DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

GEARING UP FOR DIGITAL++

REIMAGINING SECURITY AND TRUST

EDITED BY
Rama Vedashree
Munish Sharma

GEARING
UP FOR

DIGITAL++

REIMAGINING SECURITY AND TRUST

EDITED BY
Rama Vedashree
Munish Sharma

First edition: 2023

Gearing Up for Digital ++ Reimagining Security and Trust

published by:

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

4th Floor, NASSCOM Campus
Plot No. 7-10, Sector 126, Noida
Uttar Pradesh 201303, India

“Digital transformation of various governance processes is core to the vision of creating a digitally empowered society and knowledge economy and ensuring efficient delivery of services. Digital public infrastructure is going to lay the foundations of this endeavour and help bridge the digital divide which is one of the top priorities for Government of India and State Governments. **It is our shared responsibility to ensure security and trust in the solutions built on top of these infrastructure.** I am happy to note this new initiative from Data Security Council of India. An edited volume such as this, can help aggregate views from industry and technology leaders on some of the pertinent themes, as we enter a phase of accelerated digitalization.”

Alkesh Kumar Sharma
Secretary, Ministry of Electronics and Information Technology, Government of India

“India is pioneering digital inclusion at scale, and our adoption of emerging technologies for public services delivery is now receiving global recognition. The Government of India and National Security Council Secretariat (NSCS) are giving equal attention to make security and trust as the foundations of our digital transformation. Issues such as unrelenting cyber-attacks and ransomware and supply chain security not just pose threats but also act as roadblocks in technology-led governance. Cyber cooperation is now a key pillar of all our diplomatic efforts, and going forward the evolving challenges and risks of wide scale adoption of digital solutions needs a concerted effort from the government and industry. Publications such as this volume, *Gearing up for Digital++* help bring out perspectives of diverse stakeholders and contribute to informed debate, discourse and collaboration.”

Lt Gen (Dr) Rajesh Pant
National Cyber Security Coordinator, Government of India

“Digital is today embedded in all aspects of our lives, governance, business transformation, customer experience and innovation. The technology industry in India has been at the forefront of leading the digital transformation agenda globally and in India. The government has also built the public digital infrastructure that is enabling inclusion and scale. As technologies continue to evolve and enterprises and governments gear up for what's next in digital, the importance of trust and security becomes even more critical. This collection of curated articles from thought leaders will serve as a useful reference for leaders to understand varied perspectives and keep trust and security at the centre of their digital strategy.”

Debjani Ghosh
President, NASSCOM

Contents

Part 3: Future of Digital ++

Foreword

From the vantage point of a technologist, we are entering an exciting phase of digitalization. Technologies in the digital space that had seemed more like science fiction a decade ago, are now making inroads into our daily lives. We may soon witness the boundaries between our physical and digital worlds and identities fade away. Fast-paced innovation in the digital era will certainly disrupt many business models and spawn new ones, which are perhaps beyond our comprehension at present.

From a business opportunity and growth perspective, success in this phase would not just depend on the capacity and capability to innovate, but also on the environment in which futuristic businesses could thrive. Going forward, the businesses built around digital would need to be responsible and accountable in their design, development and deployment of technology. They would also need to ponder on the best ways to build privacy, security and transparency in digital systems and ensure that these principles transition from rhetoric to action.

Users would desire regulation and oversight to establish trust and confidence in the products, services and systems they adopt in their digital journey. They may also seek and exercise digital equivalents of human rights and civil liberties. Our approaches to the regulation of technology will need to become agile as we tread and get to learn more effective and efficient ways. With their growing strategic relevance, digital technologies have unfortunately become embroiled in geopolitical tussles. Notwithstanding this, we are going to see states with shared interests and values charting out frameworks for cooperation.

As part of its charter to expand India's share in the global cybersecurity product and services industry, DSCI has a thought leadership mandate transcending contemporary security and policy issues. Through initiatives such as this edited volume, DSCI looks forward to adding value to the discourse on some of the themes outlined above. It complements the core initiatives of DSCI on cybersecurity and privacy. I hope the endeavour succeeds in disseminating these ideas and themes to a wider audience of technology leaders and policy makers and benefits others interested in the subject. We will continue to undertake similar initiatives to stir candid discussions and deliberation, which inform policymaking in this dynamic space. After all, it is only through open dialogue and participation that we can shape our collective digital future.

Rajendra S Pawar
Chairman, DSCI
Chairman & Co-Founder, NIIT Group

From The CEO's Desk

It is in the nature of technology to evolve, grow in leaps and bounds, and sometimes disrupt the existing markets or even outpace laws and regulations. No doubt, technological advancements and innovations in the digital space provide endless opportunities, but at the same time they pose various challenges pertaining to ensuring security and mitigating threats to beneficiaries' privacy and freedoms. The dilemma all stakeholders face is to achieve a fine balance between the genuine needs of technological advancement and protection of privacy and security. At DSCI, we continuously strive to promote innovation, while working with the relevant stakeholders to address security and privacy concerns that emerging technologies may give rise to.

With this goal in mind, we look at the future of digitalization and gear up. It is our firm belief that the coming decade will be the defining years in which privacy and security practices, frameworks and technologies are developed, assessed, and put to the test of regulation. We at DSCI see it as our duty to help ready the industry and government ecosystems for what is yet to come, or for the unforeseen. That was the sole motivation behind this edited volume, *Gearing up for Digital++: Reimagining Security and Trust*, that is, to bring together industry leaders and experts, and ponder on what is on the 2030 horizon for cybersecurity, privacy, data protection and emerging technologies. We believe this endeavour will trigger further discussions, dialogues and also give us some sense on how we approach future proofing innovation and help laws and regulations evolve with rapidly advancing digital technologies.

Vinayak Godse
CEO, DSCI

Introduction

Rama Vedashree and Munish Sharma

Over the last decade, we have witnessed an accelerated pace of digital transformation across the world, leading to the wide scale adoption of digital technologies and enabling new drivers of economic growth. The adoption of digital technologies to transform businesses and governance functions has had wide-ranging impact on different sectors of the economy, not to mention enormous developmental and social benefits. Digitalization is also enabling governments to increase transparency and effectively deliver services, simultaneously helping them pursue inclusive and sustainable growth. The unprecedented disruption wreaked by the COVID-19 pandemic has given impetus to advance agility, resilience, and digital transformation across all industry verticals as well as governance functions.

Digitalization requires efforts on multiple fronts of technology innovation and development, infrastructure, services, data governance, regulatory frameworks, and capabilities and skills. This endeavour has its own set of challenges. For instance, despite the best efforts made to raise the levels of digital adoption, close to half of the world's population remains deprived of the transformative benefits of digital technologies. Security threats in the digital realm, growing both in numbers and sophistication, undermine business competitiveness and erode trust and confidence of the end user in digital systems. Protection from digital security threats entails

striking the right balance between national security considerations, business interests, and human rights and civil liberties.

With the ever-increasing demand for connectivity and exchange of data, it is imperative to enhance trust in digital technologies through secure, responsible, and accountable development of technology. Innovation in digital technologies is raising new governance and regulatory challenges for governments across the globe. These developments also call for international cooperation over technology standards and governance frameworks across bilateral, plurilateral, and multilateral fora. But this is easier said than done in the face of geopolitical competition permeating into the digital space, which makes fostering cooperation among states an uphill task.

With the sustained efforts of public and private sectors in building infrastructure and propel digital consumption over more than two decades, India is now one of the largest hubs for digital products and services. India's information technology industry is now one of the fastest growing in the world, and it also houses more than 1500 Global Competency Centers along with the third largest tech startup ecosystem. Concomitantly, India has undertaken digital transformation initiatives at scale and prioritized digital platforms for driving digital and financial inclusion. The private sector has also played a proactive role in reinforcing the efforts of the government for cybersecurity and protection of data and privacy.

The digital realm is witnessing an increasing convergence of the physical and virtual worlds. The application of technologies like Artificial Intelligence, 5G, IoT, and Quantum are slated to empower individuals and create immense business and employment opportunities. However, the persisting absence of clearly defined regulatory and governance frameworks may impede realizing the true potential of digitalization for India's socio-economic growth. There is no denying that the need of the hour is to instill accountability and ethics in the development of

digital technologies, build trust and confidence in their use, and support this pursuit with agile and flexible policy approaches. The security challenges here are transnational and would require accommodation between competing national interests and priorities.

Against the backdrop of the unfolding phase of digital era and its reverberations for governments, industry and society, DSCI embarked on an initiative to bring together thought leaders from the diverse backgrounds of industry, policy, diplomacy and law to pen articles and point of views on some of the pertinent themes of our times into an edited volume. "Digital ++" in the title of this volume denotes the next phase of digitalization. Aligned with DSCI's thought leadership mandate, it reflects on security, trust, privacy and other prominent issues arising out of the contemporary developments in digital space which have implications both for the industry and policy making at large.

This volume is divided into three sections. The first one touches upon the aspects of digital infrastructure and standards, sustainability and data-driven innovation. The second section revolves around security facets of supply chains, hybrid war and ransomware, self-sovereign identity, and quantum technologies. The third section spans the diverse themes of digital human rights, digital health, and cyber diplomacy and norms.

Rahul Matthan offers a comprehensive overview of India's efforts in developing digital public infrastructure. Arguing how India's approach could be a viable option for other countries and extend the benefits of digital to the next billion, he elaborates, with examples, the principles and elements of digital public infrastructure in India.

Jesse McWaters and Anand Raghuraman underscore the imperatives of global standards for a digital economy, and expand on their benefits and the emerging geopolitical competition at standards-setting bodies. They lay emphasis on the opportunity

before India to shape global digital standards, and discuss the premise of such engagement and technology priorities.

Stressing on the need of a regulatory environment that fosters responsible and trusted use of data and technology, Bojana Bellamy draws attention to organizational accountability as an essential feature in facilitating responsible data-driven innovation. She describes how incentives for the implementation of accountability measures could help create a fertile environment for business development and growth.

Arundhati Bhattacharya emphasizes on the importance of investments in digital technologies to reduce emissions, against the backdrop of the impact of climate change on economic growth. She prescribes an approach to the companies embarking on their journey towards sustainability, and explains how cloud adoption could result in the reduction of energy consumption and carbon emissions.

With supply chain security making to the top of business risks, Daisy Chittilapilly underscores the importance of visibility in supply chains and identifying gaps, and embracing technology solutions that support decisions, and making operations more efficient. She sheds light on managing supply chain risks without hindering day-to-day business.

Tom Burt delves into the increasing use of cyberweapons during geopolitical conflicts to achieve strategic objectives, deployed stand alone, as a tactic, or alongside or in support of conventional weapons in a hybrid war. He expounds the relevance of cyber norms in mitigating the risks and impacts of hybrid conflict and improve cyber resilience, and draws learnings from the ongoing Russia-Ukraine conflict.

Steve Ledzian dissects the evolution of ransomware, which over the years has emerged as a major national security risk, and argues that an effective mitigation strategy should consider this as a human driven digital intrusion rather than simply a "malware".

He prescribes preventing intrusions to check ransomware attacks, and recommends few measures effective for mitigating the risks of modern ransomware.

