123	600	595	845	800	897	960	785	669	2754
Office of Principal Scientific Advisor (PSA)	4	5	5	5	5	35	53	99	79	581	300
Police Education, Training & Research	259	297	353	278	278	287	310	335	323	301	330
National Security Council Secretariat (NSCS)	20	26	45	32	33	334	304	153	171	229	233
Criminology & Forensic Science	-	-	-	-	61	68	73	81	81	83	96
Indian Cyber Crime Coordination Centre (I4C)	-	-	-	-	-	-	-	100	80	70	59
National Intelligence Grid (NATGRID)	365	67	30	53	45	46	47	51	52	60	88
Prime Minister's Office	33	32	38	39	44	44	50	53	55	58	58
Technical & Economic Cooperation with other Countries	-	-	-	-	10	11	12	-	-	-	-
Total Budgeted Expenditure for Cybersecurity under MHA	**1,981**	**2,549**	**1,071**	**1,001**	**1,471**	**1,937**	**1,828**	**2,722**	**2,481**	**4,943**	**4,094**
Modernisation of Forensic Capacities	*Introduced in FY 2022-23*										300

Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

There is a significant reduction in total budgeted expenditure for cybersecurity under MHA in FY 2014-15 (largely due to the reduced allocation for Modernisation of Police Forces), after which there is a broad trend of increasing allocations through the years up till FY 2022-23. These increasing allocations are not consistent year-on-year and there are reductions in total allocations in FY 2015-16, FY 2018-19 and FY 2020-21.

The major budgeted allocations under MHA, over the last decade, have been directed towards Modernisation of Police Forces and Crime and Criminal Tracking Network Systems (CCTNS) and Education, Training and Research of Police. The security of information systems and upskilling of police forces is critical to maintain the integrity of prosecution processes and national security, particularly in light of digitisation of records. The consistent funds allotted for these two specific budget heads are largely realised in actual expenditures that are rarely far off from budgeted expenditures. However, data on the exact portion of these budgeted allocations being dedicated to cybersecurity is unavailable.

The following are insights from our analysis of the cybersecurity budget under MHA:

- FY 2016-17 sees introduction of allocations for Criminology and Forensic Science and National Emergency Response System and Cyber Crime Prevention against Women and Children (NERS & CCPWC) – both of which see increasing allocations in the following years up till FY 2021-22. An exception to this trend is a decrease in allocations for NERS & CCPWC in FY 2018-19 by 74% from the previous year.

- Technical and Economic Cooperation with other countries is also introduced in FY 2016-17, allocations for which are sustained for two years after this until FY 2018-19. After FY 2018-19, there no allocations are made towards this budget head. Further, it is important to note that **allocations towards Technical and Economic Cooperation with other countries are not revised or translated into actual expenditures, during the three-year period they are made.** The only exception is a revised expenditure of ₹0.3cr from a BE of ₹11cr in FY 2017-18, for which no actual spending is recorded in the budget documents.

- **The National Security Council Secretariat (NSCS) received a significant nine-fold increase in budgeted allocations from ₹33cr in 2016-17 to ₹334cr in FY 2017-18, but allocations since then have reduced substantially. Actual spending has also been consistently lower than budgeted allocations for the NSCS** since FY 2012-13, with the exception of FY 2016-17 (where actual spending is ₹39cr, and 17.8% higher than the budgeted allocation of ₹33cr) and FY 2018-19 (where actual spending is ₹812cr, significantly higher than the BE of ₹304cr).

- Allocations to the Principal Scientific Advisor (PSA) increased six-fold from ₹79cr in FY 2020-21 to ₹581cr in FY 2021-22. However, this is followed subsequently by a 93% reduced allocation in FY 2022-23. This reduction marks a break from the increasing budgeted allocations for the PSA since FY 2016-17. Until FY 2016-17, we note that actual spending aligns closely with budgeted and revised expenditures. The budgeted expenditure more than doubles from ₹35cr in FY 2017-18 to ₹99cr in FY 2019-20, but we note that actual expenditures are lower than revised and budgeted expenditures during this two-year period. For instance, in FY 2019-20, a budgeted allocation of ₹98cr is revised to ₹70cr and translates to an actual expenditure of ₹53cr.

- **The utilisation of funds allotted to the National Intelligence Grid (NATGRID) have been low throughout the last decade despite incremental increases in budgeted allocations since FY 2016-17.** We observe that actual spending has been less than half of budgeted allocations, on average, for this budget head from FY 2012-13 to FY 2019-20. The most significant case in point is the budgeted expenditure of ₹365cr in FY 2012-13 that is revised to ₹11cr and translates into an AE of ₹10cr. In FY 2015-16, the ₹53cr budgeted expenditure is revised to ₹17cr and sees an actual spending of ₹15cr. Similarly, in FY 2018-19, the budgeted allocation of ₹47cr is revised to ₹30cr and followed by an actual spending of ₹23cr. The constitutionality of certain information systems, including NATGRID, has been challenged on grounds of privacy at the Delhi High Court. The government has defended the legality of such systems by arguing that

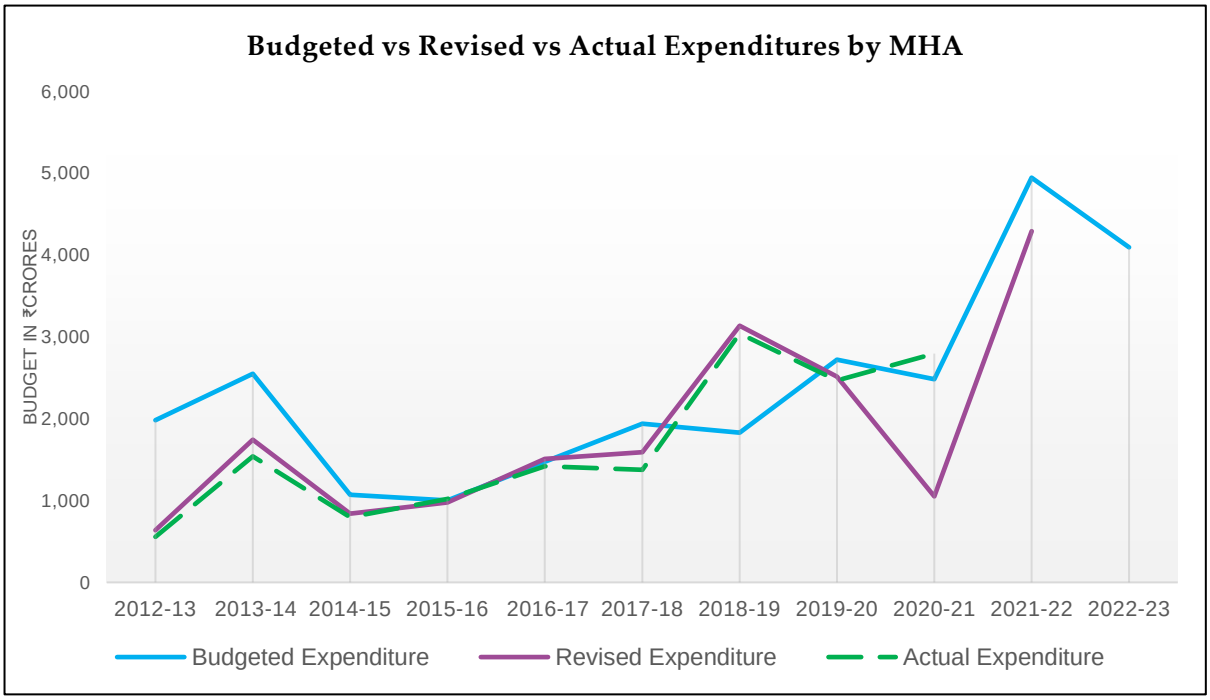
blanket permissions are not granted to agencies for real-time profiling of citizens.[97]

- **In the context of underutilisation of allocations by NATGRID, over the last decade we observe a pattern of increasing year-on-year actual expenditures** for short periods that are followed by consecutive decreases in year-on-year spending. For instance, we note decreasing actual expenditures in FY 2015-16 (-4% from FY 2014-15) and FY 2016-17 (-5.4% from FY 2015-16). This is followed by consecutive increasing actual expenditures in FY 2017-18 (27% from FY 2016-17) and FY 2018-19 (21% from FY 2017-18). This alternating trend holds for actual expenditures under NATGRID over the last eleven years.

- From FY 2020-21 to FY 2022-23, we observe that revised expenditures for NATGRID are significantly higher than budget allocations. In FY 2020-21, a budgeted allocation of ₹52cr is revised to ₹101cr but actual expenditures are much lower than both these values at ₹36cr. Similarly, in FY 2021-22, the revised expenditure for NATGRID at ₹78cr exceeds the budgeted allocation of ₹60cr and data on actual expenditure will be made available in the Union Budget 2023-24. **It is clear that NATGRID has been a priority for the government, in terms of consistent and increasing allocations however, there has been significant underutilisation of funds over the last decade.**

[97] Singh SR, "No Blanket Permission given to Any Agency on Surveillance: Centre" (*The Hindu* February 5, 2021) <https://www.thehindu.com/news/national/no-blanket-permission-given-to-any-agency-on-surveillance-centre/article33762147.ece>

Chart 12: Budgeted vs Revised vs Actual Expenditures by Ministry of Home Affairs

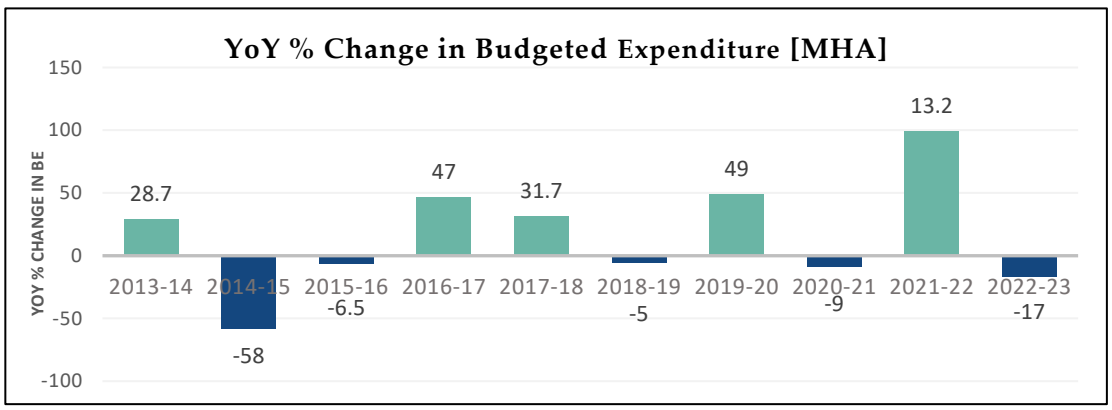


Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

- Chart 12 displays spending patterns for cybersecurity by MHA in terms of budgeted, revised and actual expenditures over the years. The presence of sharp V-shaped curves along the graph is indicative of (a) underutilisation of funds (where AE < BE) and (b) unforeseen expenditures (where AE > BE).

- In FY 2017-18, there is significant disparity between budgeted and actual expenditures for National Security Council Secretariat (BE ₹333cr to AE ₹61cr) and NERS & CCPWC (BE ₹313cr to AE ₹81cr).

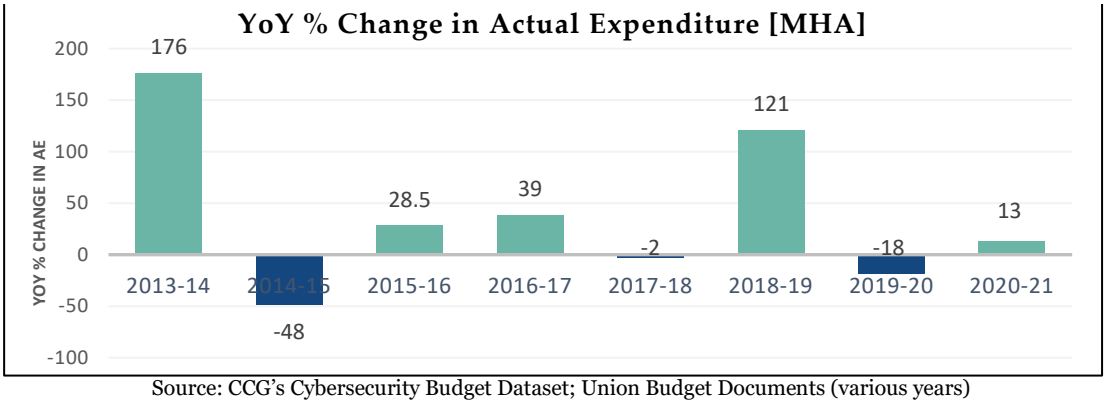
Chart 13: Year on Year Percentage Change in Budgeted Expenditures [MHA]



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Subsequently in FY 2018-19, it is the same budget heads that see higher revised and actual expenditures (NSCS: BE ₹304cr to RE ₹842cr and AE ₹812cr and NERS & CCPWC: BE ₹82cr to RE ₹872 and AE ₹848cr), leading to an overshoot of the budgeted allocation. Further, in its introduction in FY 2019-20, the Indian Cybercrime Coordination Centre (I4C) sees a BE of ₹100cr cut down to a RE of ₹46cr and finally only ₹0.7cr in actual spending.

Chart 14: Year on Year Percentage Change in Actual Expenditures [MHA]



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

While it is clear that NERS & Cyber Crime Prevention against Women and Children (CCPWC), Modernisation of Police Forces & CCTNS and National Security Council Secretariat (NSCS) have been priority areas for MHA, we note that overall allocations under MHA have seen fluctuation over the years, primarily due to variations in actual spending for the abovementioned budget heads and the introduction of new budget heads in FY 2016-17 that took place.

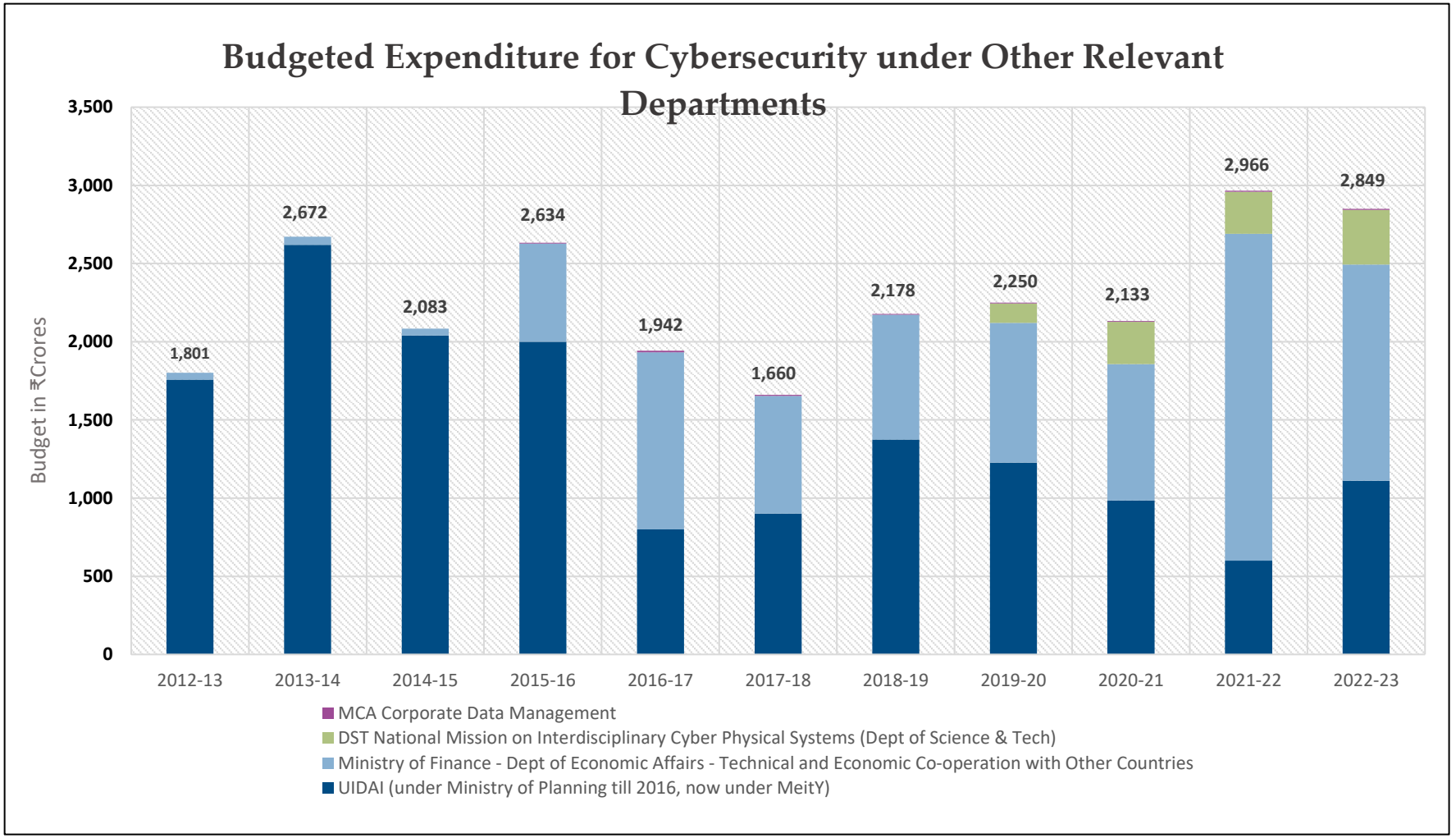
(iv) Other Relevant Departments

Under this category, we classify four budget heads from different government ministries that are relevant for cybersecurity. These include (1) Technical and Economic Co-operation with Other Countries under the Ministry of Finance's Department of Economic Affairs (2) UIDAI under MeitY (3) National Mission on Interdisciplinary Cyber Physical Systems under the Department of Science and Technology and (4) Corporate Data Management under the Ministry of Corporate

Affairs. A detailed explanation for the relevance of each of these four budget heads can found in Volume II Annexure I appended to this brief.

The total budgeted allocations towards the four identified relevant departments have been presented in Chart 15. The data for the budgeted expenditure for cybersecurity under these four relevant departments is also displayed in Table 6. The following are key insights from our analysis of the cybersecurity budget under this category:

Chart 15: Budgeted Expenditure for Cybersecurity by Other Relevant Departments



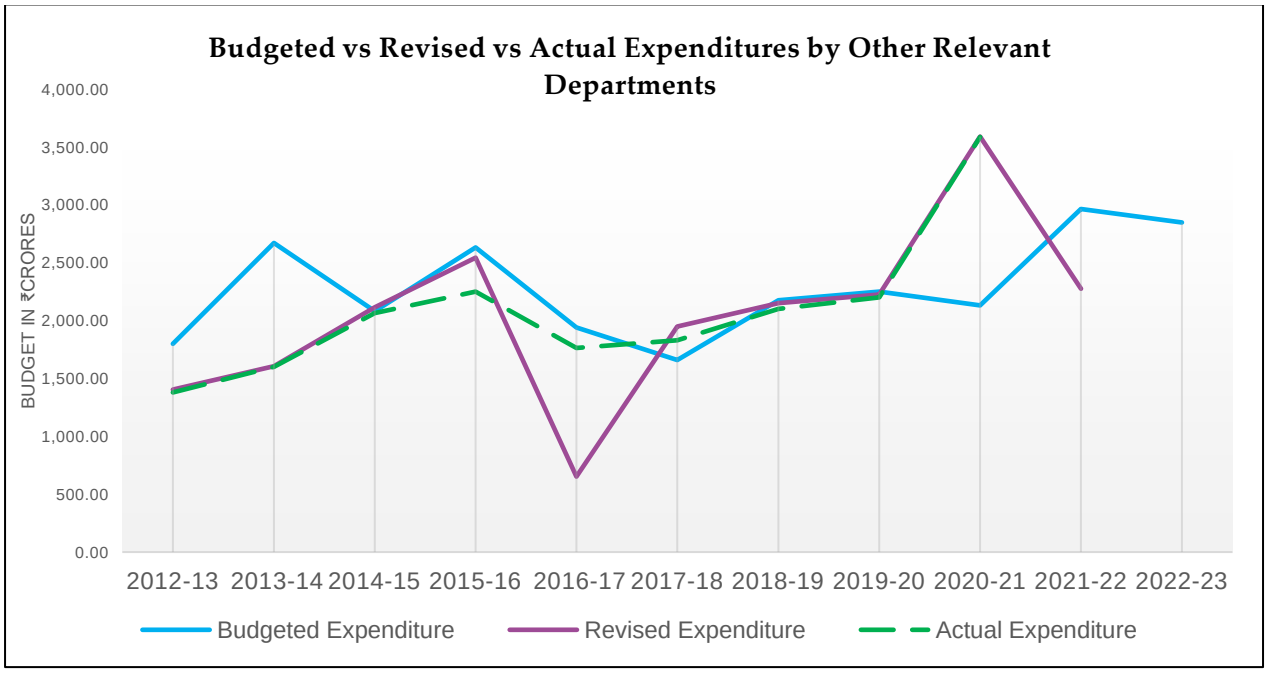
Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Table 6: Budgeted Expenditures (in ₹ crores) for Other Relevant Departments from FY 2012-13 to FY 2022-23

Other Relevant budget heads for Cybersecurity	FY 2012-13	FY 2013-14	FY 2014-15	FY 2015-16	FY 2016-17	FY 2017-18	FY 2018-19	FY 2019-20	FY 2020-21	FY 2021-22	FY 2022-23
Ministry of Finance - Department of Economic Affairs - Technical and Economic Co-operation with Other Countries	43	52	44	629	1132	754	797	894	871	2,090	1,383
UIDAI (under the Ministry of Planning till 2016, now under MeitY)	1,758	2,620	2,040	2,000	800	900	1,375	1,227	985	600	1,110
Department of Science and Technology - National Mission on Interdisciplinary Cyber Physical Systems	-	-	-	-	-	-	-	124	271	270	350
Ministry of Corporate Affairs - Corporate Data Management	-	-	-	5	10	6	6	6	6	7	6
Total Budgeted Expenditure for Cybersecurity under Other Relevant Departments	**1,801**	**2,672**	**2,083**	**2,634**	**1,942**	**1,660**	**2,178**	**2,250**	**2,133**	**2,966**	**2,849**

Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Chart 16: Budgeted vs Revised vs Actual Expenditures by Other Relevant Departments



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

The government's flagship UIDAI programme has seen average reduction in allocations since FY 2013-14. There is a significant decrease in budgeted allocations in FY 2015-16, after which allocations remain steady. It is important to note that the exact share of total allocations towards UIDAI being utilised for cybersecurity is unavailable. The sharp dip in revised expenditures for FY 2016-17 is due to unavailable data for UIDAI's revised expenditure in budget documents. The encryption of citizens' personal data in the Central Identities Data Repository (CIDR) and Personal Identity Data (PID) block, network security between authorisation bodies such as the Authentication User Agency (AUA) and e-KYC User Agency (KUA), auditing and storage provisions of metadata, and Aadhar verification systems all entail a critical cyber security component.[98] Tracking allocations for the maintenance and security of such supporting systems in the coming years will be important.

The budget for **National Mission on Interdisciplinary Cyber Physical Systems, introduced in FY 2019-20, has since seen alignment of actual expenditure with budgeted allocations and increasing allocations** as well.

[98] UIDAI, "Ecosystem of Aadhar" (*Unique Identification Authority of India | Government of India*) <https://uidai.gov.in/ecosystem/uidai-ecosystem.html>

In FY 2021-22, we note a budgeted expenditure of ₹270cr, for which data on the revised estimate is unavailable in the Union Budget 2022-23. Nevertheless, allocations have increased by 29.6% from ₹270cr in FY 2021-22 to ₹350cr in FY 2022-23.

Allocations for Corporate Data Management have remained at a ₹6cr average after its introduction in FY 2015-16. While actual spending has been less than budgeted allocation up till FY 2017-18, actuals consistently exceed the budget in subsequent years.

There is a significant boost in spending for Technical and Economic Cooperation with other countries (BE ₹44cr to AE ₹449cr) in FY 2014-15, after which budgeted and actual expenditures increase incrementally. In FY 2021-22, this budget head receives a significant allocation of ₹2,090cr, after which allocations reduce in FY 2022-23 to ₹1,383cr. Actual spending has aligned closely with allotted budgets in previous years. Given the overall increase in budgeted allocations for Technical and Economic Co-operation with other countries over the last decade, it appears that this is an area of focus for the government. This allocation enables India's engagement with and participation at international summits such as the G20, BRICS, OECD and World Economic Forum (WEF).[99] Wide ranging efforts from developing secure communication infrastructure to advancing digital inclusion for women, youth and Small Medium Enterprises (SMEs), and assessing risks of new emerging technologies in financial systems are undertaken at these global fora.[100] For example, India advanced the "use of digital solutions for healthcare, a cyber secured world and measures to strengthen resilience of businesses" at the 2020 Riyadh G20 summit's Digital Economy Task Force.

[99] International Economic Relations Division: Department of Economic Affairs: Ministry of Finance: Government of India" (International Economic Relations Division, Department of Economic Affairs, Ministry of Finance, Government of India) <https://dea.gov.in/divisionbranch/international-economic-relations-division>

[100] Annual Report, Ministry of Finance (2019-2020)" <https://dea.gov.in/sites/default/files/Annual%20Report%202019-2020%20%28English%29.pdf>

PART IV: Activity Wise Analysis

In this section, we recategorise the budget heads identified under relevant departments' ministries from Part III, under six activities that have diverse cybersecurity dimensions. These include:

(1) Cyber Incident Preparedness and Response: This activity comprises improving management and response to cyber attacks, threats and incidents to minimise their impact in terms of monetary and data losses. Improving capacities to anticipate, assess and act on risks in the cyber domain form a key component of this activity.

(2) Technical Research and Capacity Development: Efforts towards research and innovation in cyber security technologies as well as promotion of infrastructure production form the backbone of a secure cyber ecosystem. Research and development of electronics, information security and emerging technologies are included under the ambit of this activity.

(3) Human Resource Development: Ensuring security of information and networks requires people in the cyber ecosystem to have awareness and knowledge on best practices and security standards, be equipped with technical tools and follow systematised protocols in the event of a cyber attack. This component thus involves promotion of skills and qualifications among people that foster a culture of cyber security to strengthen cyber security at the national and organisational level. Programmes and departments that undertake training of human resources towards this end have a critical role in development of the country's cyber security and have been included under this activity for our analysis.

(4) International Co-operation and Investment Promotion: In order to promote a free, open and secure cyberspace, co-operation with international partners, organisations and other countries is essential. Efforts made in this direction can help balance the country's national security interests and economic prospects globally. Investments for building infrastructure to share information with other countries on criminal and

malicious cyber activity will also ensure prevention and detection of serious cybercrimes in the international sphere.

(5) Standardisation, Testing and Quality Certification (STQC): The standardisation and quality of security standards relies on organisations that can provide consistency and clarity on best practices in cyber security to governments and businesses. This activity comprises the undertaking of security services such as certifications, audits, calibration, testing and training of IT systems for private and public organisations.

(6) Digital Identity: The security and robustness of national digital identification systems is essential to protect sensitive personal information of citizens. With use of cloud technologies for storage of personal and non-personal data, cyber security plays an important role to prevent misuse of information from Digital ID systems.

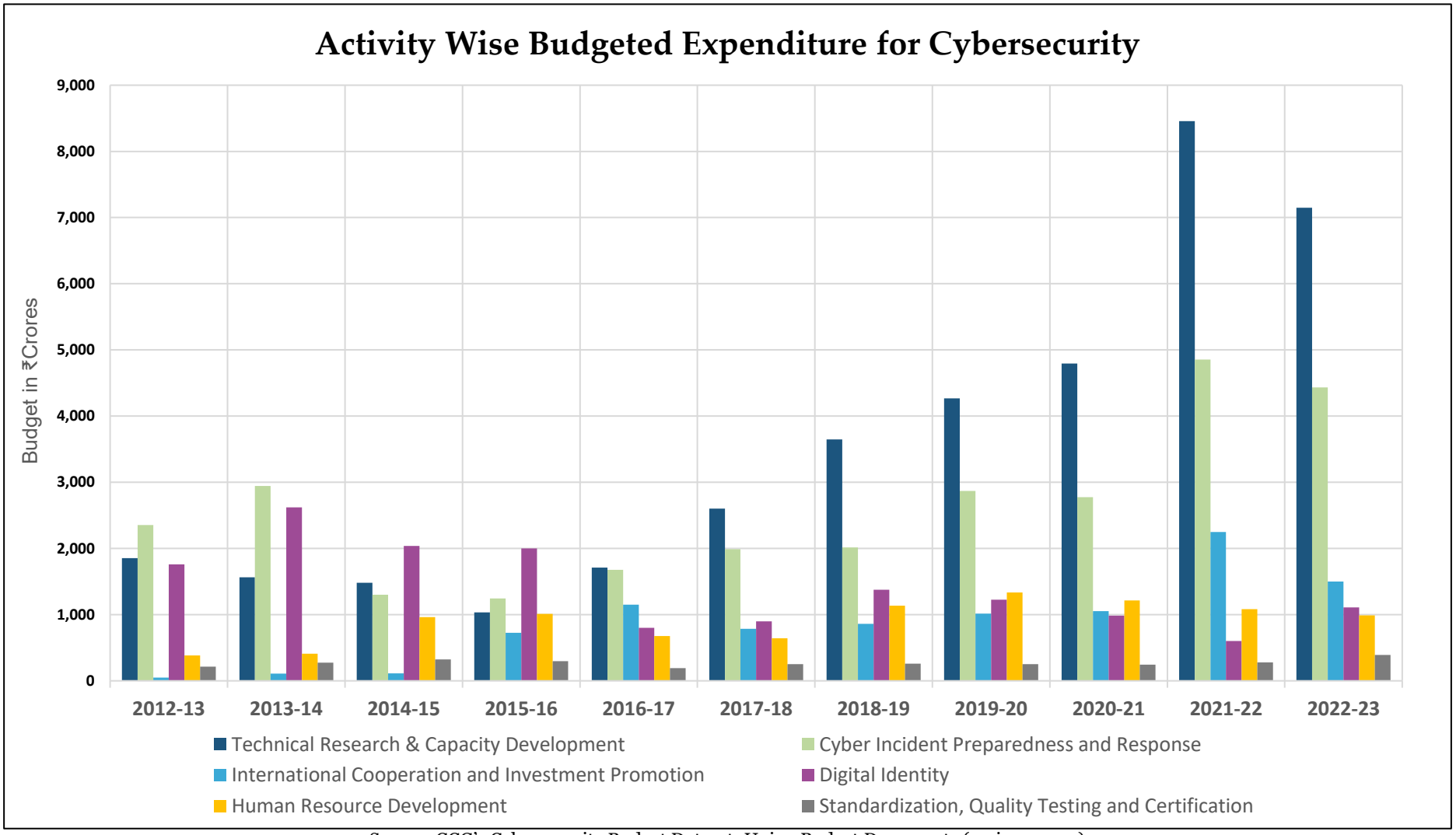
Volume II Annexure I attached to this brief can be referenced for detailed explanations of the rationale for classification of each budget head under a given activity.

Chart 17 displays the activity wise total budgeted expenditures for cybersecurity since FY 2012-13. A clear priority in cybersecurity budgeting over the last decade (in terms of quantum of allocations), has been Technical Research and Capacity Development. This activity has seen significant year-on-year increases in budgeted allocations since FY 2015-16. Efforts towards Human Resource Development, and Standardisation, Testing and Quality Certification (STQC) are concentrated in a select few programs and schemes and funds towards these activities remain consistent over the years. In FY 2022-23, we note that allocations for STQC and Digital Identity increase, despite budgeted allocations for all other four activities reducing.

The underutilisation of funds allocated for cybersecurity across activities is clear from Chart 18, that displays activity wise actual expenditures. The gap between budgeted and actual expenditures (i.e., AE < BE) is less prominent for Cyber Incident Preparedness and Response but holds for Human Resource Development and STQC. There are specific instances where unavailable budget data that tracks how budgeted allocations manifest in revised and actual spending complicates the inferences that can be made from such trends of underutilisation. For Technical Research and

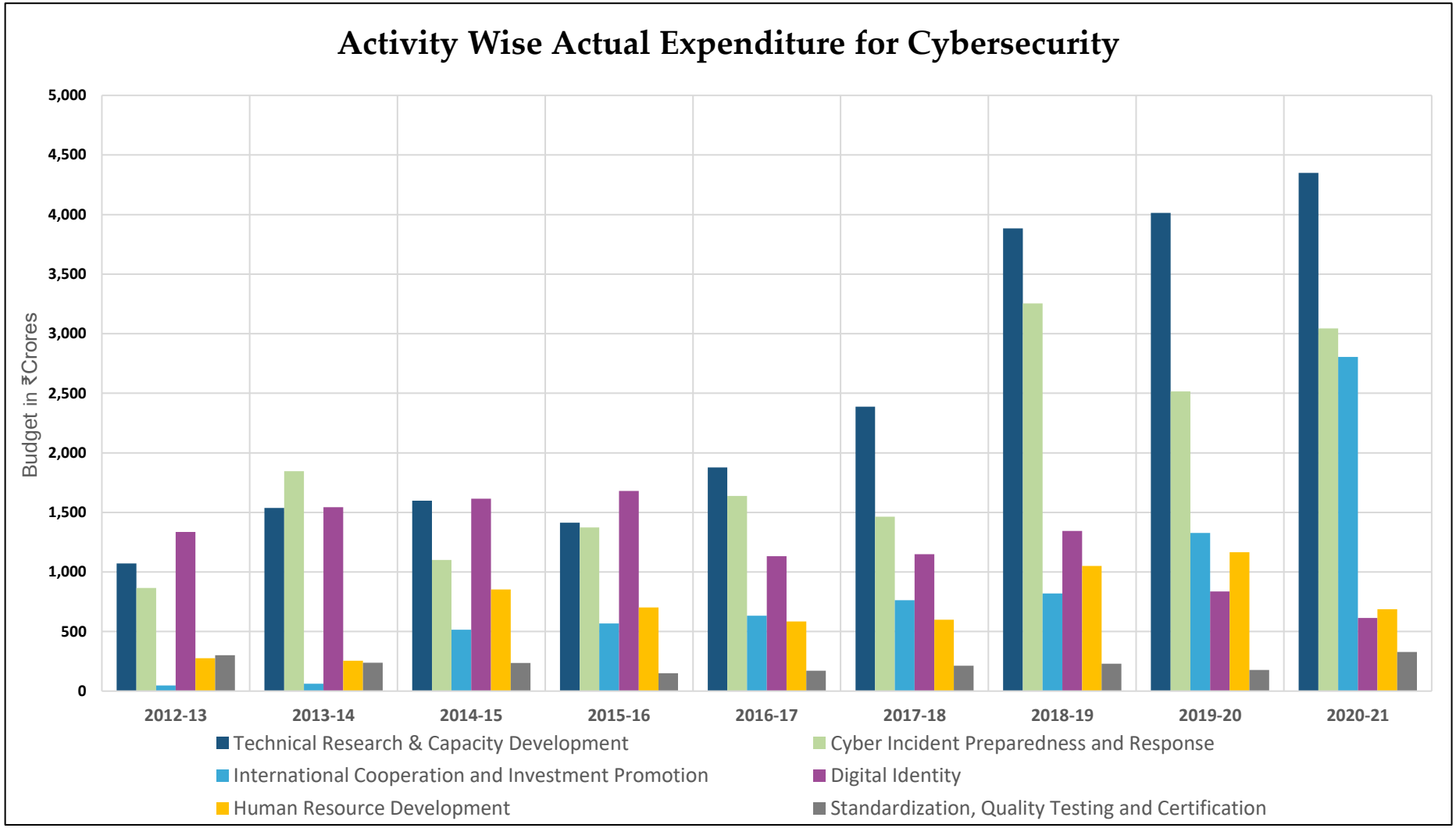
Capacity Development, actual expenditures have most closely converged with allocations albeit with marginal variations. The changes in budgeted, revised and actual expenditures are examined more closely for each activity below.