As self-sovereign identity gains pace and seeks to put the users in control of their personal data, Team Polygon describes various uses of Zero Knowledge Proofs (ZKPs) across the entire spectrum of self-sovereign identity architectural layers and explains in detail a decentralized and privacy preserving solution based on ZKPs.

In light of the global advancements in the quantum technologies space, Sunil Gupta presses on the need for immediate action to ensure security in the present context as well as to prepare for future technology advances. He underscores Quantum cryptography and Post-Quantum Cryptography as the two solutions and touches upon Crypto-agility.

Vakul Sharma attempts to decipher the concept of Digital Human Rights, and argues why this aspect needs innovative thinking. He offers a critique of the approach United Nations has taken for the protection of human rights online, assesses the policy and regulatory framework for digital human rights in the Indian context and argues to place citizens at the core of this concept.

Digital healthcare witnessed a growth spurt following the COVID-19 pandemic. Calling this trend of ubiquitous and personalized access to healthcare a new "digital normal", Sangita Reddy explains how to build trust and confidence in digital health among healthcare receivers as well as the providers. She advocates for a hybrid approach, which retains the human touch in digital healthcare too.

Syed Akbaruddin draws attention to the challenges of cyberspace diplomacy and begins with the observation that the cyberspace still has a nebulous diplomatic status. Looking at the evolution of intergovernmental processes and dialogues on cyber governance and the prevalent multistakeholder model, he argues that the contemporary dynamics of cyberspace demand state intervention.

Considering the slow progress on cyber norms, Arvind Gupta asserts that the issue of state responsibility in the cyberspace has assumed even greater urgency given deepening geopolitical uncertainties. Analysing the UNGGE process and the recent UNGGE and OEWG reports, he anticipates inclusive and candid discussions to put normative frameworks or rules of the road in place.

We hope this volume expands the existing body of knowledge and fulfils the purpose of discussing the contemporary and emerging policy issues pertaining to security, privacy, rights, trust, geopolitics, diplomacy in the digital realm. We are grateful to the contributors who took the time out of their busy work schedules to think and pen down articles and point of views for this volume. We were aided in no small measure by a committed and diligent DSCI team. Deepa Ojha facilitated coordination with the contributors and their timely submissions. Amit Ghosh and Charu Sharma drove the immaculate design and publication of this volume. Acknowledgements are also due to our copyeditor, Priyanka Sarkar. We are truly thankful to all the individuals who have either motivated or supported this publication in their professional or personal capacities.

Part 1

Accelerating Digital ++

Digital Infrastructure for The Next Billion

Rahul Matthan and Shreya Ramann

Introduction

With over 5.3 billion[1] internet users, as much as 66 percent of the global population was online in 2022. A wide range of services – health, communication, payments, commerce and even aspects of government administration – are accessible online, offering convenience, wider access and greater accountability than ever before. If anything, the COVID-19 pandemic strengthened our reliance on these digital technologies[2], demonstrating their resilience when physical interactions were radically curtailed.

For the most part, the explosion of digital technologies has been powered by private enterprises. Most of the services we access through digital means are facilitated, directly or indirectly, by infrastructure established and maintained by large technology corporations. Thanks to their global presence and vertically integrated design, these corporations serve as gatekeepers to our online experiences.

In many instances, the scale and pervasiveness of these platforms have also had harmful consequences. Regulators around the world are grappling with the monopolistic repercussions of network effects, the privacy implications of entrusting personal data to private corporations and protection of consumers from the

consequences of vertically integrated commerce at scale. On the other hand, new issues such as the lost opportunity inherent in data silos under the exclusive control of data collectors and the potential of data-driven innovation demand a different type of regulatory intervention in order to leverage data for the larger public good.

Different countries have adopted divergent approaches to these challenges. In the US, for instance, regulation has been laissez faire with private enterprises being given a free hand. For most of the history of the Internet in the US, the legislative and judicial philosophy has been to allow market forces to determine what can and cannot be done online. To the extent they were enacted, regulations tended to be light touch and after-the-fact.[3]

Europe, on the other hand, developed a strong regulatory framework aimed at protecting the rights of individuals by imposing a heavy compliance burden on data collectors. Today the General Data Protection Regulation (GDPR)[4] is widely recognized as the global benchmark for privacy regulation. Europe is currently in the process of buttressing and augmenting the GDPR with a new European Digital Strategy,[5] aimed specifically at addressing digital markets and services as well as creating spaces for data sharing to unlock the value inherent in these data silos.

Through the establishment of a powerful, population-scale Digital Public Infrastructure (DPI), India developed a framework for data governance that offers an alternative to both the American and European models mentioned above. This techno-legal architecture establishes a technology infrastructure into which legal principles can be encoded in such a way that data governance can be enforced, not through the obligation to comply with regulations but through the operation of the infrastructure itself.

India's example demonstrates that DPI is a viable alternative through which the next billion can access the benefits of digital technologies. For it to be replicable, however, we will need to better understand the essential features of the Indian model of DPI.

The Indian model of DPI

India has deployed a novel approach to the establishment of DPI that retains regulatory control over the infrastructure with the government – to ensure that data governance conforms with the law and national interests – while at the same time leveraging the power of innovation in the private sector to drive market adoption. By putting the core responsibility for data governance in the hands of the public sector, the Indian Model attempts to mitigate some of the potential risks of leaving the design of digital infrastructure entirely on the private sector. At the same time, by involving the private sector in the roll-out of the infrastructure, it benefits from the innovation and market orientation that these entities provide which is necessary for the large-scale adoption of this infrastructure.

IndiaStack

The most widely referenced example of Indian DPI is IndiaStack. This digital infrastructure is built on the foundational layer of digital identity provided by Aadhaar, India's digital identity system upon which layered applications and platforms provide services such as electronic know-your-customer (eKYC), digital signatures (eSign) and credentials (Digi-Locker).

The next layer of IndiaStack is the payments layer implemented through the Unified Payments Interface and operated by the non-profit entity, National Payments Corporation of India (NPCI). While NPCI regulates the digital payments ecosystem and manages the infrastructure through which digital payment messages are routed, private sector participation is permitted and players like Google and Walmart currently dominate the sector.[6] Arguably, owing to the efforts of these third-party entities the digital payments market in India has grown into one of the most vibrant, competitive and successful payment ecosystems in the world, clocking more than 6 billion transactions a month.[7]

The third layer in the stack is the data transfer layer which offers users greater autonomy over their personal data. Data Empowerment Protection Architecture[8] establishes a new category of intermediaries called consent managers through which consent flows are disaggregated from the data flows. The transfer of personal data from entities that currently hold that information to entities that are requesting it could be authorized by the data user to whom such data pertains, by providing their electronic consent.

Elements of DPI in India

The following three core elements are central to the Indian model of DPI:

Open Protocols

All Indian DPI are based on open specifications. Central to this is a set of open protocols that define how digital interactions take place between participants in the ecosystem. The protocols are defined by the government and maintained under its control. From time to time, these protocols are updated and all market participants conform their systems to the revised protocols. Since the protocols are open, private sector participants can easily integrate their proprietary systems with the DPI allowing them to leverage the benefits these platforms provide for their own commercial objectives. At the same time, the digital infrastructure benefits from the entrepreneurial zeal that drives the private sector to acquire more customers and build better and efficient services.

Modular and Interoperable

All Indian DPI is designed to be modular and interoperable– precisely why it is often described as a stack. They are composed of several different building blocks layered one on top of the other to create the complete infrastructure. Since the building blocks are modular, they could be re-used across a range of different DPI thereby avoiding the need to reinvent the wheel. Since they

are interoperable, one DPI could be integrated as an essential component of other DPIs and used to connect one DPI to another.

Unbundled Processes

Rather than simply digitizing existing processes, Indian DPI is created by unbundling them into their constituent elements so that they could be reassembled in the manner most suited to achieve the stated objectives. This unlocks efficiencies by rendering traditional offline processes redundant through the provision of computational guarantees of authenticity and veracity of identity. In addition, this makes it possible to re-imagine how things can be done, offering alternatives to legal requirements and procedural obligations.

In addition to these design elements, all Indian DPI are located within regulated environments that are supervised by a sectoral regulator. For the most part, DPI are regulated directly by entities established by the government for a specific purpose or by existing regulators, either directly or through non-profit organizations that function as self-regulatory organizations in the sector. These regulatory and self-regulatory organizations ensure accountability, adherence to technical specifications and compliance with the conditions of participation in the ecosystem. Regulations, to the extent that they apply, are typically light-touch policies and self-regulatory measures.

Examples of DPI

India has rolled out DPI built using these principles across various sectors. In the financial services sector, it has been rolled out through the Account Aggregator framework,[9] which has eventually become the largest open banking initiative in the world. A similar roll-out is underway in the health sector.[10] This section spotlights two examples of emerging DPI. The first is the Open Network for Digital Commerce (ONDC), a DPI aimed at addressing some of the challenges inherent to vertically-integrated and location-based commerce. The second is Bhashini, a DPI

that uses artificial intelligence and natural language processing to enable translation between various Indian languages in order to make content more widely accessible. Though these examples occupy widely divergent spaces, they demonstrate how digital platforms built on the principles described above could have immense benefits for the next 1 billion.

ONDC

The Indian digital economy is growing at an extraordinary pace. By 2030 it is projected to be a USD 800 billion market, growing 10 times from its value in 2020.[11] The proliferation of smartphones, digital payments through UPI, and the push for greater digitalization during the COVID-19 pandemic are among the many reasons behind this dramatic growth[12]. The e-commerce market alone is expected to be valued at $120 billion by 2026, a significant increase from USD 38 billion in 2021.[13]

The Indian e-commerce industry today is completely vertically integrated. Buyers and sellers must be on the same platform to be discoverable to each other. This has resulted in a dramatic consolidation of the market to the point where two large e-commerce companies dominate the market.[14] The same is the case in the mobility and delivery sectors as well. Since all these platforms are vertically integrated, ancillary but necessary services– such as warehousing, logistics and delivery – they are completely under the control of the platform, resulting in restrictive supply chains that lock sellers in and make it impossible for smaller service providers to participate. This asymmetry means that customers' choices are limited, which in turn impacts service quality and customer experience. It also results in customers losing control of their own data, locking them in through customized offerings and self-promotions. Sellers, on the other hand, are unable to transact on their own terms and at the same time they have no option but to participate given the extent to which digital platforms control consumer access.

The Open Network for Digital Commerce (ONDC)[15] has been developed against this backdrop. ONDC unbundles traditional e-commerce workflows into its constituent parts – discovery, ordering, payment and fulfilment – and offers protocols for each of them. This allows service providers to offer any one or more of these components in such a manner that it integrates with any other service provider offering any of the other services. A network of open protocols enables all ecosystem participants to be visible to each other and transact with each other through any application or platform integrated with the ONDC.

ONDC is designed using open protocols. At its heart lie the registries (which document participants and platform policies) and gateways (that enable buyers and sellers to be discoverable across ONDC-enabled platforms and interact with each other in the manner described by the protocol). Participants transact with each other across platforms through a series of open APIs that relate to different aspects of the e-commerce workflow.

The participants experience the service through applications– buyer apps through which consumers of goods and services can review catalogues and order and purchase goods and services, and seller apps through which various seller catalogues are aggregated and presented.