Chart 17: Activity Wise Budgeted Expenditure for Cybersecurity [FY 2012-12 to FY 2022-23]



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Chart 18: Activity Wise Actual Expenditure for Cybersecurity [FY 2012-13 to FY 2018-19]

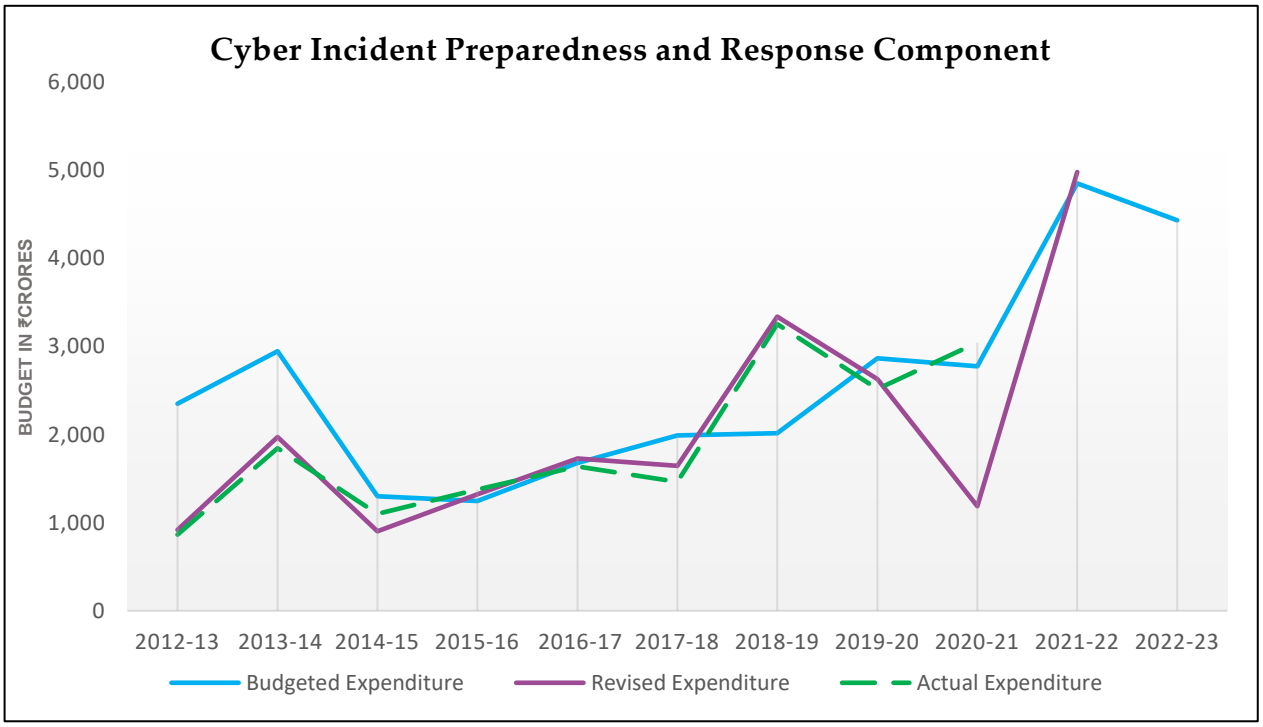


Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

(i) Cyber Incident Preparedness and Response

The Cyber Incident Preparedness and Response component has seen a steady average increase in budgeted allocations from FY 2014-15 to FY 2019-20. From FY2019-20 to FY 2022-23, we note alternating increases and decreases in total allocations. In FY 2019-20, we note a significant increase in allocations for this component - a 42% increase from the previous year. FY 2021-22 has seen the highest allocation yet to this activity at ₹4,852 crores. This significant allocation in FY 2021-22 receives a subsequent reduction by 8% in FY 2022-23 to ₹4,434 crores.

Chart 19: BE vs RE vs AE for Cyber Incident Preparedness and Response Component (FY 2012-13 to FY 2022-23)



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Variations in actual expenditure from these allocations can be seen in FY 2017-18, where there are underutilised funds, and in FY 2018-19, where revised and actual expenditures significantly overshoot the budget.

In FY 2017-18, the largest difference in budgeted and actual expenditures can be seen for National Emergency Response System & Cybercrime Prevention Women &

Children or NERS & CCPWC (BE ₹313cr to AE ₹145cr) and National Security Council Secretariat or NSCS (BE ₹334cr to AE ₹61cr). Cybersecurity Projects under Digital India (BE ₹100cr to AE ₹56cr) and MeitY's Cybersecurity CERT-IN (BE ₹41cr to AE ₹23cr) also see reduced spending in the same year.

In FY 2018-19, it is primarily the exceeding of allocations by NERS & CCPWC (BE ₹82cr to AE ₹849cr) and the National Security Council Secretariat or NSCS (BE ₹304cr to ₹812cr) that lead to the significant overshoot of the budget in this component.

There is a sharp decrease in revised expenditures for FY 2020-21 that comes from reduction in budgeted expenditures across budget heads under this activity. These include NERS & CWPCC (BE ₹855cr to RE ₹209cr), Modernisation of Police Forces (BE ₹785cr to RE ₹107cr), Cybersecurity CERT-IN under MeitY (BE ₹140cr to RE ₹90cr) and Cybersecurity Projects under Digital India (BE ₹170cr to RE ₹80cr). In accordance with these significant reductions in revised estimates, the subsequent total budgeted allocation in FY 2021-22 is reduced by 3.2%. It is relevant to note that these reductions in revised and budgeted expenditures from FY 2020-21 to FY 2021-22 are in the context of the onset of the COVID-19 pandemic, that disrupted economies and governance globally.

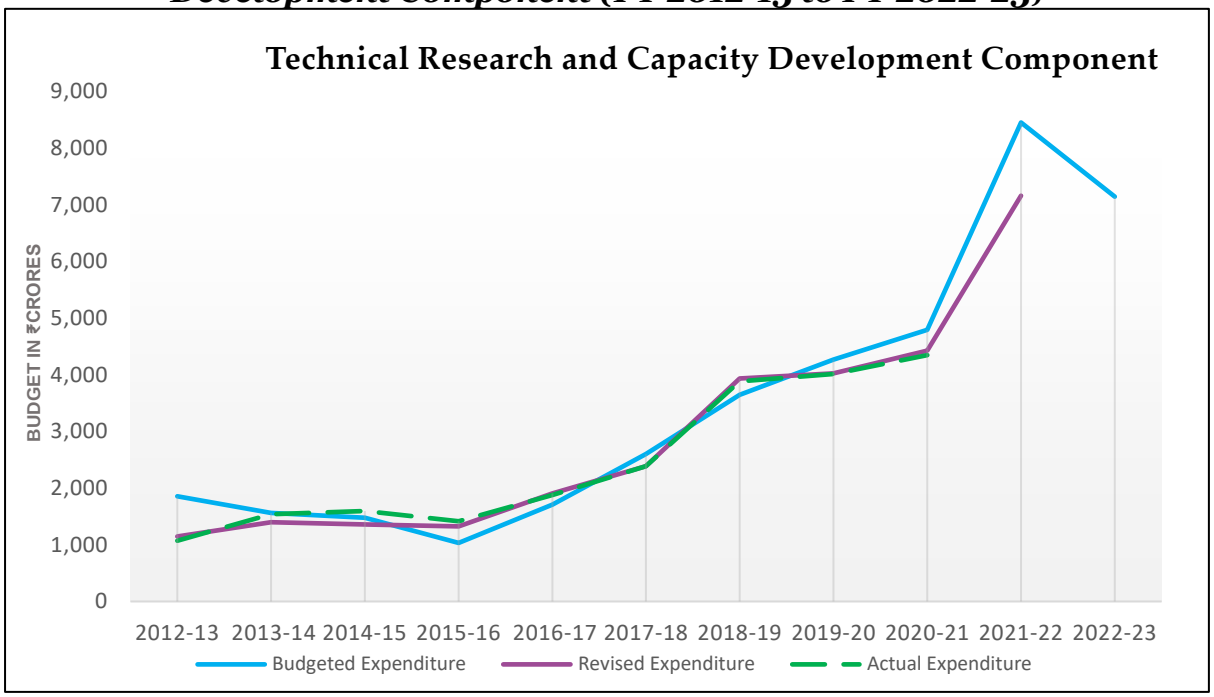
Overall, the Cyber Incident Preparedness and Response component is the second most relevant activity for cybersecurity, in terms of quantum of total budgeted allocations and relative comparison among the six activities in our analysis.

(ii) Technical Research and Capacity Development

Budgeted allocations for Technical Research & Capacity Building have consistently increased since FY 2015-16. Prominently, total budgeted allocations increase from ₹4,793cr in FY 2020-21 to ₹8,455cr in FY 2021-22, a significant 90% increase. In accordance with reduction of the total budget for cybersecurity in FY 2022-23,[101] the total allocations for this activity reduce by 15% from the previous year to ₹7,147cr.

[101] Refer Table 2 on page 25 of this report.

Chart 20: BE vs RE vs AE for Technical Research and Capacity Development Component (FY 2012-13 to FY 2022-23)



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

It is noteworthy that all budget heads under this component see increased budgeted allocations in FY 2020-21. Most substantial increases are noted for Digital Payments, Office of the Principal Scientific Advisor, and Promotion of Electronics and IT Hardware Manufacturing.

However, certain budget heads see substantially reduced allocations in FY 2021-22 from the previous year. These include 5G Connectivity Test Bed scheme (BE of ₹45cr in FY 2020-21 to BE of ₹0.01 in FY 2021-22), R&D in electronics, IT & CCBT under Digital India (BE ₹763cr in FY 2020-21 to BE ₹700cr in FY 2021-22) and Promotion of Innovation and Incubation of Future Technologies for Telecom (BE of ₹20cr in FY 2020-21 to BE of ₹5cr in FY 2021-22).

It is also significant that actual spending has aligned closely with budgeted allocations, particularly in the time period between FY 2016-17 and FY 2019-20. In FY 2021-22, we note that revised expenditures are lower than allocations across budget heads and

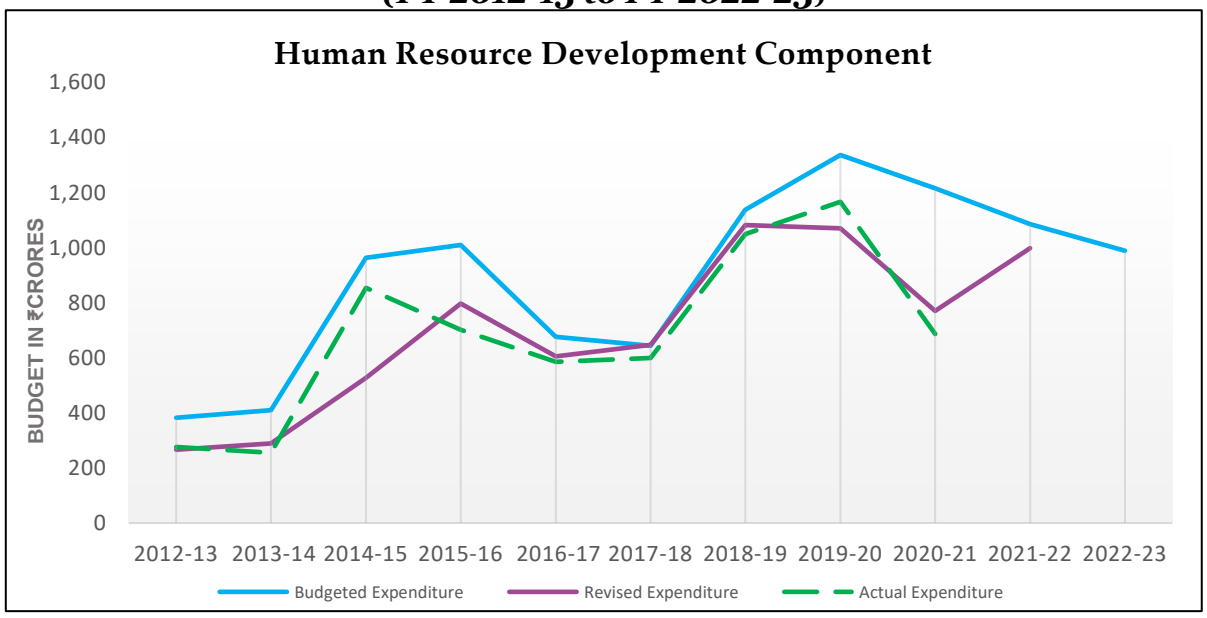
actual spending for this year is expected to match these revisions in accordance with past trends.[102]

Overall, the Technical Research and Capacity Development component is the most significant activity for cybersecurity, in terms of quantum of total budgeted allocations and relative comparison with the other activities in our analysis. This holds true in all financial years over the last decade, except in FY 2013-14 in which Cyber Incident Preparedness and Response exceeds allocations for this component.

(iii) Human Resource Development

Chart 22 indicates that actual spending has been consistently lower than budgeted allocations for Human Resource Development over the years. In FY 2014-15, the boost in allocation and expenditure comes from the Digital India's Manpower Development programme (BE ₹90cr in FY 2013-14 to BE ₹584cr in FY 2014-15) and MHA's Police Education, Training and Research (BE ₹297cr in FY 2013-14 to BE ₹353cr in FY 2014-15).

Chart 21: BE vs RE vs AE for Human Resource Development Component (FY 2012-13 to FY 2022-23)



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

[102] The data on actual expenditures for FY 2021-22 is yet to be released at the time of writing this brief and will become publicly available in the Budget 2023.

From FY 2014-15 to FY 2017-18, we note reducing budgets and spending until the introduction of the Pradhan Mantri Digital Saksharta Abhiyan (PMGDISHA) programme in FY 2017-18 that reinvigorates efforts for Human Resource Development at the ground level. The scheme is aimed at empowering citizens in rural areas by training them to operate computer or digital access devices, with a specific focus on use of digital payments via Common Service Centres and training of on-ground personnel at the panchayat level.

The reduced gap between actual and budgeted expenditures in FY 2017-18 is due to an actual expenditure of ₹100cr under PMGDISHA, for which data on the budgeted allocation at the start of the financial year is unavailable. There is a significant increase in total allocations in FY 2018-19 that comes from increased allocations across all budget heads under this component. Most significantly, Human Resource Management under DoT received more than a two-fold increase in budgeted allocation from ₹50cr in FY 2017-18 to ₹124cr in FY 2018-19.

This period of increasing total allocations from FY 2017-18 to FY 2019-20 is followed by consecutively decreasing budgeted expenditures in the next three financial years.

We further note that revised expenditures are significantly lower than budgeted allocations from FY 2018-19 to FY 2020-21. This is due to reduction in revised expenditures for PMGDISHA, Manpower Development under Digital India and MHA's Police Education, Training and Research.

In FY 2022-23, we note a stark decrease in allocations for Labour, Employment and Skill Development under DoT to ₹0.42cr from ₹5cr in FY 2021-22. There are also decreases across budget heads in this component - Manpower Development under Digital India (90% from FY 2021-22), Human Resource Management under DoT (27.5% from FY 2021-22) and PMGDISHA (16.7% from the FY2021-22) – that reflect the downward trend of allocations in FY 2022-23 in Chart 21. MHA's Police Education, Training and Research is the only budget head to receive an increased allocation in FY 2022-23, by 9.7% from the previous year.

This gap in public expenditure towards human resource development for cybersecurity needs to be examined in the context of the stated objective under India's National Cyber Security Policy (NCSP), 2013 to create a workforce of 500 thousand cybersecurity professionals.[103] To complement this the NCSP contained a dedicated strategy towards *Human Resource Development* which included provisions relating to training, enabling the setting up of relevant training and development infrastructure and institutional mechanisms.[104] This target was supposed to be met by 2018, within a five year period from date of policy introduction.[105]

In August 2015, major industry interlocutors at the National Association of Software and Service Companies (NASSCOM) estimated that the number of cybersecurity professionals in the country amounted to a modest 50 thousand.[106] In 2020, the Data Security Council of India (DSCI) estimated that the employee base of cybersecurity professionals in India was around 110 thousand professionals.[107] Besides these earlier targets not being realised, according to a 2018 *Cyber Shikshaa* Joint Skilling Project announcement between MeitY, DSCI and Microsoft, India is aiming to have 1 million skilled cybersecurity professionals by 2025.[108]

In terms of quantum of total budgeted allocations and relative comparison among the six activities in our analysis, we note that Human Resource Development is the fifth most significant activity for cybersecurity.

---

[103] Ministry of Communications and Information Technology, Department of Electronics and Information Technology, *The National Cyber Security policy,* 2nd July 2013, Objective no. 8 at p. 4 <https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf>.

[104] Ibid, Strategy J, Page 9.

[105] Lt. Col. Sanjiv Tomar, 'National Cyber Security Policy 2013: An Assessment', Manohar Parrikar Institute of defence Studies and Analysis (MP-IDSA), August 26, 2013, <https://www.idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813>.

[106] ET Bureau, '1 million cybersecurity professionals needed by 2020, (*The Economic Times,* August 25, 2015), <https://economictimes.indiatimes.com/tech/internet/cyber-security-1-million-cyber-security-professionals-needed-by-2020/articleshow/48661717.cms>

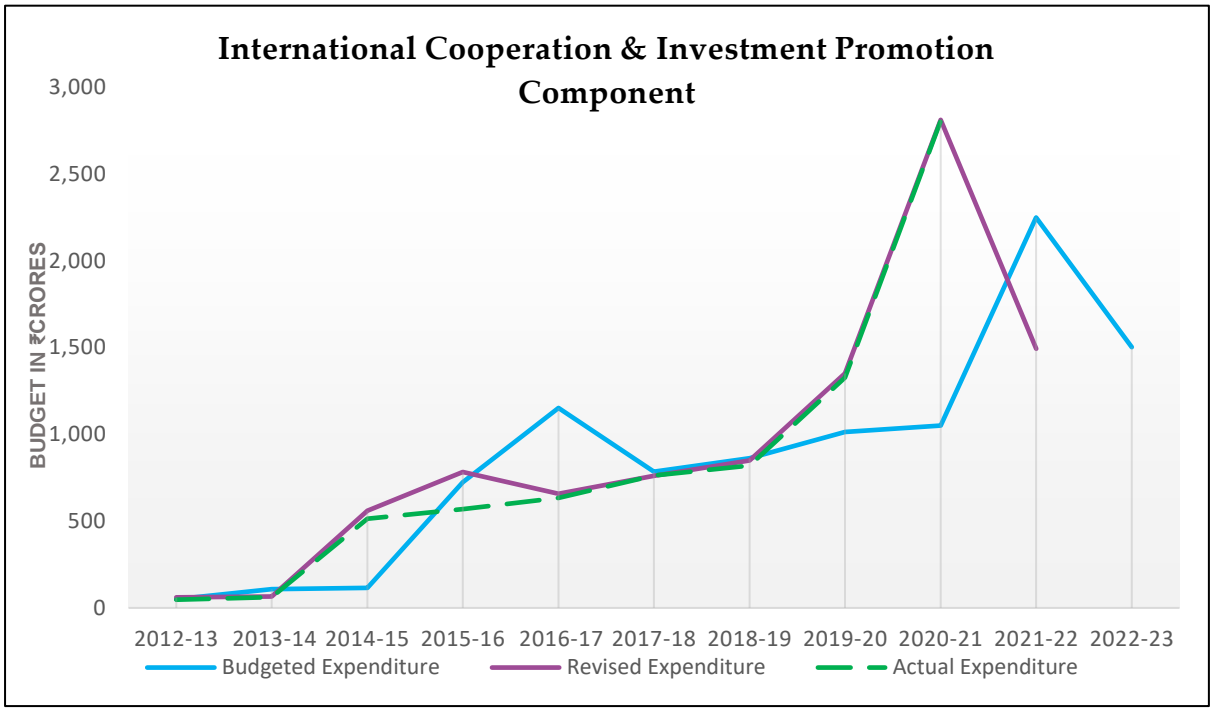
[107] *India Cybersecurity Services Landscape,* Data Security Council of India, May 21, 2020, <https://www.dsci.in/content/India-Cybersecurity-Services-Landscape>.

[108] 'Project Cyber Shikshaa', Data Security Council fo India, <https://www.dsci.in/cyber-shikshaa/>.

(iv) International Cooperation and Investment Promotion

The trends in budgeted allocations for International Cooperation and Investment Promotion are characterised by spurts of increased allocations (from the period between FY 2014 to FY 2017, and in FY 2021-22) and periods of steady allocations (from FY 2012-2014 and FY 2017-21). The budgeted allocations for this activity peak at ₹2,249cr in FY 2021-22 before being reduced to ₹1,502cr in FY 2022-23.

Chart 22: BE vs RE vs AE for International Cooperation & Investment Promotion Component (FY 2012-13 to FY 2022-23)



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

Budgeted allocations for International Cooperation & Investment Promotion increased significantly in FY 2015-16. This increase is preceded by a substantial increase in actual expenditures by Foreign Trade and Export Promotion under MeitY (AE ₹2.5cr in FY 2013-14 to AE ₹60cr in FY 2014-15) and Technical & Economic Cooperation with Other Countries under Ministry of Finance (AE ₹57cr in FY 2013-14 to AE ₹449cr in FY 2014-15). While allocations increase subsequently in FY 2016-17 as well, actual expenditures remain consistent at the same level even after this two-year influx of funds.

This is until a 17.4% increase in actual spending in FY 2019-20, which then increases more than two-fold in FY 2020-21. The promotion of IT/ITeS industries under the Digital India Scheme and the Ministry of Finance's Technical and Economic Co-operation with Other Countries programme drive this two-year period of significantly increasing actual expenditures.

There is an alignment of actual spending with revised expenditures since FY 2016-17. We see a significant increase in allocations in FY 2021-22, a positive change for efforts towards this component. Revised expenditures have also been significantly higher than budgeted allocations from FY 2018-19 to FY 2020-21. This is followed by a sharp dip in the revised expenditure for FY 2021-22 after which budgeted allocations decrease in tandem in FY 2022-23.

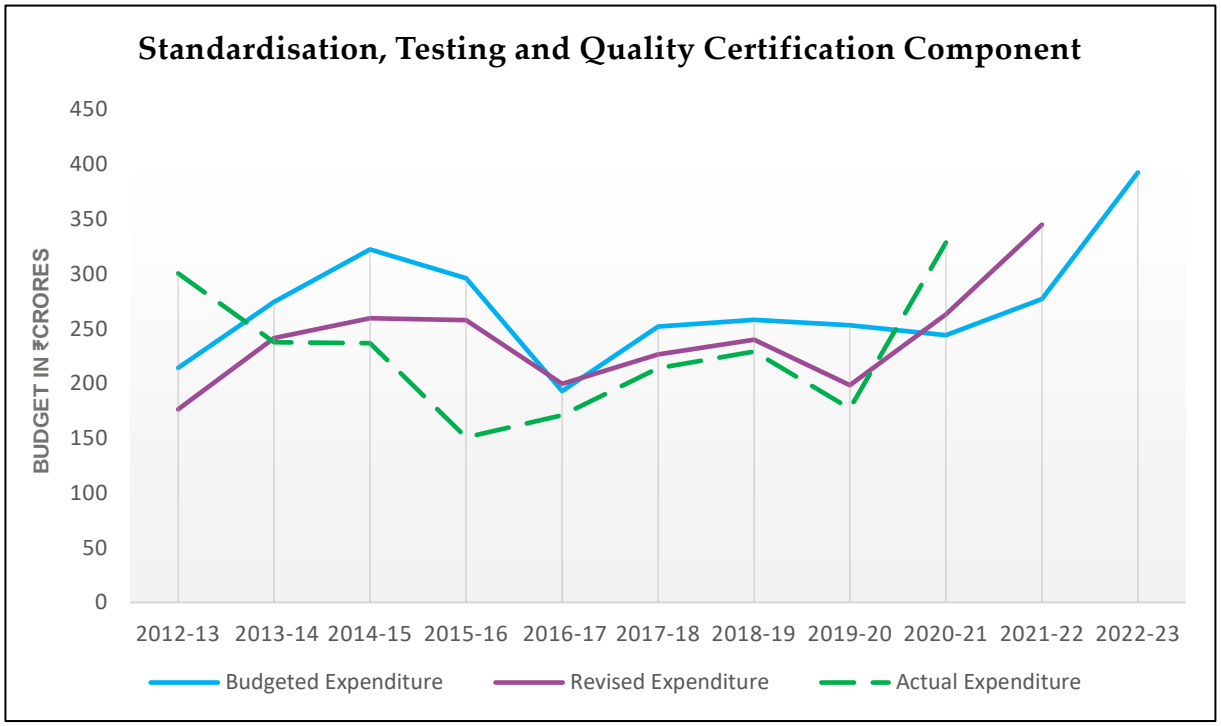
Overall, Technical & Economic Cooperation with Other Countries under the Ministry of Finance has been a driving force of spending in this component along with support from the Digital India scheme.[109] In terms of quantum of total budgeted allocations and relative comparison with the other six activities in our analysis, we note that International Cooperation & Investment Promotion is the fourth most significant activity for cybersecurity.

(v) Standardisation, Testing and Quality Certification

The budgeted, revised and actual expenditures for Standardisation, Testing and Quality Certification (STQC) are displayed in Chart 23. In FY 2022-23, there is a significant increase in allocations from the previous year towards this component. Budgeted allocations have either increased or remained consistent over the last decade with the exception of decreasing allocations between FY 2014-15 and FY 2016-17. This is due to reduction in allocations for budget heads under DoT, namely Telecom Regulatory Authority of India (TRAI), Telecom Enforcement Resources and Monitoring (TERM) and Telecom Engineering Centre (TEC).

[109] Of the nine budget heads under the Digital India Scheme included in this analysis, one of them - the promotion of IT/ITeS industries - is the only relevant budget head for the activity wise classification of international cooperation and investment promotion. The remaining eight budget heads under the Digital India scheme are categorised under various other activities in the activity-wise classification.

Chart 23: BE vs RE vs AE for Standardisation, Testing and Quality Certification Component (FY 2012-13 to FY 2022-23)



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

We observe significantly increasing allocations from FY 2012-13 to FY 2014-15 around the release of the National Cyber Security Policy in 2013. However, this same time period is characterised by decreasing actual expenditures and underutilisation of allocations. In FY 2015-16, the gap between actual spending and allocations is most significant and due to TRAI (BE ₹90cr to AE ₹59cr) TERM (BE ₹67cr to unavailable data on actual spending) and TEC (BE ₹39cr to AE ₹0.01cr).

A turning point for actual expenditures under STQC is FY 2020-21 where the significant 85.4% increase in actual spending from the previous year, comes from DoT's TRAI (BE ₹70cr to AE ₹203cr). This is despite reduced actual expenditures from budgeted allocations across all other budget heads in this component. The subsequent increase in allocations in FY 2022-23 is also due to TRAI's increased allocation (BE ₹100cr in 2021-22 to BE ₹226 in 2022-23). It is evident that in the recent years, TRAI has been a driving force of efforts towards STQC.

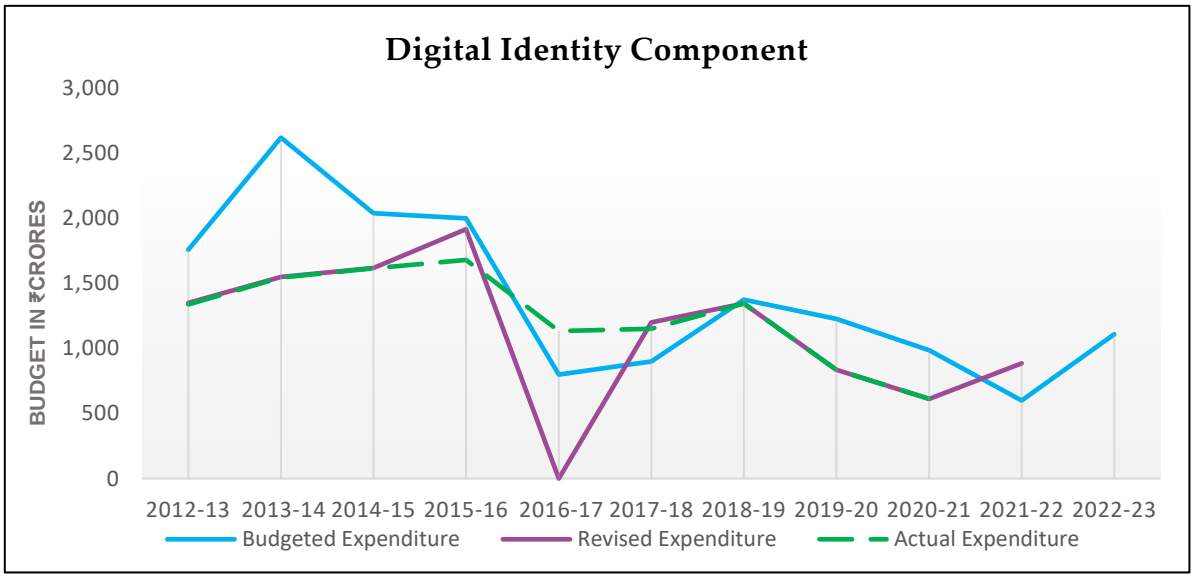
Overall, we also note that trends in actual expenditure drive the budgeted allocations for STQC such that decreased spending (i.e., between 2012-2016) is followed by subsequent decrease in allocations (i.e., 2014-17). Similarly, the significant increase in spending in FY 2020-21 is followed by consecutive increases in budgeted allocations. The underutilisation of allocated funds between FY 2013-14 and FY 2019-20 is significant but gaps between actual spending and budgeted allocation reduce post FY 2016-17.

In terms of quantum of total budgeted allocations and relative comparison with the other six activities in our analysis, we note that Standardisation, Testing and Quality Certification appears to have been treated as the least significant activity for cybersecurity.

(vi) Digital Identity

Chart 24 displays the budget trends for the digital identity component, comprised of the Unique Identification Authority of India (UIDAI). In FY 2016-17, the sharp dip in revised expenditure is due to missing data for this value in the Union Budget. Actual spending at ₹1,133cr exceeds the budgeted allocation of ₹8,00cr in FY 2016-17 but meaningful analysis over time is limited by gaps in publicly available data.

Chart 24: BE vs RE vs AE for Digital Identity Component (FY 2012-13 to FY 2022-23)



Source: CCG's Cybersecurity Budget Dataset; Union Budget Documents (various years)

With the exceptions of FY 2016-17 and FY 2017-18, actual spending has been less than budgeted expenditure over the years for digital identity. A steady reduction of funds towards the Aadhar project since FY 2018-19 is also evident and likely due to major implementation of the project being completed. In FY 2022-23, there is a marked increase in allocations towards digital identity. The maintenance of digital identity systems requires sufficient budgets to prevent breaches and security incidents of citizens' data. Any future allocations that serve to update the current systems should also be tracked under this categorisation. For instance, the proposed model of 'Federated Digital identities' to create a unique ID for citizens and interlink multiple digital IDs proposed recently[110] can be correlated to the increased allocations for this component in FY 2022-23.

[110] IT Ministry proposed new model of unique digital ID, DNA India, 30 January 2022, https://www.dnaindia.com/personal-finance/report-it-ministry-proposes-new-model-of-unique-digital-id-2931175.

PART V: Key Findings & Insights

It is important to bear in mind that none of the figures discussed in this brief are an indication of actual expenditure incurred by the Government of India on cybersecurity. These figures must be viewed as the pool of financial resources available to government to strengthen the state of cyber security and various aspects of internet governance related thereto at the national level, including the security of e-governance initiatives to facilitate the online delivery of public services to citizens. The current format of the Demands for Grants do not allow for inference of the precise share of budgeted allocations that are actually used for activities directly related to cybersecurity. All budget heads included in our analysis therefore fall on a spectrum of high significance to low significance with respect to percentage share of their budgeted allocations being utilised for cybersecurity. For certain budget heads, it is likely that a greater share of the allocation is directed towards cybersecurity related activities. For example, it is likely that for Cybersecurity projects under the Digital India scheme and CERT-In, both under the Ministry of Electronics and Information Technology, the entire allocation is directly relevant for cybersecurity. On the other hand, for budget heads such as the Prime Minister's Office under Ministry of Home Affairs, only a specific percentage of the total allocated budget is likely to be directed towards cybersecurity activities. However, there exist no relevant mechanisms to establish what percentage of these allocations can be taken as relevant for cybersecurity activities, and thus the entire allocation has been included for such budget heads in our analysis.

As we derived from Chart 1, it is most pertinent to highlight the consistently increasing allocations for cybersecurity. In fact, budgeted expenditure has more than doubled over the last ten years (Table 1). Therefore, it is reasonable to conclude that cybersecurity remains significant as a priority for the Union Government, in terms of budgetary allocation. Since FY 2012-13 there has been a Compound Annual Growth Rate (CAGR) of 8.1% in the budgeted expenditure for cybersecurity over eleven years. Over this time period, approximately 0.1% of the total government budget has been consistently dedicated to budgeted expenditures for cybersecurity annually. *However, actual expenditure under many budget heads has been consistently less than the*

budgeted and/or revised expenditure allocated to relevant departments. This requires a broader analysis into the causes of under-utilisation of allocated funds, including especially the lack of trained cybersecurity professionals in relevant departments.

A clear trend that cuts across ministries is the presence of driving budget heads and priority areas that shift budget metrics periodically and in accordance with new schemes and policies. MeitY has seen close alignment of budgeted allocations with actual spending and diversity in allocations (Chart 4). Digital Payments and IT HW Manufacturing are key budget heads under MeitY. DoT's budget is characterised by instances of underutilisation (Chart 7) and C-DoT and TERM drive the direction of spending under DoT. Actual expenditure trendlines for MHA are characterised by sharp V shape curves(Chart 11). Cyber Crime Prevention for Women & Children, NSCS and Office of the Principal Scientific Advisor are key priorities for MHA. While overall budgeted expenditures are increasing for cybersecurity, their manifestation in actual spending is not consistent, particularly in the case of MHA.