The ecosystem is operated and managed by a non-profit company established by the Department for Promotion of Industry and Internal Trade. While this is the entity responsible for building and maintaining the underlying infrastructure (including registries, gateways and protocols), no single entity will own or control the network. The network will scale through the efforts of the private sector which will be able to build multiple applications, with innovative and dynamic workflows to serve the needs of the participants.

This open and multi-stakeholder approach of ONDC is envisioned to democratize e-commerce in the country by levelling the playing field. It will provide greater discoverability for the

products and services that would otherwise not feature on the catalogues of large e-commerce platforms and also offer bespoke and custom-built solutions for customers and merchants alike. Sellers will benefit from access to a larger pool of customers and user data, that too with greater autonomy as to the terms of sale and the use of data. At the same time, buyers will have increased access to a range of solutions that are not available on traditional e-commerce platforms.

ONDC is estimated to increase e-commerce penetration to 40-50 per cent as compared to 10 per cent at present.[16] It aims to onboard 900 million Indian buyers and 1.2 million sellers, with a gross merchandise value of USD 48 billion in the next five years[17]. Platforms like Dunzo[18], PayTM[19] and Microsoft[20] have either agreed to join or are already integrated into the network, while companies such as Amazon[21] and Walmart[22] are in talks to join ONDC.

Bhashini

The primary language to consume Internet content is English, followed by Chinese.[23] Even though Indians speak over 3,000 languages and dialects[24], not a single Indian language features in the top ten languages for Internet content.[25] This means that large sections of our country are excluded from the wide-ranging benefits of the Internet.

For instance, online government services such as registering for welfare schemes, receipt of government subsidies, filing tax returns and payment of GST, are not accessible to those who cannot access these services in their own language. Further, even private digital services, which are critical to socio-economic growth such as digital retail payments, instant credit and online education services, remain inaccessible.

The proposed Digital Personal Data Protection Bill relies on the informed consent of data providers as the foundational basis for a majority of personal data processing. Such consent is likely

to be electronically obtained, which makes the very foundation of this legislation redundant in a situation where language barriers make informed consent impossible.

There is a clear need for a more accessible Internet. Around 53 per cent of the Indians who do not currently use the Internet have said in a survey that they would start using it if content were available in a language they understand.[26]

India has launched the National Language Translation Mission[27] to achieve digital inclusion through accurate translation technologies. As a part of this mission, the Ministry of Electronics and Information Technology has rolled out Bhashini[28] – a digital public infrastructure platform, which uses artificial intelligence and natural language technologies to enable speech-to-speech, text-to-text, text-to-speech, and image recognition translation. Bhashini creates a multi-stakeholder ecosystem based on open-source technology for multilingual content availability at a pan-India scale.

The key elements of this architecture are:

- *Base digital infrastructure*: The underlying technological infrastructure for Bhashini is offered as a digital public good. Designed through open-source software, its primary components are base data repositories, benchmarking systems and data collection tools.
- *Universal language contribution API*: Indian language datasets are stored in an open scalable data repository in a standardized form so they can be used for various tasks, modelling, quality checks and other purposes.
- *Bhasha Daan application*: an open-source platform that enables crowdsourcing of language data through text translation, spoken word contributions or image labelling.

Bhashini's success hinges on its ability to generate vast amounts of training datasets of text, speech and images for translation into multiple languages. The government aims to create a collaborative ecosystem to build these data repositories through open-source datasets. While individuals can contribute through the Bhasha Daan application, other actors in the ecosystem are encouraged to build diverse solutions on top of the existing architecture to contribute to these datasets. Start-ups and other private entities can use the Bhasha Daan source code to build platforms for institutions and publishers to contribute datasets, as well as support applications for translation contributions, translator directories and other innovations to scale the creation of open datasets. Private data collection companies can also contribute through the collection, validation and curation of datasets.

Bhashini leverages technology platforms in many different ways to make the Internet more accessible to those who are not able to use it even though they have access to it. By offering solutions that will translate existing content into a language more understandable to a wider number of people, it offers a scalable solution to the problem of access – one that does not involve generating content afresh in multiple different languages.

Conclusion

India's DPI model offers new solutions for digital transformation, which have global "applicability". By implementing a collaborative and multi-stakeholder approach to tackling complex societal problems, it offers equitable solutions at a scale that harness the benefits of private innovation while at the same time ensuring appropriate regulatory control over the underlying platforms. By striking a balance between public sector accountability, security and democratic access, as well as dynamic and innovative private contributions, the DPI model allows society safe access to the best of both the worlds.

References

1 Anonymous, "Statistics", International Telecommunication Union, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

2 Some countries have reported increased internet traffic of up to 60 per cent shortly after the COVID-19 outbreak, see OECD, "Keeping the Internet up and running in times of crisis", May 2020, www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/; also see Meghan Sullivan, Joel Bellman, Jamie Sawchuk, Joe Mariani, "Accelerated digital government: COVID-19 brings the next generation of digitization to government", Deloitte Insights, March 2021, https://www2.deloitte.com/xe/en/insights/industry/public-sector/government-trends/2021/digital-government-transformation-trends-covid-19.html.

3 At the federal level, post-facto action is primarily taken by the Federal Trade Commission, see Federal Trade Commission, "FTC Report to Congress on Privacy and Security: A Report to Congress", September 2021, https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

4 European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)", https://gdpr-info.eu/.

5 European Commission, "European Data Strategy: Making the EU a Role Model for a Society Empowered by Data," https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

6 National Payments Corporation of India, "UPI Ecosystem Statistics", August 2022, https://www.npci.org.in/what-we-do/upi/upi-ecosystem-statistics.

7 National Payments Corporation of India, "UPI Product Statistics", https://www.npci.org.in/what-we-do/upi/product-statistics.

8 NITI Aayog, "Data Empowerment and Protection Architecture", August 2020, https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf.

9 Reserve Bank of India, "Master Direction - Non-Banking Financial Company: Account Aggregator (Reserve Bank) Direction, 2016", https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.

10 See note no. 8.

11 Sanjeev Athreya Vinod Sankaranarayanan, "Next-gen digital commerce: ONDC changing the game for private enterprises in India", *The Times of India*, 12 June 2022, https://timesofindia.indiatimes.com/blogs/voices/next-gen-digital-commerce-ondc-changing-the-game-for-private-enterprises-in-india/.

12 Open Network for Digital Commerce, "Democratising Digital Commerce in India", January 2022, https://www.medianama.com/wp-content/uploads/2022/03/ONDCStrategyPaper.pdf.

13 Staff Reporter, "India's e-commerce market size to reach $120 billion by 2026: Report", *Economic Times*, 08 July 2022, https://economictimes.indiatimes.com/tech/technology/indias-e-commerce-market-size-to-reach-120-billion-by-2026-report/articleshow/92740817.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

14 Both Amazon and Flipkart have been able to capture more than 80 per cent of the aggressively growing e-commerce industry of India, see "Amazon, Flipkart revenues soar in FY21 as e-commerce sees aggressive sales", *Business Today*, 05 January 2022, https://www.businesstoday.in/latest/story/amazon-flipkart-revenues-soar-in-fy21-as-e-commerce-sees-aggressive-sales-318007-2022-01-05.

15 For more details on the ONDC framework please see note no. 12.

16 As stated by Shireesh Joshi, CBO of ONDC, see Meha Agarwal and Laxitha Mundhra, "[Explainer] How India's Ambitious ONDC Project Can Reinvent Indian Ecommerce", Inc 42, 23 August 2022, https://inc42.com/features/explainer-how-indias-ambitious-ondc-project-can-reinvent-indian-ecommerce/.

17 Arun Padmanabhan, "ONDC: India's bid to break ecommerce monopolies", *Economic Times*, 13 June 2022, https://economictimes.indiatimes.com/tech/technology/ettech-explainer-ondc-indias-bid-to-break-ecommerce-monopolies/articleshow/92181006.cms.

18 Staff Reporter, "Reliance-backed Dunzo's B2B logistics arm joins ONDC", *Economic Times*, 04 August 2022, https://economictimes.indiatimes.com/tech/startups/reliance-backed-dunzos-b2b-logistics-arm-joins-ondc/articleshow/93344425.cms.

19 Blog, "Paytm Mall ONDC", https://paytmmall.com/ondc-ondc-glpid-289844.

20 Abhijit Ahaskar, "Microsoft joins ONDC network, to launch a shopping app in India", *Mint*, 09 August 2022, https://www.livemint.com/companies/news/microsoft-joins-ondc-network-to-launch-a-shopping-app-in-india-11660037404466.html.

21 Vidya S," Amazon India is working closely with govt-backed e-platform ONDC, says company's top exec", *Business Today*, 14 September 2022, https://www.businesstoday.in/technology/story/amazon-india-is-working-closely-with-govt-backed-e-platform-ondc-says-companys-top-exec-347220-2022-09-14.

22 Gunja Sharan, "Flipkart, Reliance Retail & Amazon Likely To Join Open Network for Digital Commerce", Inc42, 12 May 2022, https://inc42.com/buzz/flipkart-reliance-retail-amazon-likely-to-join-open-network-for-digital-commerce/.

23 Anonymous, "Internet World Stats", 31 March 2020, https://www.internetworldstats.com/stats7.htm.

24 Census of India, 2011, "Language" (Paper 1 of 2018).

25 Anonymous, "Internet World Stats", 31 March 2020, https://www.internetworldstats.com/stats7.htm.

26 Arghanshu Bose, "Explained: What is Bhashini and how it can bridge the gap between Indian languages", *The Times of India*, 02 September 2022, http://timesofindia.indiatimes.com/articleshow/93928335.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

27 Anonymous, "National Language Translation Mission", Ministry of Electronics and Information Technology, https://nplt.in/nltm/.

28 Anonymous, "Bhashini", Ministry of Electronics and Information Technology, https://bhashini.gov.in/en.

India Can Drive Global Digital Standards

R. Jesse McWaters and Anand Raghuraman

Global standards are the oxygen of the digital domain

Every digital device on the planet – from the phone in your pocket to the cell tower on the hilltop – relies on hundreds of digital standards that might seem insignificant at first. Yet these digital standards are for these devices much like the oxygen in the air: invisible to the eye but essential to everyday life and functioning.

Digital standards refer to the technical requirements and rules governing the performance of a task or the production of a good. Today, global standards shape almost every facet of the modern Internet and digital economy. Technical Internet standards like TCP/IP and Domain Name System Security Extensions (DNSSEC) enable efficient and safe exchange of data via the Internet. Web standards like HTML and XML allow for common application and web page development. Mobile network standards like 4G and 5G define the requirements for modern mobile communications, while encryption standards such as the SHA-256 hash algorithm secure modern cryptocurrency and blockchain technologies.

As standards grow in importance in a digitized world, so too does the process of standard-setting. Governments worldwide understand that standard-setting is more than a technical

endeavour; it's an opportunity to exercise influence and advance strategic and economic interests. Accordingly, countries like the US and China as well as Germany and Japan are all investing heavily in shaping standards, particularly for emerging technologies such as 5G and AI.

Today, India has an important opportunity to shape global standards for the digital domain. As it celebrates its 75th year of Independence, the country continues to grow as a digital powerhouse and pioneer innovative models of digital governance. It has scaled digital public goods like Aadhaar and UPI payments to hundreds of millions of citizens. More recently, it has contributed to the development of global 5G standards and driven innovation in emerging tech such as AI and quantum computing. How India engages standards bodies and views standard-setting will be critical to the future of global digital economy, and the innovation that emerges within it.