It is clear from the activity wise analysis that priority has been accorded via increasing budgets (Chart 16) to the Technical R&D and Cyber Incident Preparedness and Response components by the government. We infer that the STQC component has also received renewed attention recently with increased allocation in FY 2022-23. The trend of underutilisation in the cybersecurity budget noted above,[111] can potentially be addressed by focusing on the Human Resource Development Component, that has seen limited change since FY 2014-15 despite being a stated priority in the National Cyber Security Policy 2013.

In order of high to low significance, quantified in terms of budgetary allocations, the activities treated as significant for cybersecurity from our analysis can be listed as – (1) Technical Research and Capacity Development (2) Cyber Incident Response & Preparedness (3) Digital Identity (4) International Cooperation and Investment Promotion (5) Human Resource Development and (6) Standardisation, Testing and Quality Certification.

[111] Refer page 35 of this report.

An overarching observation that cuts across all categories of our analysis', is the lack of publicly available data on the outcome of these budgets from a cybersecurity perspective. *Gaps in tracking of the budget are also evident with certain missing expenditure values. The relevant Parliamentary Committees must examine this question,* with a view to (a) identifying actual expenditure on cybersecurity products, services and related activities from the overall budget allocated to the department and (b) examining the outcomes achieved by increases in allocation of financial resources.

While publicly available data currently allows researchers to gauge the relative significance of activities that are crucial for cybersecurity in the country, the existing reporting requirements on allocated budgets do not allow for examination of whether the programmes were implemented in accordance with identified priorities.

For instance, the absence of any mention of a National Mission on Quantum Computing from all demands for grants in FY 2020-21 as noted previously[112] raises concerns around implementation of cybersecurity prioritises being announced. Additionally, this lack of clarity diminishes researchers' ability to track progress and outcomes and hold decision makers accountable.

In conclusion, it is discernible from our analysis that allocation of financial resources by the government towards cybersecurity is likely to follow the upward trend in coming years as well. In this context of making more resources available and allocations to be more distinct, the following insights are relevant to highlight:

1. Policy makers and policy researchers should analyse the instances of consistent increase in absolute budgets allocated to relevant departments and examine corresponding policy outcomes.

2. Policy makers and policy researchers should focus on ways and means to track the actual outcome of budgets allocated to relevant departments over the years.

[112] Refer pages 12 and 13 of this report.

3. It would be relevant for legislators to consider raising discussions and questions in Parliament regarding underutilisation and over commitment of funds allocated for cybersecurity. For instance, the absence of specific allocations to the 'National Mission on Quantum Computing' in the Demands for Grants for FY 2020-21 and the source of ₹ 8,000 crore announced as allocated for the same, as per the Budget Speech of 2020-21 would be significant to highlight.

4. Policy makers should consider whether the format of presentation of the budget across ministries is done in a manner that is user friendly and transparent to enable effective parliamentary scrutiny of the resources required for effective cybersecurity of the nation, and its implications. For instance, given the unique role of the Ministry of Defence in India's cybersecurity, the format of the Ministry's budget should be examined.

5. Policy makers and policy researchers should consider how to develop similar and/or simpler analytical frameworks to analyse such budgetary allocations for cybersecurity related activities at the state government and local government level.

VOLUME – II

Annexure – I
Research Methodology and Interpretation Guidance

This document contains the research methodology for the Cybersecurity Budget Brief in which we breakdown our data collection, classification and analysis processes as well as the limitations of this analysis.

I. Data Collection

The dataset collated for analysis of the cyber security budget was extracted from publicly available data[113] on allocations (budgeted and revised) and actual expenditure from the Expenditure Budget (Volume II), as approved by Parliament in accordance with the Demand for Grants, submitted by various ministries. Our dataset tracks budgeted allocations from FY 2012-2013, just before the promulgation of India's first National Cybersecurity Policy (2013), until the most recent budget for FY 2022-2023. All data has been gathered from documents made available on https://www.indiabudget.gov.in/

The data for those budget heads under specific ministries that were demonstrably relevant for cyber security were tabulated. Specifically, at least one of the following two conditions are met for all budget heads included in CCG's Cybersecurity Budget Dataset:

1) The budget head's concerned department, centre or programme contributes substantially to national level cybersecurity or development of infrastructure for cybersecurity.
2) The budget head's concerned department, centre or programme is crucial for the country's digital development agenda and therefore *should* necessarily include a cybersecurity component.

[113]Union Budget 2021, Ministry of Finance, Government of India <https://www.indiabudget.gov.in/index.php>

II. Data Classification

In CCG's Comments to the National Security Council Secretariat on the National Cyber Security Strategy, we presented — in addition to the Ministry of Defence — the following four ministries as being directly responsible for the nation's cybersecurity:

1. Ministry of Electronics and Information Technology (MeitY)
2. Ministry of Communications (MoC)
3. Ministry of Home Affairs (MHA)
4. Other Relevant Departments

In this analysis, we have identified 47 budget heads that have been categorised under their relevant ministries and/ or department. No budget heads from the Ministry of Defence (MoD) have been included as it was not feasible to infer cybersecurity related expenditures — such as the total allocation for the newly established tri services Defence Cyber Agency—from the Union budget data for the MoD in its current format.

Further, four new budget heads that were introduced in the Union Budget FY 2022-23 have been identified under their relevant ministries, but not included in our analyses. These include (1) Production Linked Incentive (PLI) for Large Scale Electronics and IT Hardware under MeitY (2) Digital Intelligence Unit Project under DoT (3) Production Linked Incentive (PLI) Scheme to Promote Telecom and Networking Products under DoT and (4) Modernisation of Forensic Capacities under MHA. These budget heads have not been included in our analysis of trends in Part III and Part IV in order to maintain consistency in budget heads tracked over the last decade. However, any future analysis of India's cybersecurity budget should include these budget heads as well, subject to continued allocations towards the same.

The data collected was grouped into two buckets for analysis –relevant departments' allocations grouped Ministry-wise and Activity-wise allocations. Both these buckets contain the same budget heads under different classification frameworks. 'Relevant departments' include those departments and budget heads that are either directly related to cybersecurity or support the functioning of the security aspects of internet

governance at large. Under Ministry-wise allocations discussed in Part A, these 47 budget heads are grouped under their respective Ministry for analysis. Under 'activity wise allocations' we have re-classified each listed budget head into six categories that relate to various aspects of cybersecurity governance. These are:

1. Cyber Incident Preparedness and Response
2. Technical Research and Capacity Development
3. Human Resources Development
4. International Cooperation and Investment Promotion
5. Standardisation, Quality Testing and Certification and
6. Digital Identity

Each of these categories align with a constituent element of the Three Pillars of the forthcoming[114] National Cyber Security Strategy – Secure, Strengthen and Synergise.[115] We elaborate upon each of these in Part B of this section.

A. Ministry-wise Relevant Departments

(i) **<u>Ministry of Electronics and Information Technology:</u>** The aim of the Ministry of Electronics and Information Technology (MeitY) is to promote e-governance with the view of empowering citizens and enhancing India's role in internet governance.[116] Matters relating to the internet (except licensing of Internet Service Providers), cyber laws, policy matters relating to information technology, administration of the Information Technology Act 2000 and other IT related laws fall within its purview.[117] Cyber security plays a key role in

[114]' India in final stages of clearing national cyber security strategy' (Business Standard 27 October 2021) <https://www.business-standard.com/article/current-affairs/india-in-final-stages-of-clearing-national-cyber security-strategy-121102700663_1.html>

[115] These three "Pillars of Strategy", namely, Secure, Strengthen and Synergise were identified by the National Security Council Secretariat as such in the call for comments on the National Cyber Security Strategy 2020-25.

[116] Government of India, Ministry of Electronics and Information Technology, 'Vision and Mission', <https://www.meity.gov.in/about-meity/vision-mission>, 25th March 2021.

[117]'The Government of India (Allocation of Business) Rules' (Rashtrapati Bhavan 14 January 1961)28 < https://cabsec.gov.in/writereaddata/allocationbusinessrule/completeaobrules/english/1_Upload_915.pdf >

promoting a culture of innovation and enabling trust the digital ecosystem and e-governance, and "e-security" is one of the key objectives of this Ministry.[118]

From MeitY's expenditure budget, we treat 19 budget heads (including 9 budget heads under the Digital India programme) presented in MeitY's Demand for Grants, as directly linked to improving the quality, infrastructure and capacity for cybersecurity and related activities. A detailed explanation for each budget head's relevance for cybersecurity under MeitY is as follows:

1. Computer Emergency Response Team (CERT-IN)

CERT-IN was established in accordance with Section 70A of the IT Act 2000. It serves as the national nodal agency to perform various functions in the area of cyber security like collection, analysis and dissemination of information on cyber incidents, issuance of guidelines, advisories, vulnerability notes and whitepapers relating to information security practices and procedures, and prevention, response and reporting of cyber incidents.[119] Any allocation to CERT-In directly contributes to improving India's cyber security – both reactively and proactively.[120]

Given CERT-IN's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Cyber Incident Preparedness and Response (I).

2. Centre for Development of Advanced Computing (C-DAC)

C-DAC is an autonomous scientific society carrying out research & development in IT&E (information technologies and electronics) and associated areas as per mandates of MeitY.[121] It seeks to strengthen national technological capabilities in the context of global developments in the field, and works to respond to

[118] Government of India, Ministry of Electronics and Information Technology, 'Vision and Mission', <https://www.meity.gov.in/about-meity/vision-mission>, 25th March 2021.
[119] Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology <https://www.cert-in.org.in/ >
[120] Ibid.
[121] Website Policies, Centre for Development of Advanced Computing <https://www.cdac.in/index.aspx?id=website_policies>

changes in the market in select foundation areas.[122] C-DAC is engaged in building capacities in emerging/enabling technologies, and innovating and leveraging its expertise, calibre and skill sets to develop and deploy IT products and solutions for different sectors of the economy.[123] Some of the thrust areas in which C-DAC is currently working include high performance, grid and cloud computing (including the National Supercomputing Mission), multilingual computing, professional electronics, software technologies, cyber security and cyber forensics, health informatics, and education & training.[124] C-DAC recognises that in order to make IT infrastructure resilient against present day threats, there is a need for cutting-edge research & development efforts in cyber security.[125] It has been actively involved with a number of sub-areas of the cyber security domain – end point security, mobile and web security, SCADA security, network security, honeynet technologies and Security Operations Centre (SOC) as-a-service, to name a few.[126] C-DAC also offers a range of endpoint security products like AppSamvid,[127] Browser JS Guard,[128] M-Kavach,[129] USB Pratirodh[130] and Application and Device Control (ADC).[131]

Given C-DAC's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Technical Research & Capacity Development (II).

[122] Corporate Profile, Centre for Development of Advanced Computing < https://www.cdac.in/index.aspx?id=CorporateProfile>
[123] Ibid
[124] Demand No. 24, Notes on Demands for Grants 2021-21, Ministry of Electronics and Information Technology <https://www.indiabudget.gov.in/budget2020-21/doc/eb/sbe24.pdf>
[125] Cyber Security and Cyber Forensics, Centre for Development of Advanced Computing < https://www.cdac.in/index.aspx?id=cyber_security>
[126] Cyber Security and Cyber Forensics, Centre for Development of Advanced Computing <https://www.cdac.in/index.aspx?id=cyber_security>
[127] AppSamvid - An Application Whitelisting Software, Centre for Development of Advanced Computing <https://www.cdac.in/index.aspx?id=cs_eps_AppSamvid>
[128] Browser JSGuard, Centre for Development of Advanced Computing <https://www.cdac.in/index.aspx?id=cs_eps_jsguard>
[129] M-Kavach - Mobile Device Security Solution, Centre for Development of Advanced Computing <https://www.cdac.in/index.aspx?id=cs_eps_MKavach>
[130] Downloads, Centre for Development of Advanced Computing <https://www.cdac.in/index.aspx?id=download>
[131] ADC, Centre for Development of Advanced Computing <https://www.cdac.in/index.aspx?id=cs_eps_ADC_>

3. Centre for Materials for Electronics and IT (C-MET)

C-MET is engaged in the development of viable technologies primarily in the area of electronic materials.[132] The mission of C-MET is to develop a knowledge base in electronic materials and their processing technology, and become a source of critical electronic materials, know-how and technical services for the industry and other sectors of the economy.[133] In doing so, it is imperative to undertake and impart cyber security measures.[134] C-MET recognises this need in working with high technology electronic materials for electronic waste recycling technologies and RoHS (Restriction of Hazardous Substances) compliance, renewable energy, microwave dielectrics & packaging, multilayer ceramics for actuators, sensors for smart cities and supercapacitors.[135]

Given C-MET's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Technical Research & Capacity Development (II).

4. Society for Applied Microwave Electronics Engineering and Research (SAMEER)

SAMEER was set up as an autonomous research & development laboratory with a broad mandate to undertake R&D work in the areas of microwave and radio frequency engineering, and electromagnetics.[136] The mission of this department is to engage in product development driven by technology and user requirements, and to keep pace with rapidly changing technology by continuous training of its manpower.[137] It has developed various atmospheric instruments

[132] Centre for Materials for Electronics Technology, Ministry of Electronics and Information Technology, Government of India <https://www.meity.gov.in/content/c-met>
[133] Vision and Mission, Centre for Materials for Electronics Technology, Ministry of Electronics and Information Technology, Government of India <https://www.cmet.gov.in/about_vision_mission>
[134]Annual Report 2019-20, Centre for Materials for Electronics Technology, Ministry of Electronics and Information Technology, 94 <https://cmet.gov.in/sites/default/files/annual-reports/AnnualReport-2019-20%28InEnglish%29_0.pdf >
[135] Research and Development,, Centre for Materials for Electronics Technology <https://www.cmet.gov.in/research-and-development>
[136] About SAMEER, Society for Applied Microwave Electronics Engineering & Research, Ministry of Electronics & Information Technology, Government of India <https://www.sameer.gov.in/aboutsameer.asp#page >
[137] Ibid

(CW bistatic RASS, radio theodolite, etc.), wireless frequency hopping data links, cell phone deactivators, wireless modems and India's first MST (mesosphere-stratosphere-troposphere) radar.[138] These technologies are often built on networked systems and can transform the way users interrelate and develop. Ensuring their security online and offline is of utmost importance.[139] As 'IT and communications' is one of the pillars of SAMEER,[140] cyber security is thus embedded in its operations.

Given SAMEER's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Technical Research & Capacity Development (II).

5. Standardisation Testing and Quality Certification (STQC)

The development of technical standards, testing and certification for compliance therewith is essential to ensuring good governance of cybersecurity. STQC provides quality assurance services in the area of IT and e-governance.[141] It also plays a role in the development of e-governance standards, guidelines and frameworks in emerging areas and technologies.[142] The STQC Directorate also provides testing,[143] calibration,[144] training and certification services[145] to industries for improvement of quality and reliability of electronics and IT products. One such certification is the "ISO 27001 Information Security

[138] Ibid
[139] About SAMEER, Society for Applied Microwave Electronics Engineering & Research, Ministry of Electronics & Information Technology, Government of India <https://www.sameer.gov.in/aboutsameer.asp#page >
[140] Ibid.
[141] Ministry of Electronics and Information Technology, Government of India, STQC, <https://www.meity.gov.in/content/stqc>.
[142] Vision, Mission & Objective, Standardisation Testing and Quality Certification Directorate, Ministry of Electronics & Information Technology, Government of India <https://www.stqc.gov.in/vision-mission-objective>
[143] About Electronics Testing, Standardisation Testing and Quality Certification Directorate, Ministry of Electronics & Information Technology, Government of India <https://www.stqc.gov.in/about-electronics-testing>
[144] About Calibration, Standardisation Testing and Quality Certification Directorate, Ministry of Electronics & Information Technology, Government of India < https://www.stqc.gov.in/about-calibration >
[145] About Certification, Standardisation Testing and Quality Certification Directorate, Ministry of Electronics & Information Technology, Government of India <https://www.stqc.gov.in/about-certification>

Management System (ISMS)"[146] which is facilitated by a team of ISMS lead auditors, qualified as per international requirements.[147]

Given STQC's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Standardisation, Quality Testing and Certification (V).

6. Controller of Certifying Authorities (CCA)

The CCA licenses and regulates the Certifying Authorities in the issuing of Digital Signature Certificates (DSC) for electronic authentication of users, and aims to promote the growth of e-commerce and e-governance through the wide use of digital signatures.[148] The CCA maintains the Root Certifying Authority of India (RCAI) and a repository of digital certificates.[149] The CCA also issues licenses for operating as a Certifying Authority to individuals and companies, and is an important body for setting standards for the creation and maintenance of secure electronic records and secure electronic signatures.[150] The CCA is appointed under S. 17 of the IT Act, 2000 to perform supervisory functions over Certifying Authorities.[151] In order to ensure that the signatures are protected from hackers attempting to steal identities and other misuse, ensuring cyber security of CCA's network infrastructure is essential. In turn, Certifying Authorities are mandatorily required to make use of hardware, software and procedures that are secure from intrusion and misuse, and adhere to security procedures to ensure the secrecy and privacy of electronic signatures.[152]

---

[146] Information Security Management Systems (ISMS), Standardisation Testing and Quality Certification Directorate, Ministry of Electronics & Information Technology, Government of India <https://www.stqc.gov.in/information-security-management-system-isms>
[147] Information Security Management System, Standardisation Testing and Quality Certification Directorate, Ministry of Electronics & Information Technology, Government of India < https://www.stqc.gov.in/information-security-management-system-isms>
[148] Controller Of Certifying Authorities, Digital India <https://digitalindia.gov.in/content/controller-certifying-authorities-cca
[149] Controller Of Certifying Authorities, Digital India <https://digitalindia.gov.in/content/controller-certifying-authorities-cca >
[150] About CCA, Controller of Certifying Authorities, Ministry of Electronics & Information Technology, Government of India <https://cca.gov.in/about.html>
[151] Sections 17 and 18, Information Technology Act, 2000.
[152] Section 30, Information Technology Act, 2000.