The way forward requires policymakers and technologists – in India and around the globe – to revisit their existing assumptions and approach to standard-setting. Policymakers must recognize the immense value of global standards and harmonization; these are inseparable from the benefits of the modern digital ecosystem, which have fuelled India's economic growth over the past 30 years. At the same time, technologists must understand that digital standards must be inclusive if they are to be accepted and trusted globally. Optimizing for the "West" to the exclusion of the "Rest" is no longer tenable in the 21st century.

Level-setting – understanding the role of standards and their benefits

Standards are not new, nor are global standards. From the size of cannon shells and railway tracks to lightbulb bases and radio receivers, standards have played a critical role in the development and adoption of new technologies – both within countries and

internationally. Nevertheless, the value of technical standards is often misunderstood today, and it is worth revisiting in brief.

Consider as an example the modern shipping container. While global shipping companies had long relied on containers to hold cargo, it took the creation of globally standardized containers to unlock the full power of modern inter-modal logistics.

This required countries and key Standards Development Organisations (SDOs), such as the International Organization for Standardization (ISO), to standardize shipping containers into modular categories with distinct sizes, weights, and ratings. Prior to standardization, containers of different sizes were loaded on and off ships manually as break bulk cargo, where items were counted individually and handled by huge crews of dock workers and longshoremen. This raised the costs of moving goods, reduced the speed of shipment, limited choice in routes and shipping companies, and increased the risk of safety incidents.

Standardization of shipping containers addressed these gaps and enabled a variety of benefits, including:

- **Connectivity:** Standardized shipping containers enabled the development of global multimodal shipping and logistics hubs, which revolutionized the movement of goods across borders.
- **Cost Efficient Competition:** Standardized shipping containers reduced the cost of loading, unloading, and storing bulk cargo, and allowed shipping companies to compete more aggressively on the basis of price, routes, and shipping time.
- **Access:** Standardized shipping containers reduced the cost of adding new logistics hubs and ports to mainline shipping networks, promoting access and availability of world-class shipping and logistics services to countries all over the world.

- **Safety:** Standardized shipping containers enabled safer loading and unloading and reduced the risks of accidents. It also allowed countries to mechanize port operations, which further reduced risks of safety incidents.
- **Trade:** Standardized shipping containers and the global logistics capabilities they created greatly reduced the cost of international trade, particularly of commodities, and also enabled just-in-time manufacturing.

Standard shipping containers are just one important example of the power of standards – as well as the costs that all parties incur in their absence. But they illustrate the suite of benefits that emerge from standards, including those in the digital domain. For example:

- The **TCP/IP** technical Internet standard allows any computer to connect to another over the internet safely and securely. Every major Internet business and web page today rests on this common protocol and the networking it enables, which has powered a revolution in digital commerce and online engagement.
- The **USB** standard allows users to plug in accessories into any laptop equipped with USB ports, irrespective of the model and the maker. This allows for greater efficiency and convenience and eliminates the cost of having to purchase different accessories for different ports.
- **4G and 5G** mobile standards developed by 3GPP enable interoperability between networks, greater competition among device makers, access to high-speed data links, and new forms of digital commerce.
- The **EMV** payments security standard developed by global card networks provide high-quality security to credit and debit card transactions, reducing rates of fraud, building trust, and driving greater adoption of digital payments.

Clearly, promoting interoperability among devices, users, and systems is the primary function of standards, but also the bare minimum. Standards can also help improve the quality of devices and technological processes, promote competition and cost-efficiencies, and ultimately build trust in the broader digital ecosystem.

Standards setting as contested ground

For the first three decades of the Internet's development, digital standards discussions were largely dusty affairs dominated by engineers, technical experts, and bureaucrats based in the US, Europe, or Japan. Discussions on Internet protocols or mobile standards were contentious of course, but disagreements within international SDOs focused largely on technical issues rather than broader geopolitical considerations.

Recent years have changed this equation. Modern standards discussions, while still firmly grounded in technical debates, are increasingly perceived to be an arena for geopolitical competition. Several factors are driving this perception, including:

Intensifying US-China Technological Competition

China's rise as a technological competitor to the US has thrust standard-setting into the spotlight. Over the past 30 years, China has gradually scaled its participation and leadership within prominent SDOs, though it still remains far behind the US. Indeed, a recent Atlantic Council analysis of 39 of the most important SDOs found that the US holds at least 50 per cent of the votes in 11 of these bodies.[1] None of the other countries analysed within the report's data set – China, Germany, Japan, France, Italy, South Korea, United Kingdom, Canada, Others– holds the majority of votes in even a single standards body, which underscores the strength of US incumbency in the global standard-setting ecosystem.

Nonetheless, China is determined to shift this balance, and in 2018, Beijing announced an ambitious effort to reshape its approach to standard-setting, called China Standards 2035.[2] Charting a medium-term vision, China Standards 2035 argued that the country must intensify its leadership in SDOs and control standards in critical emerging technologies, such as 5G, AI, and IoT, in order to secure its technological future. These conclusions have in turn raised American concerns that Chinese participants in SDOs will favour standards that advance Beijing's geopolitical interests even if this means adopting "weaker" technical requirements.

Developing Countries Demand A Seat at The Table

Developing countries, including India, were largely excluded from standard-setting discussions during the first phase of the modern Internet's development. Yet as their capabilities grow, so too does their determination to shape new standards rather than accept Western-centric models in full.

For example, BRICS countries have sought to develop alternate payment systems to bypass the European control of SWIFT. Many developing countries have also looked to the United Nations' International Telecommunications Union to advance ICT standards that help them meet the Sustainable Development Goals. The result is that the standards ecosystem is growing more diverse and differentiated, though there is still considerable room for developing countries to exert influence on the global level.

Emerging Technologies Require New Standards

Emerging technologies such as AI, machine learning, 5G, IoT, blockchain, digital IDs, and quantum computing are still in their infancy globally, and standards for these technologies have yet to be developed fully. Policymakers around the world recognize that these technologies will have significant transformative effects on society and catalyse new forms of economic growth; as such,

even countries that may not be driving cutting-edge innovation see an imperative to contribute to global standards discussions. As noted earlier, this creates significant opportunity for developing countries to engage in global standards setting and ensure diverse interests and use cases are built into new technologies.

India's opportunity to shape global digital standards

India has a critical opportunity to shape global standards in the 21st century, and as the world's largest digital democracy and fifth-largest economy, its voice is sorely needed. In two decades, India has transformed its digital ecosystem through innovative private-public partnerships and strong investments in digital public infrastructure that have scaled to hundreds of millions of its citizens. Digital ID platforms like Aadhaar have emerged as the centrepiece of the "India Stack," while digital payments networks like Unified Payments Interface (UPI) have underpinned a radical evolution in India's e-commerce ecosystem. These domestic capabilities are the pride and joy of a new Digital India, and they should give India confidence to engage in global standards discussions from a position of strength.

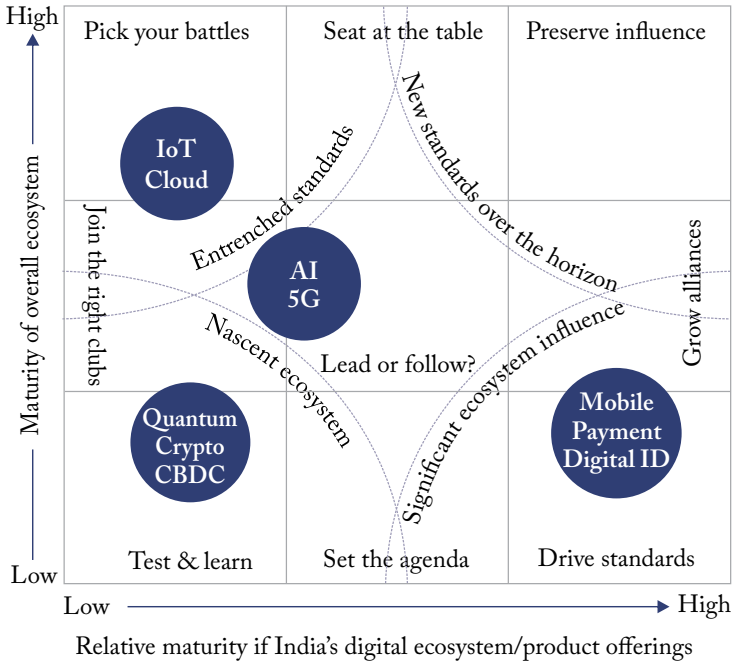
But what should that engagement look like? What technologies should India prioritize and look to shape through global standards activism? How does the adoption of global standards fit into India's goals to build a dynamic local digital ecosystem?

These questions, among others, require India to develop a coherent strategic framework for standard-setting, one that surveys the technology landscape and identifies priority areas of focus. Indeed, digital standards and global technology policy will be at the forefront of India's G20 presidency in 2023. The next year creates a unique window of opportunity to elevate India's technology priorities and ensure that India's interests receive ample weight in global standards discussions.

Developing this framework will require India to carefully assess the relative strength of its domestic technological offerings vis-à-vis the maturity of the overall global digital ecosystem. The higher its relative strength, the more likely India will be in a position to drive standards or set the agenda on that particular technology. Meanwhile, the lower its relative strength vis-à-vis the overall global ecosystem, the harder it will be for India to shape standards– either because those standards are too entrenched or because they are ripe for technological disruption. The latter could sooner or later be overturned by technology or regulatory intervention – making less sense to invest heavily in standard-setting.

Figure 1 below surveys India's technology landscape and provides a rough assessment of the relative strength across several important technologies.

Figure 1: Identifying Priority Areas for Standards Engagement



(Source: R. Jesse McWaters and Anand Raghuraman)

This assessment, while meant to be illustrative, provides a useful model with which Indian policymakers can (1) identify priority areas for standards engagement and (2) calibrate strategies for engagement depending on the type of standards ecosystem.

- **Nascent Standards Ecosystem:** In areas where Indian and global digital ecosystems are both "nascent," such as quantum, cryptocurrencies, and central bank digital currencies, substantive engagement in standard-setting may be premature. Indian policymakers can instead focus on developing a relative technological edge through investments in scientific research, startups, and regulatory sandboxes. At the same time, they can monitor the global landscape for emerging standard-setting efforts and seek to join new SDOs or associated initiatives as they coalesce.

- **Significant Ecosystem Influence:** Wherever India has significant domestic capabilities and global ecosystem influence, such as in mobile payments and digital IDs, policymakers should strive to project India's knowledge, engage with the international community, and seek to promote adoption of global standards that reflect Indian interests. Leveraging platforms like the G20 will be critical in this regard, though India can also seek to assert influence in established technical SDOs, such as ISO or IEEE.

- **Entrenched Standards Ecosystem:** India may not have an advantage in all technologies relative to the global ecosystem, and it will encounter domains with "entrenched standards." Cloud and IoT are perhaps two such domains where global players have already cemented a strong advantage in standard-setting and product offerings. In these areas, India will need to calibrate its strategy and carefully "pick its battles" to ensure Indian priorities receive due consideration. For example, within cloud computing, India can focus on data privacy standards

and anonymization techniques that might align with its interests. In a similar vein, India can continue to push 5G standards to focus on the needs of rural users. New Delhi's successful advocacy on behalf of the 5G standard is a powerful example of this strategy; here, India engaged confidently with 3GPP and was able to influence 5G standards to meet its needs, rather than discarding global standards in favour of an "India-only" solution.

Conclusion

The 21st century will usher in a profound new era of technological change, and countries across the world, including India, will need to come together to set new rules of the road. Harmonized digital standards are an important tool in this regard. The benefits they enable – such as greater connectivity, cost-efficient competition, access, safety, and trade – are vital to ensuring technology remains a force for positive change in the years to come. As a rising power and digital powerhouse, India must continue to engage vigorously in standard-setting bodies. It should help the international community create strong standards that are inclusive by design and look to engage standards bodies from a position of strength and confidence. This is an ambitious project for a new Digital India, but one that can showcase its ability to wield influence and shape the future of the global digital commons.

References

1 Giulia Neaher, David Bray, Julian Mueller-Kaler, and Benjamin Schatz, "Standardizing the future: How can the United States navigate the geopolitics of international technology standards?", Atlantic Council, 14 October 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/standardizing-the-future-how-can-the-united-states-navigate-the-geopolitics-of-international-technology-standards/.

2 Matt Sheehan, Marjory Blumenthal, Michael R. Nelson, "Three Takeaways from China's New Standards Strategy", Carnegie Endowment for International Peace, 28 October 2021, https://carnegieendowment.org/2021/10/28/three-takeaways-from-china-s-new-standards-strategy-pub-85678.

Cultivating An Environment for Responsible and Trusted Data-Driven Innovation

Bojana Bellamy

India is not only a global leader in IT services, it is also a major agricultural economy – more than half of the population derives its livelihood primarily from agriculture.[1] IT and agriculture may appear to be totally unrelated sectors, but they are not. India's Ministry of Agriculture and Farmers Welfare has launched a "Digital Agriculture Mission"[2] to leverage the use of digital technologies in agriculture. Conversely, a foundational principle in traditional agriculture might supply the formula for success in digital innovation across all industry sectors: a good harvest starts with a good soil.

A seed will sprout if given proper light and water, but the plant cannot thrive unless the soil facilitates the development of healthy roots. Similarly, a new idea conceived by an entrepreneurial mind will have difficulty maturing into a successful business venture without a regulatory environment that nurtures and incentivizes its development. It is of utmost importance to cultivate an appropriate environment for business opportunity and growth, especially one that fosters responsible and trusted uses of data and technology. Risk-based rules and organizational accountability are the two essential regulatory pillars of an environment where innovation can thrive.

Accountability nurtures innovation

Accountability can be likened to soil aeration, which permits air, water, and nutrients to reach the roots, encouraging growth. Organizational accountability – such as privacy and data management programmes, with risk assessments and other elements – "aerates" business capabilities by helping operationalize legal and ethical rules, principles and standards, fostering strategic data-based initiatives and enabling sustainable and trusted business practices.

Over time, accountability has gained traction – in data privacy laws (like EU's GDPR[3] and Brazil's LGPD[4]), in certification models (such as the CBPR System[5]), and in regulatory guidance (such as those issued by regulators in Canada,[6] Hong Kong,[7] Singapore,[8] and the UK[9]).

Accountability lays the groundwork for building a pro-innovation, future-proof, and technology-neutral legal regime that is able to anticipate and remain relevant in the face of technological developments, business practices, and societal needs. An accountability-based model ensures enough flexibility to cover as-yet unknown data uses while promoting responsible organizational practices.

In particular, accountability encourages organizations to adopt measures that implement statutory privacy requirements, internal and external policies, as well as standards and ethical principles; it helps them demonstrate the existence and effectiveness of such measures both internally and externally upon request. An accountability-based law or regulation establishes specific elements and expected outcomes, while leaving organizations to decide how to build, implement, and demonstrate their individual accountability frameworks.

Accountability is all about changing behaviours and corporate culture in the long run. The benefits are not limited to achieving legal compliance and avoiding sanctions; accountability also

facilitates public trust and generates new business opportunities. Indeed, it provides a roadmap that organizations can apply to the governance of new technologies (for example, responsible AI) and new situations (for example, COVID-19 pandemic).

The core elements of accountability are highlighted in the Accountability Framework of the Centre for Information Policy Leadership, depicted in the image below:

The CIPL Accountability Framework

The elements of accountability – leadership and oversight; risk assessment; policies and procedures; transparency; training and awareness; monitoring and verification; and response and enforcement – are drawn from similar elements in other regulatory areas, which makes it law-agnostic. These elements are consistent with other areas of corporate law and compliance, including anti-bribery, anti-money laundering, export control and competition- which makes them familiar to corporate leaders. They have been used by organizations, regulators, and courts to determine if an organization has maintained an effective and comprehensive compliance programme in any given regulatory area.

When applied in the data protection context, the accountability framework requires companies to take concrete steps to operationalize all aspects of data governance, privacy law compliance, and the data cycle – from collection and generation, to use, sharing, and deletion. Because a key element of accountability is risk assessment, accountability focuses on, and prioritizes, the mitigation of data processing risks to individuals. This approach enables organizations to implement legal rules and privacy protections more precisely and effectively, based on actual risk and harm to individuals. Thus, accountability is an effective alternative to overly granular and rigid legal requirements that apply across the board regardless of the risks involved.

In essence, an accountability-based privacy law requires companies to achieve the following outcomes, without prescribing how to do it:

- **Establish leadership and oversight for data protection and the responsible use of data,** including governance, reporting, buy-in from all levels of management, and appointing appropriate personnel to oversee the organization's accountability programme and report to management and the board.

- **Assess and mitigate the risks** that data collection and processing may raise to individuals, including weighing the risk of the information use against its benefits. Risk assessment also means conducting periodic reviews of the organization's overall privacy programme and information uses in light of changes in business models, law, technology, and other factors, and adapting the programme to changing levels of risk.

- **Establish internal written policies and procedures** that operationalize legal requirements, create concrete processes and controls to be followed by the organization, and reflect applicable law, regulations, industry standards, as well as the organization's values and goals. These policies

and procedures also include the appropriate use of privacy enhancing and privacy preserving technologies.

- **Provide transparency to all stakeholders internally and externally** about the organization's data privacy programme, procedures and protections, the rights of individuals in relation to their data, and the benefits and/or potential risks of data processing. This also includes communicating with relevant data privacy authorities, business partners, and third parties.

- **Provide training for employees to ensure** awareness of the internal privacy programme, its objectives and requirements, and the implementation of its requirements in line with employees' roles and job responsibilities. This ensures that data privacy is embedded in the culture of the organization so that it becomes a shared responsibility.

- **Monitor and verify the implementation and effectiveness of the programme and internal compliance** with the overall privacy programme, policies, procedures, and controls through regular internal or external audits and redress plans.

- **Implement response and enforcement procedures** to address inquiries, complaints, data breaches, internal non-compliance, and to otherwise enforce compliance.

There is no "one-size-fits-all" formula for implementing and demonstrating accountability, but any given law should allow options for how organizations build, implement, and demonstrate their accountability frameworks. See, for example, recently proposed bills in the United States[10] and Canada,[11] both of which seek to address privacy concerns while promoting innovation in the digital economy. They are not identical by any means but they both include provisions that address the core accountability principles.

Incentivizing a bountiful harvest

Just as good soil facilitates a good harvest, organizational accountability is the "good soil" that facilitates responsible data-driven innovation. It creates consumer trust and enhances an organization's brand and reputation, which is essential for any business, including public sector bodies. Responsible data practices also generate confidence and trust with regulators and enforcement authorities. Furthermore, it enables organizations to engage in broader beneficial uses of data by minimizing risks and demonstrating compliance with applicable laws and regulations. These are all prerequisites for organizational success in the long term.

Given that accountability provides many concrete benefits to all stakeholders – organizations, privacy enforcement authorities, and individuals – companies are motivated to build, implement, and demonstrate good accountability practices.

However, given the critical importance to the digital economy, lawmakers and privacy enforcement authorities should provide specific additional incentives that encourage organizations to adopt accountability measures by rewarding those who have made the investment.

Such incentives could include the recognition of demonstrated accountability (or participation in a formal accountability scheme such as the CBPR) as a mitigating factor in the enforcement context or in the setting of fines, or as evidence of due diligence when selecting third party processors or vendors to whom it is safe to transfer personal information.

Arguably, an even more impactful incentive would permit organizations that have adopted accountability measures to pursue a broad range of new, beneficial uses of personal data. Such uses could be tested in the context of a "regulatory sandbox" specially designed for this purpose. A regulatory sandbox allows qualifying

(here, accountable) businesses to test innovative products, services, business models, and delivery mechanisms in the real market, with real consumers. In the data protection context, this could include testing new data processing activities, data collection methods, or the offering of new information services with appropriate regulatory safeguards and oversight.

Of course, when providing such incentives, privacy enforcement authorities must safeguard against any weakening of their legitimate data protection enforcement obligations (or any appearance of such weakening). Enforcement authorities are functionally independent bodies, and while they have an important role to play in supporting organizations on the road to accountability, there is a fine line between assistance and leniency. The incentives are intended to encourage the uptake of accountability rather than to downplay an enforcement authority's prerogative to take appropriate action where necessary. Thus, for example, using demonstrated accountability as a mitigating factor in an enforcement context or as evidence of due diligence in a contracting context should occur within clearly articulated guidelines.

Moreover, using demonstrated accountability as a basis for facilitating broader uses of data, such as in a regulatory sandbox setting, should be clearly defined and subject to appropriate oversight. And, when enforcement authorities showcase accountability "best practices" as an incentive for more organizations to implement such practices, they must do so in a way that does not compromise the authority's subsequent ability to enforce against organizations that purport to adhere to best practices but fail to do so. In short, any proactive incentivizing of accountability, through whatever mechanism, must keep in mind one of the ultimate goals of accountability – enabling trust in the digital economy and society.

Propagating data ethics

In the ever-evolving landscape of data protection regulation, there is a growing interest in the emerging field of data ethics, which seeks to clarify right and wrong purposes or means of processing personal data. It has a strong relation to traditional data protection principles, including fairness, transparency, and proportionality.

Significantly, data ethics is firmly embedded in organizational accountability. Several of the accountability elements discussed above would naturally include ethical considerations in the decision-making process. For instance, when considering fair processing requirements, organizations need to weigh ethical issues so as not to adversely impact individuals. Similarly, any risk assessment should take into consideration the risk of harm flowing from unethical data uses.

Already today, organizations use their codes of business ethics to inform their data processing decisions. Many build their privacy and data management programmes on their ethical values and principles. Hence, ethical behaviours and ethical decision-making will not be alien to any organization that has already implemented an accountability framework. In that way, data ethics is not a separate concept from properly implemented accountability. Accountable organizations are already well equipped to consider data ethics and responsible data uses in the development of advanced technologies, such as AI, neurotechnology, and Web3.