Given CCA's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Standardisation, Quality Testing and Certification (V).

7. Foreign Trade and Export Promotion

Foreign trade and exports require electronic filing, clearance of import and export documents, payment of customs and license fees, electronic exchange of document between parties, etc.[153] All of these services are provided using electronic devices and online networks. In promotion of software and electronic exports, efforts to aid elimination of online frauds and trading with fraudulent parties is essential, thereby furthering cyber security and encouraging foreign trade and export promotion.

For the purpose of this brief, the activity-wise classification for Foreign Trade and Export Promotion in the budget analysis will be: International Cooperation and Investment Promotion (IV).

8. Manpower Development Programmes

The objective of the programme is to generate specialised manpower required to support the growing needs of the electronics and IT export industry.[154] Initiatives like the 'Information Security Education and Awareness Programme'[155] and 'Special Manpower Development Programme in VLSI Design and Related Software'[156] are directly concerned with cyber security. This budget head falls under MeitY's Digital India Initiative.[157]

---

[153] Electronic Data Interchange (EDI) For Trade, Ministry of Electronics and Information Technology, Government of India <https://www.meity.gov.in/content/electronic-data-interchange-edi-trade-etrade >

[154] Demand No. 26, Notes on Demands for Grants 2019-20, Ministry of Electronics and Information Technology < https://www.indiabudget.gov.in/budget2019-20(I)/ub2019-20/eb/sbe26.pdf >

[155] Information Security Education & Awareness, Ministry of Electronics and Information Technology, Government of India <http://www.isea.gov.in/>

[156] Capacity Building, Ministry of Electronics & Information Technology, Government of India < https://www.meity.gov.in/content/capacity-building-4>l

[157] *The Digital India Initiative is directly linked to a drive for a massive digitisation within the government and its various departments. With a huge investment towards adopting technology for government functioning, the government should also be spending towards developing resilience to make the cyber ecosystem of the country more secure. Although it is not clear whether the Digital*

For the purpose of this brief, the activity-wise classification for Manpower Development Programmes in the budget analysis will be: Human Resource Development (III).

9. National Knowledge Network

The National Knowledge Network project has been initiated to establish a strong and robust Indian network which will be capable of providing secure and reliable connectivity.[158] With its multi-gigabit capability, the network aims to connect all universities, research institutions, libraries, laboratories, healthcare and agricultural institutions across the country to enable a collaborative research and knowledge paradigm.[159] The development of national information infrastructure via ultra-high speed backbone connectivity for e-governance, computational capabilities and connection between different sectoral networks fall under the purview of this project.[160] Essential components of the network's design[161] address security requirements in light of innovations in convergence, and cyber security frameworks to protect the flow of information as prerequisites in implementation.[162] This budget head falls under MeitY's Digital India Initiative.

Given National Knowledge Network's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Technical Research & Capacity Development (II).

India programme includes a specific component on cybersecurity, we believe that it is so central to the nation's digital development agenda that it necessarily requires at least a portion of the allocated budget to be directed towards improving cybersecurity. The descriptions of each budget head in this section highlight the relevant schemes under the Digital India Initiative that have been included in this analysis.

[158] About, National Knowledge Network <https://nkn.gov.in/en/about-us-lt-en >

[159] Ibid

[160] Ibid

[161] Design and Architecture, National Knowledge Network <https://nkn.gov.in/en/design-and-architecture-en >

[162] Ibid

10. Promotion of Electronics and IT Hardware Manufacturing

Electronics manufacturing is an important pillar of the national digital development agenda.[163] The budget head has included expenditures for a Scheme for Promotion of Manufacturing of Electronic Components and Semiconductors (SPECS).[164] The expenditure for listed electronics under SPECS will go towards electronic plants, machinery, equipment and associated utilities and technology including expenses for Research & Development.[165] This budget head also complements the National Policy on Electronics 2019 (NPE 2019), which envisions positioning India as a global hub for Electronics System Design and Manufacturing (ESDM) by encouraging and driving capabilities in the country for developing core components, including chipsets and creating an enabling environment for the industry to compete globally.[166] This budget head falls under MeitY's Digital India Initiative.

For the purpose of this brief, the activity-wise classification for Promotion of Electronics and IT Hardware Manufacturing in the budget analysis will be: Technical Research & Capacity Development (II).

11. Cyber Security Projects including National Cyber Coordination Centre and others

The objective of the Cyber Security Projects scheme is to adopt a holistic approach towards securing the cyberspace of the country by pursuing multiple initiatives like a security policy, compliance and assurance measures, security requirements, incident-early warning & response, security training, security specific Research & Development, and enabling of legal frameworks and

[163] Demand No. 27, Notes on Demands for Grants 2022-23, Ministry of Electronics and Information Technology, Government of India < https://www.indiabudget.gov.in/doc/eb/sbe27.pdf >
[164] Scheme for Promotion of Manufacturing of Electronic Components and Semiconductors, Ministry of Electronics and Information Technology, Government of India <https://www.meity.gov.in/esdm/SPECS >
[165] Ibid
[166] Demand No. 27, Notes on Demands for Grants 2022-23, Ministry of Electronics and Information Technology, Government of India < https://www.indiabudget.gov.in/doc/eb/sbe27.pdf >

collaboration.[167] The National Cyber coordination Centre is the national level agency for coordination in operational aspects of cybersecurity, it was set up to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.[168] This budget head falls under MeitY's Digital India Initiative.

For the purpose of this brief, the activity-wise classification for Cyber Security Projects in the budget analysis will be: Cyber Incident Preparedness and Response (I).

12. Research and Development in Electronics/IT

Proliferation and absorption of emerging technology by supporting research and development is a crucial objective of this program, aside from creating essential R&D infrastructure, and scientific and technical human capital.[169] A core focus is to aid development of indigenous technology and know-how and its transfer to Indian companies for manufacturing.[170] R&D in IT includes areas like High Performance Computing (HPC), National Supercomputing Mission, perception engineering, bioinformatics, Free & Open-Source Software (FOSS), green and ubiquitous computing and digital preservation.[171] Several focus areas under electronics and Convergence Communication and Broadband Technologies (CC&BT) R&D also come under the purview of this scheme and are important for cyber security development.[172] This budget head falls under MeitY's Digital India Initiative.

[167]Demand No. 24, Notes on Demands for Grants 2020-21, Ministry of Electronics and Information Technology, Government of India <https://www.indiabudget.gov.in/budget2020-21/doc/eb/sbe24.pdf >
[168] Press Information Bureau, 'Cybersecurity', 18 December 2018, < https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1556474 >
[169] Demand No. 24, Notes on Demands for Grants 2020-21, Ministry of Electronics and Information Technology, Government of India <https://www.indiabudget.gov.in/budget2020-21/doc/eb/sbe24.pdf >
[170] Ibid
[171] Ibid
[172] Ibid

For the purpose of this brief, the activity-wise classification for Research and Development in Electronics/ IT in the budget analysis will be: Technical Research & Capacity Development (II).

13. Promotion of Digital Payments

Promotion of Digital Payments has been accorded the highest priority by the Government of India[173] to bring every segment of the country under the formal fold of digital payment services.[174] The vision is to provide the facility of seamless digital payment to all citizens in a convenient, easy, affordable, quick and secure manner.[175] The vision is to provide seamless digital payment facility to all citizens of India in a quick, easy, affordable and secured manner.[176] This budget head falls under MeitY's Digital India Initiative.

For the purpose of this brief, the activity-wise classification for Promotion of Digital payments in the budget analysis will be: Technical Research & Capacity Development (II).

14. Pradhan Mantri Digital Saksharta Abhiyan (PMGDISHA)

The scheme is aimed at empowering citizens in rural areas by training and equipping them to operate computers and digital access devices with a focus area in digital payments.[177] In undertaking the promotion of digital literacy in the country,[178] the scheme contributes to cyber security awareness among citizens. This budget head falls under MeitY's Digital India Initiative.

Given PMGDISHA's mandate and for the purpose of this brief, their activity-

[173] Demand No. 27, Notes on Demands for Grants 2022-23, Ministry of Electronics and Information Technology, Government of India < https://www.indiabudget.gov.in/doc/eb/sbe27.pdf >
[174] Ibid
[175] Ibid
[176] Digital Economy and Digital Payments Division, Ministry of Electronics and Information Technology, Government of India, < https://www.meity.gov.in/digidhan>.
[177] Overview of PGMDISHA, Ministry of Electronics and Information Technology< https://www.pmgdisha.in/about-pmgdisha/ >
[178]Ibid

wise classification for the budget analysis will be: Human Resource Development (III).

15. Promotion of IT/ ITeS Industries

Two schemes (North East BPO Promotion Scheme and India BPO Promotion Scheme)[179] under the IT for Jobs pillar have been launched under the Digital India Programme to incentivise BPO/ITES operations across the country. The schemes are particularly targeted towards digitally deficit areas for creation of employment opportunities for the youth and the balanced regional growth of IT/ITES Industry.[180] This budget head falls under MeitY's Digital India Initiative.

For the purpose of this brief, the activity-wise classification for Promotion of IT/ ITeS Industries in the budget analysis will be: International Cooperation and Investment Promotion (IV)

16. E-Governance

The ultimate objective of the scheme is to "make all government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realise the basic needs of the common man".[181] Latest initiatives under this scheme include a programme on good governance and best practices and a programme on enabling all schools with virtual classrooms.[182] All e-governance policies and programmes must necessarily account for existing and potential cyber security threats in order to ensure

[179] BPO Promotion Schemes, Ministry of Electronics and Information Technology, Government of India <https://www.meity.gov.in/bpo-promotion-schemes>
[180]Demand No. 24, Notes on Demands for Grants 2020-21, Ministry of Electronics and Information Technology, Government of India <https://www.indiabudget.gov.in/budget2020-21/doc/eb/sbe24.pdf >
[181] National e-governance Plan, Ministry of Electronics and Information Technology, Government of India <https://www.meity.gov.in/divisions/national-e-governance-plan >
[182] Demand No. 24, Notes on Demands for Grants 2020-21, Ministry of Electronics and Information Technology, Government of India <https://www.indiabudget.gov.in/budget2020-21/doc/eb/sbe24.pdf >

continued accessibility of essential services for the common man. This budget head falls under MeitY's Digital India Initiative.

For the purpose of this brief, the activity-wise classification for e-governance in the budget analysis will be: Cyber Incident Preparedness and Response (I).

17. Convergence, Communication & Strategic Electronics

The objective of programmes under Convergence, Communication & Broadband Technologies and Strategic Electronics (CC&BT) is to facilitate research & development in emerging, next generation wired and wireless broadband network, and broadcast and strategic technologies leading to their cost effective deployment for bringing economic benefits.[183]

Given CC&BT's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Technical Research & Capacity Development (II).

18. National Institute of Electronics & Information Technology (NIELIT)

NIELIT is an autonomous scientific society under the administrative control of MeitY, and plays a pivotal role in generating competent human resources for the Information Technology workforce via education in the non-formal sector.[184] IT training and literacy courses are undertaken at four levels by the NIELIT – 'O' level (Foundation), 'A' level (Advance diploma), 'B' level (MCA equivalent) and 'C' level (M-Tech) – via its centres and affiliate institutions across the country.[185] Other IT courses that are not typically offered by universities and institutions in the formal sector are also promoted by

[183] R&D in Convergence, Communications & Broadband Technologies and Strategic Electronics, Ministry of Electronics and Information Technology <https://www.meity.gov.in/content/rd-ccbt >
[184] Introduction, National Institute of Electronics & Information Technology, Ministry of Electronics & Information Technology, Government of India <https://www.nielit.gov.in/content/introduction-3 >
[185] Introduction, National Institute of Electronics & Information Technology, Ministry of Electronics & Information Technology, Government of India <https://www.nielit.gov.in/content/introduction-3 >

NIELIT.[186] These include CCC (Course on Computer Concept), BCC (Basic Computer Course), courses on bio-informatics and information security, and other high level courses.[187]

Given NIELIT's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Human Resource Development (III).

19. National Informatics Centre (NIC)

The NIC is the nodal organisation providing network backbone and e-governance support to the central government departments, states, union territories and district administrations in the country. Research and development to strengthen the government's technology infrastructure organisation and improve its development, management and use are also undertaken by the NIC.[188] It is effectively the technology partner of the Government of India, providing ICT infrastructure, advise on use of emerging technologies and developing IT systems for the government.[189] Security of government's critical cyber infrastructure forms a significant area of work under NIC; it has its own Computer Emergency Response Team (CERT) that coordinates with CERT-In and the National Critical Information Infrastructure Protection Centre (NCIIPC).[190] Additionally, the NIC operates national data centres, pan India VC infrastructure, a national cloud and command and control centres that enable delivery of citizen centric e-services.[191]

Given NIC's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Technical Research & Capacity Development (II).

[186] Ibid
[187] Ibid
[188] Research and Publications, National Informatics Centre <https://www.nic.in/research-publications/>
[189] Our Mandate, National Informatics Centre <https://www.nic.in/mandate/>
[190] Security, National Informatics Centre <https://www.nic.in/servicecontents/security/>
[191] Core Services Towards a Digital Nation, National Informatics Centre < https://www.nic.in/services-main-page/>

Ministry of Communication: Within the Ministry of Communication (MoC), we treat the following 14 budget heads under the MoC's Department of Telecom (DoT) to be directly related expenditures towards improving the infrastructure, capacity and quality for cyber security and related activities. Our reasoning for the selection of each budget head is as follows:

20. Telecom Regulatory Authority of India (TRAI)

The TRAI was established to regulate telecom services, including fixation and revision of tariffs for telecom and internet services.[192] Telecommunications serve as a gateway to multiple businesses and therefore, prone to cyber risk. Such risks must be combatted to protect both the telecom service providers and subscribers. TRAI issues directives and orders for the telecom sector, undertakes stakeholder consultations, and consumer initiatives toward combating these risks, thereby making a contribution towards protecting cyberspace.[193] TRAI also establishes standards for regulation and licensing frameworks of telecommunication services, internet service providers[194] and provides recommendations to the government telecom sector.[195]

Given TRAI's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Standardisation, Quality Testing and Certification (V).

21. Human Resource Management under National Institute of Communication Finance

As a training institute, the National Institute of Communication Finance (NICF) strives to encourage participants to exchange best practises and ideas, and learn new trends in the telecom sector and thus, promotes human capacity development

[192] History, Telecom Regulatory Authority of India <https://www.trai.gov.in/about-us/history >
[193] Report on Activities 2020, Telecom Regulatory Authority of India <https://www.trai.gov.in/sites/default/files/Report_27-08-2021.pdf>
[194] Licensing, Telecom Regulatory Authority of India < https://www.trai.gov.in/telecom/licensing >
[195] https://www.trai.gov.in/sites/default/files/Report_27-08-2021.pdf page 11

in the field of information and communications technology.[196] The NICF organises workshops, conferences, symposia and training programmes across levels to equip officers in the Ministry of Communications to work in areas of digital payments, telecom policies, spectrum management, USO regulation, etc.[197]

For the purpose of this brief, the activity-wise classification for Human Resource Development under NICF in the budget analysis will be: Human Resource Development (III).

22. Wireless Planning and Coordination

The budget provision is for expenditure of the Wireless Monitoring Organisation, which provides for technical and allied data on the basis of monitoring observations for radio frequency management, enforcement of national and international radio regulations.[198] The Organisation also carries out certain statutory functions under the Indian Telegraph Act 1885 to keep a round-the-clock watch on radio transmissions for effective national radio frequency management.[199] This includes (i) provision towards civil works; and (ii) for expenditures relating to the Wireless Planning and Co-ordination Wing.[200] This Wing issues licenses for transmitting and receiving stations and conducts examinations for wireless operators as per international standards.[201]

For the purpose of this brief, the activity-wise classification for Wireless Planning and Coordination in the budget analysis will be: Cyber Incident Preparedness and Response (I).

[196] About NICF, National Institute of Communication Finance, Ministry of Communications, Government of India <https://www.nicf.gov.in/about-nicf.php>
[197] About NICF, National Institute of Communication Finance, Ministry of Communications, Government of India <https://www.nicf.gov.in/about-nicf.php>
[198] Demand No. 13, Notes on Demands for Grants 2020-21, Department of Telecommunications, Ministry of Communications, Government of India <https://www.indiabudget.gov.in/budget2020-21/doc/eb/sbe13.pdf>
[199] Ibid
[200] Ibid
[201] Ibid

23. Telecom Engineering Centre (TEC)

TEC is a technical body representing the interests of the Department of Telecommunication.[202] Its functions include preparing specifications of common standards with regard to telecom network equipment, services and interoperability, issuing interface approvals, certificate of approvals, formulation of standards and fundamental technical plans, and developing expertise to imbibe the latest technologies and results of research and development.[203] TEC provides technical support to DoT and technical advice to TRAI and TDSAT, and coordinates with C-DOT on the technological developments in the telecom sector for policy planning by DoT.[204]

Given TEC's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Standardisation, Quality Testing and Certification (V).