Conclusion

Any government that seeks to encourage digital innovation across sectors and industries should consider the broad-scale adoption of organizational accountability, which will help create a fertile environment for business development and growth. Even in jurisdictions (like the US and India) where comprehensive data

protection laws have not yet been adopted, government leaders can still develop clear incentives for the implementation of accountability measures. Such incentives will help organizations justify the resources and efforts necessary to maximize their investment in the digital economy. Indeed, accountability is essential for creating consumer trust, which is key to a region's digital future.

References

1 Agriculture is the primary source of livelihood for about 58 per cent of India's population. See India Brand Equity Foundation, "Agriculture in India: Information about Indian Agriculture & its Importance", https://www.ibef.org/industry/agriculture-india.

2 Anonymous, "Digital Agriculture Mission", Press Information Bureau, 05 April 2022, https://pib.gov.in/PressReleasePage.aspx?PRID=1813681.

3 European Union's General Data Protection Regulation (GDPR), 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

4 Brazil's *Lei Geral de Proteção de Dados* (LGPD), 2018, http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

5 Asia-Pacific Economic Cooperation, "APEC's Cross-Border Privacy Rules (CBPR) System", https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system.

6 Office of the Privacy Commissioner of Canada, "Getting Accountability Right with a Privacy Management Program", April 2012, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/.

7 Office of the Privacy Commissioner for Personal Data (Hong Kong), "Ethical Accountability Framework for Hong Kong, China", October 2018, https://www.pcpd.org.hk/misc/files/Ethical_Accountability_Framework.pdf.

8 Personal Data Protection Commission Singapore, "Guide to Accountability under the Personal Data Protection Act", September 2021, https://www.pdpc.gov.sg/help-and-resources/2019/07/guide-to-accountability-under-the-personal-data-protection-act.

9 Information Commissioner's Office, "Accountability Framework", https://ico.org.uk/for-organisations/accountability-framework/.

10 United States Congress, "American Data Protection and Privacy Act (ADPPA)" (introduced in the House of Representatives as H.R. 8152 on 21 June 2022). It is the first bicameral, bipartisan proposal for a comprehensive federal privacy law in the United States. See "American Data Protection and Privacy Act", https://www.congress.gov/bill/117th-congress/house-bill/8152.

11 Canada's Consumer Privacy Protection Act (CCPPA), the first of three statutes in the draft "Digital Charter Implementation Act, 2022," introduced in the House of Commons as Bill C-37 on 16 June 2022. See "Consumer Privacy Protection Act", https://www.parl.ca/LegisInfo/en/bill/44-1/c-27.

The Trail to Net Zero in India

Arundhati Bhattacharya

Climate change is one of the most pressing issues humanity has ever faced. The cost of climate change weighs heaviest on the world's most vulnerable communities, amplifying global inequality. In the last few years, we've learned that climate crisis is one of the most unifying challenges of our time, as extreme weather events have indiscriminately affected the world. We've also learned that the climate crisis is an intersectional issue that exacerbates problems of poverty, affects human rights, and limits our collective progress towards all 17 of the Sustainable Development Goals (SDGs). This makes the crisis a key strategic issue to be immediately addressed by countries, businesses, civil society and individuals.

It will require collaboration, regulatory changes, and technological advances to meet this urgent challenge of climate change and the opportunities that come when we succeed – equality, improved health, economic growth, job creation and a more sustainable world for all.

Ostensibly, the largest contributor to climate change globally has been greenhouse gas emissions and greenhouse gas emissions comes mainly from burning fossil fuels for electricity, heat, and transportation. As the world has raced on its path to development, fossil fuels have literally been the fuel for creating the modern world. While this rapid pace of development has lifted millions

out of poverty and has helped countries achieve better indicators of living, the indiscriminate use of fossil fuels – and therefore, continued emission of greenhouse gases – threatens to push the elusive goal farther away for many countries.

The story in India is no different. In India, the exponential rise in population has increased the pressure on its natural resources. The migration from rural to urban centres has also created stress on urban infrastructure. For a growing economy like India, one of the main sustainability challenges is its high dependency on fossil fuels and associated emissions. Despite all the efforts taken by India, emissions are expected to rise further as a growing population and economic growth fuels the demand for energy.

The rise in carbon emissions is accompanied by a rise in temperature. According to the Intergovernmental Panel on Climate Change (IPCC), at the present rate, global temperatures would reach 1.5 degrees celsius above pre-industrial levels by 2040.[1] This rise in temperature, though gradual, is putting India's most vulnerable population at risk of severe disruption. The IPCC report estimates that by the middle of the century, around 35 million people in India could face annual flooding.[2] Rising sea levels will also impact infrastructure, natural ecosystems, and livelihoods, especially in coastal cities like Mumbai and Chennai.

To combat the effects of climate change, India has been assiduously working on different sustainability initiatives to achieve the SDGs. India has invested significant resources in sustainability initiatives such as river rejuvenation, resource efficiency, air pollution, and clean energy. But given the diversity and scale of India, the way forward for meaningful progress is through extensive collaboration across industries, NGOs, communities, and individuals. All of this is supported by radical transformation, exponential thinking and development and application of new and emerging technologies.

India has achieved some success through its efforts. In the Climate Change Performance Index (CCPI) 2022, it held 10th

position and was rated high in the Greenhouse Gas (GHG) emissions, energy use, and climate policy categories, and medium in renewable energy.[3] As part of the Paris Agreement, India announced its Nationally Determined Contribution (NDC) targets.[4] It has made substantial progress on two of the three targets. Under the first target of lowering the emissions intensity of its GDP by 33-35 per cent, India achieved a 21 per cent reduction. On the second target of increasing fossil-free electricity generation to 40 per cent by 2030, India achieved 38 per cent of non-fossil fuel capacity, making India the only country among G20 nations to meet its NDC targets.[5] The third target of achieving 2.5-3 billion tonnes of carbon sink by 2030 through afforestation efforts is in progress.

At COP26 in 2021, India pledged to cut its net carbon emissions to zero by 2070, along with four more immediate targets for 2030:

- Increase the country's non-fossil energy capacity to 500 GW.
- Meet 50 per cent of its energy requirements from renewable sources.
- Reduce the carbon emissions intensity of the economy by more than 45 per cent.
- Lower total projected carbon emissions by 1 billion tonnes.

The Indian government's policy actions and investments will significantly impact how successfully it can combat climate change at home and inspire action in other countries through its leadership globally. Domestically, there is growing political consensus on low-carbon focused development that prioritizes poverty reduction and sustainable development.[6] India announced its **National Action Plan on Climate Change (NAPCC)** in 2008 as a roadmap to address climate change. NAPCC has

eight missions including enhanced energy efficiency, sustainable habitats, a "green" India, sustainable agriculture, and strategic knowledge for climate change.

On the international front, India has begun taking an active role in climate negotiations and forged progressive partnerships to address various aspects of climate change adaptation, mitigation, and resilience, including with the US and EU on clean energy, and platforms such as the Coalition for Disaster Resilient Infrastructure[7] and the International Solar Alliance (ISA)[8] with France. In May 2022, India's top CEOs came together under the aegis of the World Economic Forum to supercharge India's climate action and decarbonization efforts and bolster the government's efforts to achieve net zero by 2070.[9]

Impact of climate change on economic growth

Climate change impacts economic growth. Estimates suggest that by the year 2100:

- India's GDP will decline by 2.6 per cent if global temperature increase is held below 2°C, but this rises to 13.4 per cent in a 4°C scenario based on projections of temperature and precipitation changes, and the effect on labour productivity in different sectors.[10]
- There will be around 10 per cent decline in India's GDP at 3°C of global warming due to declining agricultural productivity, sea-level rise and increased health expenditure.[11]

Estimates also suggest the national poverty rates could rise by 3.5 per cent by 2040 compared to a zero-warming scenario, equating to approximately 50 million more poor people.[12]

On the flip side, an effort to actively lead decarbonization efforts and transition to a green economy could generate significant economic gains for India.[13] India could gain approximately USD

11 trillion by 2070, by supplying the products and services the world will need to address climate change, such as green hydrogen and negative emission technologies, and accelerating investments in technologies that reduce carbon emissions.

Investments in digital technologies to reduce emissions

Climate action will require not just moving to cleaner and greener forms of energy, but also focusing on decarbonization. In this effort, there are several digital technologies that can play a critical role in helping achieve huge reductions in carbon emissions. Analysis by the World Economic Forum[14], in association with Accenture, categorized high-impact digital technologies into four clusters:

1. *Foundation technologies:* measurement and reporting, big data analytics
2. *Enabling technologies:* cloud, 5G, blockchain, augmented/ virtual reality
3. *Decision-making technologies:* digital twin, artificial intelligence/machine learning
4. *Sensing and control technologies:* IoT, drones and imaging, automation, and robotics

These new and emerging technologies are not only deepening our understanding of the problems that affect us, but also in overcoming them. Governments and businesses need to measure, report, calculate and track their emissions in order to reduce them.

When deployed and scaled across industries, these technologies have huge potential. The WEF report found that even in high emissions industries such as energy (34 per cent of total 2020 emissions), materials (21 per cent), and mobility (19 per cent), the adoption of digital technologies could result in 20 per cent of reductions needed by 2050 to achieve targets set by the International Energy Agency.[15]

As a first step, companies embarking on their sustainability transformation journeys need to ask themselves the following questions about their climate strategy:

1. What do we do? And why? [products and services, mission]
2. How do we do it? [operating mode and value chain]
3. Whom do we influence? [employees, customers, society]

The answers to these questions will determine the digital technology best suited to help them on their sustainability journey. Take cloud adoption, for example. Cloud computing offers numerous long-term economic gains, including greater flexibility, cost efficiency, speed, and business continuity, but an often-overlooked advantage is its impact on the environment. Adoption of the cloud also results in reduction of energy consumption, waste, and carbon emissions.[17]

A recent APAC study by S&P Global Market Intelligence has shown significant energy savings of 80 per cent from moving business applications and IT workloads from on-premises enterprise and public sector data centres to the cloud.[16] With cumulative investment in data centre capacity in India expected to reach USD 28 billion by 2025, there will be a substantial reduction in energy consumption and carbon emissions as IT workloads are moved to the cloud.

There are several ways in which a move to the cloud reduces costs and saves energy:

a. As workloads move to the cloud, data centres become akin to utilities and inefficiencies across various companies can be eliminated through a higher server and more optimal utilization rate.

b. Data centres could also deploy highly energy-efficient and custom-made servers, and the use of advanced power distribution systems and cooling technology by cloud

data centres. Making such investments at an individual company level – even if they are significant users of technology – becomes impossible.

Since the cloud service provider can serve several customers using the same infrastructure, investing in high-end equipment that delivers the same, or better, performance at a much lower cost to the environment becomes a better option economically. The benefits of reduction in carbon emissions can be made available to everyone – making it more likely that companies would invest in and achieve their net zero strategies. Within data centres, emissions can be further reduced by increasing the efficiency of software code (which helps achieve more with each kilowatt hour of energy used), operating in co-location facilities, and using high-efficiency, water-free, zero-waste infrastructure to reduce energy use.