24. Technology Development and Investment Promotion

Technology development is fundamental to improve technological performance by adding value to the existing technology, to make it up to date for its users. Currently, technology development programs under DoT are ongoing in next generation mobile technologies like 4G and 5G.[205] The investment promotion activities under DoT include formulating standard operating procedures for Foreign Direct Investments (FDI) policies in telecom[206], an investment facilitation centre that helps channelise investments in the telecom sector[207]

[202] TEC Functions, Telecommunication Engineering Centre, Department of Telecommunications, Ministry of Communications, Government of India < https://www.tec.gov.in/tec-functions >
[203] Ibid
[204] Ibid
[205] Annual Report 2021-22, Department of Telecommunications, Ministry of Communications, Government of India <https://dot.gov.in/sites/default/files/Final%20Eng%20AR%20Min%20of%20Tele%20for%20Net%2009-02-22.pdf> page 181
[206] FDI Policy in Telecom, Department of Telecommunications <https://dot.gov.in/fdi-policy-telecom#>
[207] Investment Facilitation Centre, Department of Telecommunications <https://dot.gov.in/investment-facilitation-centre>

and investments in telecom equipment manufacturing.[208] Promoting investments in technology development is important to strengthening technologies available for cybersecurity purposes.

For the purpose of this brief, the activity-wise classification for Technology Development and Investment Promotion in the budget analysis will be: International Cooperation and Investment Promotion (IV).

25. South Asia Sub-Regional Economic Cooperation (SASEC) under Information Highway Project

The focal point of this project is to make ICT more accessible, affordable, inclusive, sustainable and useful to remote and rural communities, entrepreneurs, and research and training institutes.[209] It is expected to help SASEC countries improve their productivity and efficiency and participate fully in the global information economy.[210] We include this budget head as a direct investment towards infrastructure for better cyber security in India

For the purpose of this brief, the activity-wise classification for SASEC under the Information Highway Project in the budget analysis will be: International Cooperation and Investment Promotion (IV).

26. Telecom Testing and Security Certification Centre

The Telecom Testing and Security Certification Centre is set up to adopt and develop security standards, test tools and systems for security testing and certification of telecom equipment.[211] Testing of software applications, networks and programs cannot be done in the absence of adequate knowledge

[208] Telecom Equipment Manufacturing, Department of Telecommunications <https://dot.gov.in/telecom-equipment-manufacturing>
[209] Regional: SASEC Information Highway Project (Bangladesh, Bhutan, India, Nepal), South Asia Subregional Economic Cooperation< https://www.sasec.asia/index.php?page=project&pid=23&url=sasec-information-highway-project >
[210] Ibid
[211] Telecom Testing and Security Certification Centre, Press Information Bureau, Ministry of Communications, Government of India < https://pib.gov.in/newsite/PrintRelease.aspx?relid=101720 >

and assessment of cyber security practices, which should form a component of the Centre's work.

For the purpose of this brief, the activity-wise classification for Telecom testing and Security Certification Centre in the budget analysis will be: Standardisation, Quality Testing and Certification (V).

27. Telecom Computer Emergency Response Team

The Telecom Computer Emergency Response Team (Telecom CERT) was created after consideration of the telecom sector as a core sector that forms the backbone of communication networks in the country. The aim is to provide the stakeholders of the telecom sector with timely information to take appropriate proactive and preventative actions against cyber breaches.[212]

Given the Telecom CERT's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Cyber Incident Preparedness and Response (I).

28. Central Equipment's Identity Registry (CEIR)

CEIR acts as a central system for all the network operators to alert the other networks of any black listed mobile devices, so that once a device is black listed, it will not work on any other network even if the SIM is changed.[213] This protects the network providers from mobile theft and counterfeiting of mobile phones and denies access to sensitive information on any device.

Given CEIR's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Standardisation, Quality Testing and Certification (V).

[212] 'Cyber security: Telecom sector set to have own emergency response team' (Financial Express 18March 2018) <https://www.financialexpress.com/industry/technology/cyber-security-telecom-sector-set-to-have-own-emergency-response-team/1115627/ >

[213] Central Equipment Identity Register, Department of Telecommunication <https://ceir.gov.in/Home/index.jsp >

29. 5G Connectivity Test Bed

The aim of this project is to build a test bed that closely resembles a real world 5G deployment.[214] The long-term benefit of this project can only be reaped if adequate security of the hardware system is ensured, and algorithms used are carefully protected.

For the purpose of this brief, the activity-wise classification for 5G Connectivity Test Bed in the budget analysis will be: Technical Research & Capacity Development (II).

30. Promotion of Innovation and Incubation of Future Technologies for Telecom Sector

Under the Ministry of Communication's umbrella Champion Services Sector Scheme (CSSS), the DoT has proposed two sub-schemes for promotion of innovation and incubation of future technologies for the telecom sector, expenditures for which are covered under this budget head.[215] First is the setting up of a Digital Communication Innovation Square (DCIS) to promote indigenous manufacturing and deployment of future technologies for the Indian communication services sector.[216] Second, to participate in relevant international events and undertake brand-building of India as a telecom manufacturing and services destination.[217]

For the purpose of this brief, the activity-wise classification for Promotion of Innovation and Incubation of Future Technologies for Telecom Sector in the budget analysis will be: Technical Research & Capacity Development (II).

---

[214] Indigenous 5G Testbed Project <http://www.ee.iitm.ac.in/5g/#:~:text=The%20goal%20of%20the%20project,a%20real%2Dworld%205G%20deployment.&text=The%20project%20will%20deliver%20an,MTC%20including%20NB%20IoT%20services>

[215] Annual Report 2020-21, Department of Telecommunications, Ministry of Communications, Government of India <https://dot.gov.in/sites/default/files/Annual%20Report%202020-21%20English%20Version.pdf> p. 26

[216] Ibid

[217] Ibid

31. Centre for Development of Telematics (C-DoT)

C-DoT contributes to the Indian telecom network's digitalisation by undertaking research and development on the indigenous design, development and production of telecom technologies that are suited to the Indian landscape. The centre facilitates indigenous research on wireless technology, switching and routing, security and network management and also emerging fields of Internet of Things (IoT), Artificial Intelligence (AI), 5G, etc.[218] Not only does C-DoT engage with cyber security as an inherent component of design in all these technologies from switching and routing to IoT, but it also offers products like SAMVAD, a secure calling and messaging application.[219]

Given C-DoT's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Technical Research & Capacity Development (II).

32. Labour, Employment and Skill Development

This budget head covers expenditures for the Pandit Deen Dayal Upadhayay Sanchar Kaushal Vikas Prathishthan Pilot Scheme,[220] that proposes to create skill development training centres in rural areas in order supplement skilled telecom manpower for growth of the telecom sector.[221] Improved training and skill development has to be a critical part of the employment strategy of any country.[222] Such training and skill development should necessarily include

[218] Corporate Profile, Centre for Development of Telematics, Telecom technology Centre, Government of India <https://www.cdot.in/cdotweb/web/aboutus.php?lang=e>
[219] Saved, Centre for Development of Telematics, Telecom Technology Centre, Government of India <https://www.cdot.in/cdotweb/web/product_page.php?lang=en&catId=4&pId=23>
[220] Demand No. 13, Notes on Demands for Grants 2020-21, Department of Telecommunications, Ministry of Communications, Government of India <https://www.indiabudget.gov.in/budget2020-21/doc/eb/sbe13.pdf>.
[221] Launch of Pilot Scheme to open 'Pandit Deendayal Upadhyaya Sanchar Kaushal Vikas Pratisthans', Skill Development Unit, Department of Telecommunications, Government of India, 26th May 2017 <https://dot.gov.in/sites/default/files/Pandit%20Deen%20Dayal%20Upadhyaya%20Sanchar%20Kaushal%20Vikas%20Pratisthan%20_0.pdf>
[222]Employment and Skill Development <https://niti.gov.in/planningcommission.gov.in/docs/plans/mta/11th_mta/chapterwise/chap9_employ.pdf>

cyber security components. Thus, this expenditure is crucial towards building the human resources required for skilling future cyber security professionals.

For the purpose of this brief, the activity-wise classification for Labour, Employment and Skill Development in the budget analysis will be: Human Resource Development (III).

33. Telecom Enforcement Resources and Monitoring Cells (TERM)

TERM is the vigilance arm of the DoT and is the nodal unit for C-DoT in the DoT.[223] TERM Cells are field offices for the DoT that perform network monitoring, vigilance and security functions.[224] Monitoring of network parameters, subscriber verification audits for mobile service operators, inspection of illegal telecom market activities include some of the functions of the TERM Cells.[225] TERM also serves as the interface between telecom service providers and security agencies.[226]

Given TERM's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Cyber Incident Preparedness and Response (I).

(ii) **Ministry of Home Affairs:** The Ministry of Home Affairs (MHA) discharges multifarious responsibilities, the important among them being – internal security, border management, centre-state relations, administration of union territories, management of Central Armed Police Forces, disaster management, etc.[227] Its Cyber and Information Security (C&IS) division deals with matters relating to

[223] Annual Report 2008-2009, Department of Telecommunication, Ministry of Communications and Information Technology, Government of India< https://dot.gov.in/sites/default/files/AR_English_2008-09_0.pdf > p. 49
[224] Annual Report 2008-2009, Department of Telecommunication, Ministry of Communications and Information Technology, Government of India< https://dot.gov.in/sites/default/files/AR_English_2008-09_0.pdf > p. 49
[225] Ibid p.50
[226] Ibid p.50
[227] About The Ministry, Ministry of Home Affairs, Government of India <https://www.mha.gov.in/about-us/about-the-ministry>

cyber security, cyber crime, National Information Security Policy & Guidelines (NISPG) and implementation of NISPG, National Intelligence Grid (NATGRID), etc.[228] Under the MHA, we treat the following 10 budget heads as being directly related to the maintenance and enhancement of cyber security and response to cyber crime:

34. Police Education, Training and Research Purposes

The prevention and punishment of cyber crimes is highly dependent on the level of training and research conducted to familiarise law enforcement officials with both the technicalities and legal processes concerned with cyber security. There is an urgent need for training and upskilling in this field to prevent malicious activities that pose serious threats to the nation's security. The budget allocation for Police Education, Training and Research covers expenditures on national police training institutions across the country and schemes under the Bureau of Police Research & Development (BPR&D). [230]

For the purpose of this brief, the activity-wise classification for Police, Education Training and Research Purposes in the budget analysis will be: Human Resources Development (III).

35. Criminology and Forensic Science

The allocation for Criminology and Forensic Science covers administrative expenditures for the National Institute of Criminology and Forensic Science, which is involved in the training of criminal justice functionaries and others as well as research in criminology and forensic science. With the rise in the cyber crime rates, implementation of cyber security within a criminal and forensic context is necessary to understand criminal minds in physical and virtual spaces. This budget head also covers expenditures on the Directorate of Forensic Science and Central Forensic Science Laboratories (CFSLs). The modernisation of Central Forensic Science Laboratories, with an emphasis on

[228] Cyber And Information Security (C&IS) Division, Ministry of Home Affairs, Government of India <https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division >

human resources development and Research & Development schemes, establishment of regional Forensic Laboratories and DNA Centres are all covered by this expenditure. Modernisation of forensic capacities includes the setting up of cyber and/or digital forensics divisions within CFSLs.

For the purpose of this brief, the activity-wise classification for Criminology and Forensic Science in the budget analysis will be: Technical Research & Capacity Development (II).

36. Modernisation of Police Forces and Crime and Criminal Tracking Network and Systems (CCTNS)

This is to provide allocation for schemes for modernisation of police forces, assistance to states for upgrading police infrastructure, e-Prison and CCTNS.[229] The CCTNS aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing by improving delivery of citizen centric services through effective usage of ICT, among others.[230] With the view of reducing manual and redundant record keeping, the CCTNS seeks to provide investigating police officers with tools and technology to further investigation of crime and detection of criminals.[231] The digitalisation of law enforcement functions necessitates that the cyber security facets of this modernisation should be appropriately tackled.

For the purpose of this brief, the activity-wise classification for Criminology and Forensic Science in the budget analysis will be: Cyber Incident Preparedness and Response (I).

[229] Demand No. 48, Notes on Demands for Grants 2019-20, Ministry of Affairs, Government of India < https://www.indiabudget.gov.in/budget2019-20/doc/eb/sbe48.pdf >
[230] Crime and Criminal Tracking Network & Systems, National Crime Records Bureau, Ministry of Home Affairs, Government of India <https://ncrb.gov.in/en/crime-and-criminal-tracking-network-systems-cctns>
[231] Ibid

37. Indian Cyber Crime Coordination Centre (I4C)

The aim of the Indian Cyber Crime Coordination Centre (I4C) is to act as a nodal point in fighting cyber crime. It undertakes reporting of cyber crime at the national level, forensic analysis and investigation of cyber crimes that are continuously evolving as a result of new digital technology and techniques. The Centre produces cyber threat intelligence reports and facilitates co-ordination of incident response between stakeholders. Further, it seeks to prevent misuse of cyberspace by extremist and terrorist groups. The multiple components of the I4C scheme are created to achieve said goal.[232]

Given I4C's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Cyber Incident Preparedness and Response (I).

38. Technical and Economic Cooperation with Other Countries

To reduce cyber vulnerabilities, enhanced technical co-operation and strengthening relations with other countries is essential. Under MHA, technical cooperation with forensics laboratories that handle cases of cyber crime in Brazil and Sri Lanka were undertaken by Indian representatives in 2019.[233] This budget head also covers expenses for the work under MHA's Cyber and Information Security (CIS) division for its participation in international conventions on cyber security and cybercrimes.[234]

For the purpose of this brief, the activity-wise classification for Technical and Economic Cooperation with Other Countries in the budget analysis will be: International Cooperation and Investment Promotion (IV).

[232] Details About Indian Cybercrime Coordination Centre (I4C) Scheme, Ministry of Home Affairs, Government of India <https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme >
[233] Annual Report 2019-20, Ministry of Home Affairs, Government of India at p.164 <https://www.mha.gov.in/sites/default/files/AnnualReport_19_20.pdf>
[234] Annual Report 2018-19, Ministry of Home Affairs, Government of India at p.3 <https://www.mha.gov.in/sites/default/files/AnnualReport_19_20.pdf>

39. National Emergency Response System and Cyber Crime Prevention against Women and Children (NERS & CCPWC)

The CCPWC scheme consists of an online cyber crime reporting unit, forensic units, capacity building units, research and development unit and awareness creation unit. [235] The forensic units are designed to collect, preserve and analyse evidence related to cyber crime in line with the provisions of the IT Act and Evidence Act.[236] The Online Cybercrime Reporting Portal is a central citizen portal to register online complaints of cyber crime.[237] The Capacity Building Unit assists in the capacity building of central and state police forces, prosecutors, judges, and other stakeholders.[238]

Given NERS & CCPWC's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Cyber Incident Preparedness and Response (I).

40. The National Security Council Secretariat (NSCS)

The office of the National Cyber Security Coordinator (NCSC) functions within the aegis of the National Security Council Secretariat (NSCS), which supports the work of the National Security Council. In December 2019, it was the NSCS that issued a call for public comments for India's new National Cyber security Strategy for 2020-2025.[239]

Given the NSCS's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Cyber Incident Preparedness and Response (I).

[235] Details About CCPWC (Cybercrime Prevention Against Women and Children) Scheme, Ministry of Home Affairs, Government of India < https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-CCPWC-CybercrimePrevention-against-Women-and-Children-Scheme>
[236] Ibid.
[237] Ibid
[238] Ibid
[239] vide www.ncss2020.nic.in (this URL is no longer functional)

41. Office of the Principal Scientific Advisor (PSA)

In November 1999, Cabinet Secretariat established the Office of the Principal Scientific Adviser to the Government of India. The PSA's office aims to provide pragmatic and objective advice to the Prime Minister and the Cabinet on matters related to science, technology and innovation with a focus on application of science and technology in critical infrastructure, economic and social sectors in partnership with government departments, institutions and industry.[240] The PSA's role includes enabling preparedness in emerging domains of science and technology.[241]

The Empowered Technology Group (ETG) formulates and oversees national policies on research and development of technologies and provides advice that determines the direction of government's R&D and technology development plans,[242] and hence has a bearing on cyber security research and policy.

Given the PSA's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Technical Research & Capacity Development (II).

42. Prime Minister's Office

The PMO is the highest decision-making body on cyber security matters; the National Cyber security Coordinator reports to the PMO and NSA. The administrative structure of the PMO also includes an Officer on Special Duty (OSD) for Communications and Information Technology,[243] emphasising the role of cyber security at the highest levels in governance.

[240] PSA's Role, Office of the Principle Scientific Advisor, Government of India <https://www.psa.gov.in/about-us >
[241] About the PSA Office, Office of the Principle Scientific Advisor, Government of India <https://www.psa.gov.in/about-us >
[242] Ibid.

[243] List of Officers, Prime Minister Office <https://www.pmindia.gov.in/en/list-of-officers-pmo/>

For the purpose of this brief, the activity-wise classification for PMO in the budget analysis will be: Cyber Incident Preparedness and Response (I).

43. National Intelligence Grid (NATGRID)

Through the National Intelligence Grid (NATGRID) the government aims to link databases as an input in combating terrorism and create a facility to improve capability to counter internal security threats.[244] NATGRID is conceptualised as an interface to connect approved user agencies (security/ law enforcement) with designated data providers (airlines, banks, SEBI, railway, telecom, etc.).[245] It is envisioned by the government to be a seamless and secure database that provides real-time access to data on immigration, banking, individual taxpayers, air and train travel.[246] The project was approved by way of a notification after clearance was obtained from the Cabinet Committee on Security, but no legislation has been passed by Parliament to support this project.[247]

Given NATGRID's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Technical Research & Capacity Development (II).