Based on these estimates, research from Access Partnership projects[18] show:

- Cost savings of **USD 2.2 billion** in 2022. These total to approximately **USD 24 billion** between 2022 and 2030 when data centre capacity expands, and more organizations leverage the hyperscale cloud facilities.
- CO_2 emissions reduction of **2.2 million metric tonnes (Mt)** in 2022 due to migration to cloud alone, which rises to **2.8 million Mt** if cloud operators source 100 per cent renewable power for their operations.
- The longer-term impact of such a move is even more significant. Total reduction in CO_2 emissions will amount to approximately 48 million Mt between 2022 and 2030 due to migration to cloud, but this increases to **60 million Mt** if the cloud operators source 100 per cent of renewable energy for their newly established cloud infrastructure.

Business sentiment in India on sustainability

Increasingly, businesses are placing sustainability at the centre of their plans, in part due to external pressures from regulators, but even more so to achieve efficient business operations.

A study commissioned in India by the cloud computing company Salesforce found that managers across small, medium, and large businesses are actively focused on achieving their net-zero goals as a key business imperative.[19] A majority of surveyed businesses (84 per cent) noted the importance of technology in helping to achieve a net zero target, with almost six in ten (57 per cent) saying the role of technology will be very important. This underlines the importance of technologies such as cloud computing in supporting businesses in their net-zero goals. Key findings of the study include:

- **Stronger action on climate change:** The Indian government's climate action has resonated well in the business community, but eight in ten (83 per cent) managers support a more ambitious net-zero target of 2050, and 79 per cent of them support the provision of subsidies and incentives to businesses for the development of renewable energy technology.
- **Emphasis on sustainability commitments:** Almost two thirds (63 per cent) of the businesses surveyed said that if a supplying business had a net zero target, then it would make them more likely to purchase their products or services. This shows that businesses having sustainability goals and net zero targets is an important factor for doing business now, and more so in the future.
- **Future growth opportunities:** Businesses are seeing the transition to net-zero as a growth opportunity, resulting in higher jobs and economic activity – they are three times as likely to think that achieving a net zero economy by 2050

in India will result in more jobs than less jobs (58 per cent compared to 18 per cent).

Call to action for the Indian government

This section provides key recommendations to advance India's efforts on addressing climate change:

- **Develop cutting-edge climate technology:** India's climate efforts should bring a renewed focus on developing and nurturing technological innovations that reduce emissions and increase energy efficiency. This can be achieved by addressing barriers to their deployment, providing funding for new ideas to start-ups and "ecopreneurs". While it has accelerated investments in renewable energy, India must also prioritize emerging carbon-removal technologies and more efficient, "smart" technologies and processes that optimize energy use for households and businesses.

India has invested significant resources in developing digital public platforms for identity, payments, and health, and this has cemented its global leadership in innovation. Developing a similar stack for sustainability would not only foster a new sector of growth, but also boost India's reputation globally as the storehouse of innovative technologies.

- **Increase investment in cloud:** Cloud computing offers an economic and environmental opportunity. It reduces energy consumption, waste, and carbon emissions through server virtualization and shifting of workloads across the globe and less end-of-life IT wastage. The study mentioned above has shown India's migration to cloud is expected to reduce CO_2 emissions by at least 48 million metric tonnes (Mt) between 2022-2030.[20] Emissions will reduce even further if cloud operators begin sourcing 100 per cent renewable power for their operations.

Policy initiatives to encourage this shift to the cloud should be implemented to take greatest advantage of cloud's potential to alleviate the effects of climate change. These may include policies on the use of sustainable sources of energy and financial incentives for the use of energy-efficient technologies.

- **Address sustainability skills gap:** The workforce needs to pivot to capabilities, skill sets, and tools necessary for a net zero economy transition.

  New hiring should ensure climate-related expertise and upskilling initiatives should prepare employees to recognize the imperative for climate action and make decisions in line with the climate agenda of their organizations.

  With a growing emphasis on publicly disclosing climate risks and opportunities, employees will also need to acquire capabilities in leveraging big data and conducting modelling exercises of physical and transition-related risks of climate change, and new roles will be established such as carbon accountants, researchers, and energy consultants.

- **Environment AI:** There are many potential uses of harnessing AI to achieve sustainability outcomes. It has already been used in India for detecting arsenic pollution in drinking water, helping monitor air pollution hotspots, and real-time flood forecasting. Other potential uses include monitoring deforestation, enabling smarter decision-making for decarbonizing industries, and efficiently allocating renewable energy. AI is also well-suited to helping project climate-related hazards, through long-term projections of sea-level rise or upgrading early warning systems for hurricanes, droughts, and floods.[21]

- **Adopt a shared digital platform to track emissions:** The government and organizations should adopt a shared digital platform to track emissions and forecast emission patterns. Having a shared digital platform will ensure better decision making and a single source of truth when measuring and tracking emissions within their own organization and potentially their supply chain.

References

1 Intergovernmental Panel of Climate Change (2022), "FAQ_Chapter 1: Global Warming of 1° celsius," https://www.ipcc.ch/sr15/faq/faq-chapter-1/#:~:text=At%20the%20present%20rate%2C%20global,emissions%20reaching%20zero%20by%202055.

2 Intergovernmental Panel of Climate Change (2022), "Climate Change 2022: Impacts, Adaptation and Vulnerability," https://www.ipcc.ch/report/sixth-assessment-report-working-group-ii/.

3 Jan Burck, Thea Uhlich, Christoph Bals, Niklas Höhne, Leonardo Nascimento, Jamie Wong, Ana Tamblyn, Jonas Reuther (2022), "Climate Change Performance Index, Results," https://ccpi.org/wp-content/uploads/CCPI-2022-Results_neu.pdf.

4 Press Information Bureau (2015), "India's Intended Nationally Determined Contribution is Balanced and Comprehensive: Environment Minister," https://pib.gov.in/newsite/printrelease.aspx?relid=128403.

5 Jayashree Nandi (2021), "India only G20 nation to meet climate goals", *Hindustan Times,* https://www.hindustantimes.com/environ-ment/ india-only-g20-nation-to-meet-climate-goals-101629061426571.html.

6 ScienceDirect (2016), "Approaches to low carbon development in China and India", https://doi.org/10.1016/j. accre.2016.11.001.

7 United Nations (2021), "The Coalition for Disaster Resilient Infrastructure (CDRI)", https://sdgs.un.org/partnerships/coalition-disaster-resilient-infrastructure-cdri.

8 International Solar Alliance (2021), "About," https://isolaralliance.org/.

9 World Economic Forum (2022), "Indian CEOs' Alliance to Supercharge Race to Net Zero," https://www.weforum.org/press/2022/05/indian-ceos-alliance-to-supercharge-race-to-net-zero.

10 Kahn M., Mohaddes K., Ng R., Hashem Pesaran M., Raissi M. and Yang J. (2019), "Long-Term Macroeconomic Effects of Climate Change: A Cross-Country Analysis," IMF Working Paper, https://www.imf.org/en/Publications/WP/Issues/2019/10/11/Long-Term-Macroeconomic-Effects-of-Climate-Change-A-Cross-Country-Analysis-48691.

11 Tom Kompas, Van Ha Pham, Tuong Nhu Che (2018), "The Effects of Climate Change on GDP by Country and the Global Economic Gains From Complying With the Paris Climate Accord, Earth's Future 2018," https://agupubs.onlinelibrary.wiley.com/doi/ full/10.1029/2018EF000922.

12 Emmanuel Skoufias, Mariano Rabassa, Sergio Olivieri Skoufias (2011) "The Poverty Impacts of Climate Change", *Economic Premise*, No. 51. World Bank, https:// openknowledge.worldbank.org/bitstream/handle/10986/10102/600730BRI0EP511v-40BOX358307B001PUBLIC1. pdf?sequence=1&isAllowed=y.

13 Deloitte (2021), "India's turning point How climate action can drive our economic future", https://www2.deloitte.com/ content/dam/Deloitte/in/Documents/about-deloitte/in-india-turning-point-noexp.pdf.

14 World Economic Forum (2022), "Digital solutions can reduce global emissions by up to 20%", Here's how, https://www.weforum.org/agenda/2022/05/how-digital-solutions-can-reduce-global-emissions.

15 Ibid.

16 Amazon Web Services (2021), "The Carbon Reduction Opportunity of Moving to the Cloud for APAC", https://d1.awsstatic.com/institute/The%20carbon%20opportunity%20of%20moving%20to%20the%20cloud%20for%20APAC.pdf.

17 NASSCOM (2021), "India: The Next Data Centre Hub", https://nasscom.in/knowledge-center/publications/india-%E2%80%93-next-datacenter-hub.

18 Salesforce (2022), "Trail to Net Zero for India", https://www.salesforce.com/content/dam/web/en_in/www/documents/pdf/net_zero_report_india.pdf.

19 Ibid.

20 Ibid.

21 AI for the Plant Alliance (2022), "How AI Can Be a Powerful Tool in the Fight Against Climate Change", https://www.zawya.com/en/press-release/research-and-studies/87-of-climate-and-ai-leaders-believe-that-ai-is-critical-in-the-fight-against-climate-change-alltfipu.

Part 2

Securing Digital ++

Reimagining Security for Tomorrow's Supply Chains

Daisy Chittilapilly

March 2020 shall go down in history as a crucial turning point for the world. Over two and a half years later, individuals, companies, and communities look quite different from what they used to. We are finding better ways to live, work, do business, and connect with each other – a true testament to our resilience and agility in the face of the most daunting of crises. At the heart of this, and the fuel powering these transitions, is technology, allowing us to come back stronger and better prepared than ever before.

That said, there is no denying that the crisis has set us back in several aspects, giving rise to unprecedented challenges with which we continue to contend with. The most evident amongst these is the breakdown of global supply chains. Over the past year, supply-chain leaders have taken conscious action to adapt quickly and effectively to boost inventories in response to frenetic demand cycles and ramp up their digital and risk-management capacities. However, despite notable progress, delays, component shortages, etc., continue to wreak havoc across supply chains, highlighting vulnerabilities that must be addressed on priority basis.

The supply chain ecosystem is at risk

Leaders are not oblivious to these risks. However, while they recognize the urgency for reinvention, some are still struggling to funnel the time, resources, and talent needed for it. Considering that many companies require a complete restructuring of existing supply chains and a rejig of strategy for setting up new ones, it is not surprising that leaders are making do with what they have while focusing on fortifying other business functions.

This is not a new way of thinking. For years, just-in-time, lean supply chains have been the preferred choice, reducing the amount of inventory through greater efficiency in production, distribution, and last-mile delivery, thus allowing more funds to be invested in other areas. But this works only when the companies' Tier I and Tier II supplier are near-impervious to external elements, which is not true in most cases. So, a change in the mindset towards supply chain management, where leaders seek full visibility of every layer and closely follow industry, market, geopolitical, and environmental trends for imminent slowdowns is essential. This means collecting massive volumes of data around potential disruptions and analysing the ramifications they could have on the business. Again, with visibility into their supply chains being limited, anticipating and staying ahead of problems is tricky.

At the same time, while many are embracing digital technology to bolster their supply chains, a large number of enterprises still stand by manual or traditional methods, relying on instinct and experience rather than data and precision. This stems largely from the belief that an IT overhaul is too expensive and time-consuming. And for the ones that do take the leap, IT implementations often fail. According to McKinsey, 60 per cent of the time it's because they aren't completed on time, are over budget, or don't deliver the expected outcomes.[1] This indicates that processes lack the necessary capabilities, or the switch was poorly managed.