(iii) Other Relevant Departments:

44. Unique Identification Authority of India (UIDAI)

The Unique Identification Authority of India (UIDAI), aims to provide Aadhaar, an identity infrastructure for delivery of various social welfare programs and

[244] Demand No. 24, Notes on Demands for Grants 2020-21, Ministry of Electronics and Information Technology, Government of India <https://www.indiabudget.gov.in/budget2020-21/doc/eb/sbe24.pdf >

[245] Unstarred Question No:3493, Answered On: 11.08.2015, Status Of NATGRID, (Lok Sabha) <http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=22670&lsno=16 >

[246] 'Explained | What is NATGRID, India's counter-terrorism platform?' (Money Control News, 13 September 2021) <https://www.moneycontrol.com/news/india/explained-what-is-natgrid-indias-counter-terrorism-platform-7459611.html>

[247] Gunjan Chawla and Smitha Krishna Prasad, Response to Call for Submissions on 'Surveillance Industry and Human Rights', Centre for Communication Governance at National Law University Delhi, February 2019, https://ccgdelhi.org/wp-content/uploads/2019/02/CCG-NLU-Response-to-Call-for-Submissions-on-Surveillance-Industry-and-Human-Rights_February-2019.pdf.

effective targeting of these services.[248] The government envisions it to add value to a range of applications and services that involve confirmation /verification as Aadhaar uniquely establishes online authentication of the identity of individuals through biometric attributes which determines proof of identity and proof of presence.[249] Ensuring the privacy and security of this centralised database is crucial to protect citizens' sensitive personal data and information entrusted to it.[250] To ensure the security and confidentiality of identity records and authentication information is part of the UIDAI's mission.[251]

Given UIDAI's mandate and for the purpose of this brief, their activity-wise classification for the budget analysis will be: Digital Identity (VI).

45. Department of Science & Technology - National Mission on Interdisciplinary Cyber Physical Systems (NM-ICPS)

Cyber Physical Systems (CPS) are a new class of engineered systems that integrate computation and physical processes in a dynamic environment.[252] CPS includes technology areas of cybernetics, mechatronics, design and embedded systems, Internet of Things (IoT), Big Data, Artificial Intelligence (AI) and others.[253] The CPS systems are expected to drive innovation in sectors like agriculture, water, energy, transportation, infrastructure, security, health and manufacturing.[254] Cyber security plays a critical role in the safeguarding the implementation and use of these technologies. The National Mission on Interdisciplinary Cyber Physical Systems (NM-ICPS) in its first phase of

[248] About UIDAI, Unique Identification Authority of India, Government of India, < https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html>.
[249] Vision & Mission, Unique Identification Authority of India, Government of India < https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/vision-mission.html>
[250] Chinmayi Arun, *Towards a Database Nation,* The Hindu, 27 September 2016, https://www.thehindu.com/opinion/op-ed/Towards-a-database-nation/article15000828.ece; Kritika Bhardwaj, *Explainer: Aadhaar is vulnerable to identity theft because of its design and the way it is used*, Scroll.in, 2 April 2017, https://scroll.in/newsrepublic/833230?s=cm.
[251] Vision & Mission, Unique Identification Authority of India, Government of India < https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/vision-mission.html>
[252] Demand No. 87, Notes on Demands for Grants 2020-21, Ministry of Science and Technology, Government of India < https://www.indiabudget.gov.in/budget2020-21/doc/eb/sbe87.pdf >
[253] Ibid
[254] Ibid

implementation has a dedicated domain for cyber security and cyber security for physical infrastructure.[255]

For the purpose of this brief, the activity-wise classification for the Department of Science & Technology's National Mission on Interdisciplinary Cyber Physical Systems in the budget analysis will be: Technical Research & Capacity Development (II).

46. Ministry of Corporate Affairs - Corporate Data Management

The Scheme of Corporate Data Management seeks to create an in-house data mining and analytics facility in the Ministry of Corporate Affairs to effectively utilise the vast repository of information held in its corporate registry.[256] In addition to providing authentic and clean data to all stakeholders in a more accessible manner, the facility aims at making available the information in an organised and structured manner to the Ministry and to other policy and decision-making agencies within and outside the government.[257]

For the purpose of this brief, the activity-wise classification for the Ministry of Corporate Affair's Corporate Data Management in the budget analysis will be: Cyber Incident Preparedness and Response (I).

47. Ministry of Finance - Technical and Economic Cooperation with Other Countries

The budgetary provision is for contribution towards technical and economic cooperation with other countries (this includes contributions to the United Nations Development programme, the Global Environment Trust Fund, etc.)[258] under the Department of Economic Affairs.

---

[255] National Mission on Interdisciplinary Cyber Physical Systems, Science and Engineering Research Board, Department of Science & Technology, Government of India <http://serb.gov.in/nm-icps.php>
[256] Ministry of Corporate Affairs, Government of India, *About: Corporate Data Management*, < https://www.mcacdm.nic.in/about-us.php>
[257] Ibid
[258] Department of Economic Affairs, Ministry of Finance, Government of India, *Demand No. 30*, Demands for Grants, 2022-23, < https://www.indiabudget.gov.in/doc/eb/sbe30.pdf>

For the purpose of this brief, the activity-wise classification for the ministry of Finance's Technical and Economic Cooperation with Other Countries in the budget analysis will be: International Cooperation and Investment Promotion (IV).

B. Activity Wise Allocations

In accordance with the Three Pillars strategy to Secure, Strengthen and Synergise the country's cyber security framework, we re-classified the 47 identified budget heads from the ministry-wise classification under the following six activities that represent different components of the cyber security ecosystem. This re-classification of budget heads has been presented below in tabulated formats to allow for a comprehensive overview of what each activity in this analysis comprises. The four relevant budget heads for cyber security across ministries introduced in the Union Budget 2022-23[259] have not been included in the dataset used for activity-wise analysis to avoid inflation of total budgeted allocations for FY 2022-23. Further, while certain departments undertake a range of activities, they have been classified in accordance with their predominant area of activity.

(i) Cyber Incident Preparedness and Response Component (Secure/Strengthen)

This activity comprises improving management and response to cyber attacks, threats and incidents to minimise their impact in terms of monetary and data losses. Improving capacities to anticipate, assess and act on risks in the cyber domain form a key component of this activity.

MeitY	DoT	MHA	Other

[259] These include (1) Modernisation of Forensic Capacities under MHA (2) Digital Intelligence Unit Project under DoT (3) Production Linked Incentive (PLI) Scheme to Promote Telecom and Networking Products Manufacturing in India under DoT and (4) PLI for Large Scale Electronics and IT Hardware under MeitY.

Cyber Security (CERT-IN)	Telecom Computer Emergency Response Team	Modernisation of Police Forces and Crime and Criminal Tracking Network Systems (CCTNS)	Ministry of Corporate Affairs - Corporate Data Management
E-governance (Digital India)	Wireless Monitoring, Planning and Coordination (Total)	Indian Cyber Crime Coordination Centre (I4C)	
Cyber security projects (NCCC and others) (Digital India)		National Emergency Response System and Cyber Crime Prevention against Women and Children (NERS & CCPWC)	
		National Security Council Secretariat (NSCS)	
		Prime Minister's Office (PMO)	

(ii) Technical Capacity Building and Research & Development Component (Strengthen/Synergise)

Efforts towards research and innovation in cyber security technologies as well as promotion of infrastructure production form the backbone of a secure cyber ecosystem. Research and development of electronics, information security and emerging technologies are included under the ambit of this activity.

MeitY	DoT	MHA	Other
National Informatics Centre (NIC)	Centre for Development of Telematics (C-DoT)	Criminology and Forensic Science	National Mission on Interdisciplinary Cyber Physical

			Systems (Department of Science and Tech)
National Knowledge Network (Digital India)	Promotion of Innovation and Incubation of Future Technologies for Telecom Sector	Office of Principal Scientific Advisor (PSA)	
Promotion of electronics and IT Hardware Manufacturing (Digital India)	5G Connectivity Test Bed	National Intelligence Grid (NATGRID)	
R&D in electronics/IT/Convergence, Communications & Broadband Technologies (CCBT) (Digital India)	Promotion of Innovation and Incubation of Future Technologies for Telecom Sector		
C-DAC (Centre for Development of Advanced Computing)			
C-MET (Centre for Materials for Electronics and IT)			
C-MET (Centre for Materials for Electronics and IT)			
SAMEER (Society for Applied Microwave Electronics Engineering and Research)			
Convergence, Communication & Strategic Electronics			

(iii) Human Resource Development Component (Strengthen)

Ensuring security of information and networks requires people in the cyber ecosystem to have awareness and knowledge on best practices and security standards, be equipped with technical tools and follow systematised protocols in the event of a cyber attack. This component thus involves promotion of skills and qualifications among people that foster a culture of cyber security to strengthen cyber security at the national and organisational level. Programmes and departments that undertake training of human resources towards this end have a critical role in development of the country's cyber security and have been included under this activity for our analysis.

MeitY	DoT	MHA	Other
National Institute of Electronics & Information Technology (NIELIT) (erstwhile DOEACC)	Human Resource Management (National Institute of Communication Finance)	Police Education, Training and Research	
Manpower Development (Digital India)	Labour, Employment and Skill Development		
Pradhan Mantri Digital Saksharta Abhiyan (PMGDISHA) (Digital India)			

(iv) International Cooperation and Investment Promotion Component (Secure/Synergise)

In order to promote a free, open and secure cyberspace, co-operation with international partners, organisations and other countries is essential. Efforts made in this direction can help balance the country's national security interests and economic prospects globally. Investments for building infrastructure to share

information with other countries on criminal and malicious cyber activity will also ensure prevention and detection of serious cybercrimes in the international sphere.

MeitY	DoT	MHA	Other
Promotion of IT/Information Technology Enabled Services (ITeS) Industries (Digital India)	Technology Development and Investment Promotion	Technical and Economic Cooperation with Other Countries	Ministry of Finance - Department of Economic Affairs - Technical and Economic Cooperation with Other Countries
Foreign Trade and Export Promotion	South Asia Sub-Regional Economic Cooperation (SASEC) Information Highway Project		

(v) Standardisation, Quality Testing and Certification Component (Strengthen)

The standardisation and quality of security standards relies on organisations that can provide consistency and clarity on best practices in cyber security to governments and businesses. This activity comprises the undertaking of security services such as certifications, audits, calibration, testing and training of IT systems for private and public organisations.

MeitY	DoT	MHA	Other
Standardisation, Testing, Quality and Certification (STQC)	Telecom Regulatory Authority of India (TRAI)		
Controller of Certifying Authorities (CCA)	Telecom Testing and Security Certification Centre		

	Telecom Enforcement Resources and Monitoring Cells (TERM)		
	Central Equipment Identity Register (CEIR)		
	Telecom Engineering Centre (TEC)		

(vi) Digital Identity Component (Secure, Synergise)

The security and robustness of national digital identification systems is essential to protect sensitive personal information of citizens. With use of cloud technologies for storage of personal and non-personal data, cyber security plays an important role to prevent misuse of information from Digital ID systems.

MeitY	DoT	MHA	Other
			Unique Identification Authority of India (UIDAI)

This classification includes UIDAI as the predominant digital identity infrastructure provider.

III. Data Analysis

CCG's Cyber security Budget Dataset forms the primary source for all data referenced, and trend analysis presented in this report. The objective of our data analysis is to present a descriptive overview of the changes in allocations and their outcomes for the schemes and programs identified as relevant for cyber security in this report. This furthers our understanding of the various frontiers for cyber security spending in India and lays the foundations for future cyber security expenditure analysis.

The quantitative analysis in the brief employs two primary mathematical computations to understand changes and trends in the cyber security budget across ministries from FY 2012-13 to FY 2022-23. These include, Compound Annual Growth Rate (CAGR) and Year-on-Year percentage change (YoY % Change) across financial years. The formulas for both and the contexts of their utilisation in this report are presented below.

CAGR is a percentage-based metric used for determining the annual rate at which expenditures grow over a certain period of time. This formula is applied to understand long term trends in the total cyber security allocations and spending from FY 2012-13 to FY 2022-23, for which the rate of change varies year-on-year.

$$\text{CAGR} = \left(\frac{V_{Latest}}{V_{Initial}} \right)^{\left(\frac{1}{t}\right)} - 1$$

where; V_{Latest} is value for the latest financial year up till which CAGR is to be computed

$V_{Initial}$ is the value for the starting financial year from which CAGR is to be computed

t is the number of years for which CAGR is being computed

YoY% changes enable comparison of expenditures from a point in time in one year, to the same point in time from the previous year. This formula is applied to understand annual change in budgeted and actual expenditures for each ministry's total cyber security allocation in Part III of this report.

$$\text{YoY \% Change} = \frac{(E_1 - E_b)}{E_b} \times 100\%$$

where; E_1 is the next year's expenditure value

E_b is the previous /base year's expenditure value

IV. Interpretation Guidance

It is important to bear in mind that none of the figures discussed in this brief are an indication of actual expenditure incurred by the Government of India on cybersecurity. Instead, these figures must be viewed as the pool of financial resources available to government to strengthen the state of cyber security and various aspects of internet governance related thereto at the national level, including the security of e-governance initiatives to facilitate the online delivery of public services to citizens.

This is due to the fact that entire budgeted allocations for all the programmes and schemes in our analysis are not utilised exclusively for cybersecurity and its related activities. The current format of the Demands for Grants does not allow for inference of the precise share of budgeted allocations that are actually used for activities directly related to cybersecurity. All budget heads included in our analysis therefore fall on a spectrum of high significance to low significance with respect to percentage share of their budgeted allocations being utilised for cybersecurity. For certain budget heads, it is likely that a greater share of the allocation is directed towards cybersecurity related activities.

For example, it is likely that for Cybersecurity projects under the Digital India scheme and CERT-In, both under MeitY, the entire allocation is directly relevant for cybersecurity. On the other hand, for budget heads such as the Prime Minister's Office under MHA, only a specific percentage of the total allocated budget is likely to be directed towards cybersecurity activities. However, there exist no relevant mechanisms to establish what percentage of these allocations can be taken as relevant for cybersecurity activities, and thus the entire allocation has been included for such budget heads in our analysis.

The dataset upon which the present analysis is based, is available on request to ccg@nludelhi.ac.in

V. Limitations of Analysis in the Cybersecurity Budget Brief

1. Expenditure figures in this brief are estimations of the total cybersecurity budget that are indicative of the entire pool of resources

available for cybersecurity. These figures must be viewed as the pool of financial resources available to government to strengthen the state of cyber security and various aspects of internet governance related thereto at the national level, including the security of e-governance initiatives to facilitate the online delivery of public services to citizens, and not actual direct spending on cybersecurity. This is due to the fact that entire budgeted allocations for all the programmes and schemes in our analysis are not utilised exclusively for cybersecurity and its related activities. The current format of the Demands for Grants does not allow for inference of the precise share of budgeted allocations that are actually used for activities directly related to cybersecurity. All budget heads included in our analysis therefore fall on a spectrum of high significance to low significance with respect to percentage share of their budgeted allocations being utilised for cybersecurity. For certain budget heads, it is likely that a greater share of the allocation is directed towards cybersecurity related activities. For example, it is likely that for Cybersecurity projects under the Digital India scheme and CERT-In, both under the Ministry of Electronics and Information Technology, the entire allocation is directly relevant for cybersecurity. On the other hand, for budget heads such as the Prime Minister's Office under Ministry of Home Affairs, only a specific percentage of the total allocated budget is likely to be directed towards cybersecurity activities. However, there exist no relevant mechanisms to establish what percentage of these allocations can be taken as relevant for cybersecurity activities, and thus the entire allocation has been included for such budget heads in our analysis.

2. This analysis does not include certain ministries that are of relevance to cybersecurity. There are budget heads under the Ministry of Defense, Ministry of External Affairs, Department of Telecommunication and Ministry of Home Affairs that can possibly be utilised for cybersecurity-related activities. However, their expenditure values are at best an estimate of the total funds available which may be utilised for cybersecurity-related functions. It is not possible to infer from the current format of the Demands for Grants the precise share of these allocations that are actually used for activities directly related to cybersecurity. While it is important to highlight these areas of potential for cybersecurity – as supporting allocations – including them in our analysis would inflate allocations for cybersecurity and skew findings.

3. Incomplete expenditure data under certain ministries' Demand for Grants limits the scope and applicability of the analysis in this brief. There are instances of unavailable expenditure data for budget heads under the Ministry of Electronics and Information Technology and the Department of Telecommunications over the last decade. In some cases, budget heads have allocated expenditures but data on revised and actual expenditures remains unavailable without articulations of the reasons for such gaps. Incomplete budget datasets limit the veracity of analysis due to the ambiguity between cases of underutilisation of funds and bottlenecks in presentation of data in the Union Budget.

4. Four new budget heads that were introduced in the Union Budget FY 2022-23 have not been included in our analysis. These have been identified under their relevant ministries and include, (1) Production Linked Incentive (PLI) for Large Scale Electronics and IT Hardware under Ministry of Electronics and Information Technology (2) Digital Intelligence Unit Project under Department of Telecommunications (3) Production Linked Incentive (PLI) Scheme to Promote Telecom and Networking Products under Department of Telecommunications and (4) Modernisation of Forensic Capacities under Ministry of Home Affairs. These budget heads have not been included in our analysis of trends in Part III and Part IV in order to maintain consistency in budget heads tracked over the last decade. However, any future analysis of India's cybersecurity budget should include these budget heads as well, subject to continued allocations towards the same.

Centre for Communication Governance
National Law University Delhi | Sector 14, Dwarka
New Delhi – 110078, India
ccgdelhi.org | privacylibrary.ccgnlud.org
Email: ccg@nludelhi.ac.in Twitter: @CCGNLUD