So, leaders have quite the task ahead of them to identify the biggest gaps in their supply chains, embrace technology solutions that enable them to make smarter decisions, make total operations more efficient, and solve problems before they affect the entire supply chain.

Leaders are stepping up to the challenge

In order to build resilience, leaders are continuing to look at localization and nearshoring to bolster their supply chains. But this involves large-scale pivots in building capacity and tightening last-mile delivery – something for which they may not have the bandwidth presently. Additionally, many are struggling to establish an adequate supplier ecosystem that can enable localization. Despite these roadblocks, a McKinsey survey recently found that almost 90 per cent of companies expect to engage in some degree of regionalization over the next three years.[2]

As this happens – as supply networks go wider and deeper, they're also becoming more complex. Visibility remains a key issue. According to a McKinsey study, only 2 per cent of companies have visibility into their supply base beyond the second tier.[3] To combat this, many leaders are investing actively in digital technologies like AI/ML, robotics, data analytics, and other software tools to bring more intelligence and efficiency into their supply chain management practices. According to an industry report, over 50 per cent of supply chain organizations will use machine learning (ML) to augment decision-making capability by 2026.[4] Similarly, even traditional industries like construction, defence, etc., are planning to invest heavily in advanced analytics going forward.

The flipside is that as supply chains get more digitized and generate vast volumes of data, they're also far more likely to fall prey to cyberattacks. Overall, India has seen an increase of over 500 per cent in cyberattacks since the pandemic.[5] No industry is exempt and attacks on the supply chain are increasing on a daily basis. The

SolarWinds attack on the United States Federal Government and the Armor Piercer campaign that targeted government employees and military personnel in India – are just a few examples of how brazen bad actors have come to be. For businesses, these lapses can run them to the ground. A Cisco study found that cyber intrusions cost almost 75 per cent of SMBs up to ₹7 crores in business losses in 2020-21.[6]

More worrying is the fact that it's only expected to get worse– Gartner predicts that by 2025, 45 per cent of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.[7] Going forward, the most crucial element for leaders in ensuring the longevity and success of their reimagined, digitally enhanced supply chains is near-infallible security. How do you do it in an easy-to-manage-and-deploy way that does not hinder day-to-day business?

Securing the supply chains of tomorrow

The first step is to evaluate the current security posture and identify the biggest gaps. A Cisco study found that over one-thirds of cybersecurity technologies used by Indian companies are outdated.[8] Therefore, it is more important than ever for businesses to refresh their infrastructure and continually reassess risks. This is where a cyber mesh infrastructure can profoundly change the game. A flexible and agile security solution that protects identities beyond the traditional security perimeter to provide a comprehensive view of the organization is key for enabling secure supply chains.

Next, a Zero Trust approach based on the belief of "never trust, always check" is no longer just a good-to-have. It is core to a robust security strategy. It assumes that every action and every entity is potentially malicious, and thus performs security round-the-clock in near real-time. The rewards are already apparent, and Gartner predicts that by 2025, 60 per cent of organizations will embrace

zero trust as a starting point for security.[9] While the principles of Zero Trust may not be new, the need to implement them from the ground up has never been greater.

At the same time, it's vital to mobilize your entire ecosystem to plug all the gaps. Every business depends on suppliers such as service providers, contractors, and systems integrators to provide input. But suppliers can also introduce risk. Cyber supply chain risk management (C-SCRM) aims to understand and mitigate supplier risk. Suppliers are outside entities that offer varying levels of transparency into their business policies and practices. Without visibility and industry standards, it's difficult to assess the level of risk that suppliers may introduce into your business. Here, a powerful C-SCRM tactic is instrumental in ensuring the confidentiality, integrity, and availability of the supply chain, its participants, and the data that travels across it.

Of course, we know that even the best technology can fail without the right people to put it to the right use. Security for the supply chain is a particularly niche discipline, and the demand for cybersecurity professionals far outstrips supply. A survey by the global IT association, ISACA found that in 2022, 60 per cent of Indian organizations had unfilled cybersecurity positions, and 42 per cent of cybersecurity teams are understaffed.[10] So, investments in talent must be on the top of the minds for firms as they strive to improve their resilience and growth.

All of this is easier said than done. At Cisco, we've been working with several customers to bolster their supply chains, as well as help them switch to hybrid work and business models. We've seen first-hand how challenging it can be, even for digital natives. The power of partnerships cannot be overstated in a feat of this scope. It is critical for senior leaders to seek out and join hands with the right partners who can streamline and simplify this undertaking.

Our next calling

India is at a great inflection point. How we secure our supply chains today is directly consequential to cementing India's place at the top of the global economy tomorrow. To make this happen, we need the government, industry bodies like the Data Security Council of India and NASSCOM, tech companies, as well as entrepreneurs, small businesses, researchers, etc., to come together and work for a brighter, more secure future for India.

References

1 Marilú Destino, Julian Fischer, Daniel Müllerklein, and Vera Trautwein, "To improve your supply chain, modernize your supply-chain IT", *McKinsey & Company*, 09 February 2022, https://www.mckinsey.com/capabilities/operations/our-insights/to-improve-your-supply-chain-modernize-your-supply-chain-it.

2 Knut Alicke, Ed Barriball, and Vera Trautwein, "How COVID-19 is reshaping supply chains", *McKinsey & Company*, 23 November 2021, https://www.mckinsey.com/capabilities/operations/our-insights/how-covid-19-is-reshaping-supply-chains.

3 Ibid.

4 Sarah Hippold, "The Rise of the Ecosystem — and 4 More Supply Chain Predictions", *Gartner*, 12 January 2022, https://www.gartner.com/en/articles/the-rise-of-the-ecosystem-and-4-more-supply-chain-predictions.

5 Staff Reporter, "Cybercrime went up by 500% during pandemic: Chief of Defence Staff", *The Hindu,* 12 November 2021, https://www.thehindu.com/news/national/cybercrime-went-up-by-500-per-cent-during-pandemic-chief-of-defence-staff/article37457504.ece.

6 Staff Reporter, "Indian SMBs lost upto ₹7 crore in cyber attacks in last 12 months: Cisco", *The Hindu,* 27 September 2021, https://www.thehindu.com/business/Industry/indian-smbs-lost-upto-7-crore-in-cyber-attacks-in-last-12-months-cisco/article36691991.ece?homepage=true.

7 Susan Moore, "7 Top Trends in Cybersecurity for 2022", *Gartner*, 13 April 2022, https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022.

8 Staff Reporter, "Over a third of Indian companies use outdated cybersecurity technologies: Report", *The Economic Times,* 08 December 2021, https://economictimes.indiatimes.com/tech/technology/over-a-third-of-indian-companies-use-outdated-cybersecurity-technologies-report/articleshow/88165411.cms?from=mdr.

9 Jay Fitzgerald, "Gartner: 8 Ways Cybersecurity Will Change Companies", *The Channel Co.*, 25 June 2022, https://www.crn.com/news/security/gartner-8-ways-cybersecurity-will-change-companies.

10 Staff Reporter, "Increase in Cybersecurity Skills Gap in India, 60% Companies Say Positions Not Filled", *News18*, 30 March 2022, https://www.news18.com/news/education-career/increase-in-cybersecurity-skills-gap-in-india-60-companies-say-positions-not-filled-4924964.html.

Hybrid War: Understanding and Responding to The Proliferation of Threats

Tom Burt

In Ukraine, the Middle East, and in other parts of the globe we are increasingly seeing nation-states using cyberweapons to deny, disrupt, degrade, or destroy targeted devices, systems or networks. In some instances, these attacks stand alone. In other cases, they have been deployed as a tactic in long-standing hostilities between nations, or strategically alongside or in support of conventional weapons in a hybrid war. These new developments should worry governments, civil society, industry, and individuals worldwide.

Nation state threats

State actors deploy offensive cyber operations to advance their national interests. Historically, we have seen nation states using cyber weapons engage in espionage or theft of intellectual property. Increasingly, we also see nation states engaging in destructive attacks and as instruments of war. These offensive cyber operations are among the most sophisticated and persistent threats faced by the Internet and technology users worldwide. In response, technology and cybersecurity companies are investing significant resources to discover, understand, and counter these threats.

From the vantage point of Microsoft[1], and as detailed in the 3rd annual Microsoft Digital Defense Report[2], we can see that China, Iran, North Korea, and Russia are the countries of origin for the most commonly observed threat actors targeting digital networks. The threat actors we identify as being associated with a nation state either fall under a government's chain of command, or they support a state's national interests and are coordinated with or supported by a state, or they operate from a given country with operations, which align with a state group or state-aligned group.

Customers and users are increasingly implementing new security protections to defend against sophisticated threats. However, just as defenses evolve, the threats are also evolving. Nation state and state-affiliated threat actors are adapting in response to improved defenses. Advances in automation, cloud infrastructure, and remote access technologies are being used by threat actors to extend their attacks against a wider set of targets. We are also seeing the priorities and risk tolerance of threat groups evolve as their national interests evolve.

For example, we are seeing new approaches and large-scale attacks against corporate supply chains, which provides threat actors with new approaches to exploit unpatched vulnerabilities, to expand techniques to compromise networks, and to hide their operations in the functionality of the popular software which they have compromised.

Threat actors continue to use new tactics to deliver attacks and evade detection by exploiting zero-day vulnerabilities. The number of publicly disclosed zero-day vulnerabilities over the past year is on par with those from the previous year, which was the highest on record. Although many organizations assume they are less likely to be a victim of zero-day attacks if vulnerability management is integral to their network security, exploits are happening at a much faster rate, and once deployed they are discovered and rapidly reused by other threat actors – both nation state and cyber criminals – leaving unpatched systems at risk.

Hybrid war

In 2022, we witnessed the first major hybrid war when Russia combined cyber-attacks and influence operations with its ongoing military operations as it planned, launched, and continued its war in Ukraine. This war exemplifies how cyber-attacks can be used to cause harm through the cyberspace in coordination with kinetic military action.

Even before Russia's invasion, Ukraine was subject to more cyber-attacks each year than any country in the world except the US, mostly emanating from Russia. Progressively, we saw cyber threats moving from commercial customers to the government and the systems of organizations who work closely with the Ukrainian government. We saw these nation state cyber operations using a number of tactics, techniques, and procedures, including:

- Spear phishing with malicious attachments or links.
- Exploitation of IT services supply chains to impact downstream customers.
- Exploitation of public-facing applications to initially gain access to networks.
- Use of administrative accounts and protocols, and native utilities for network discovery and lateral movement.

After the war began in February 2022, initially with a round of cyber-attacks hours before the physical invasion of Ukraine, Microsoft observed actors associated with the Russian military and intelligence launch multiple waves of destructive cyber-attacks, destructive efforts that have continued throughout the war. Targets have included government agencies, energy systems, telecommunication systems, media, the IT sector, finance sector and other critical infrastructure – many of which were targets of both physical and cyber-attacks. The targets of destructive cyber-attacks include more than 50 Ukrainian agencies and enterprises, while espionage-focused intrusions targeted many

others. From the start of conflict through to June 21, 2022, 64 per cent of Russian cyber-threat activity recorded by Microsoft Threat Intelligence Center (MSTIC) was directed against Ukraine-based organizations. Much of the rest were espionage or surveillance actions targeting governments and related organization in the Baltics, the Nordics and other countries supporting Ukraine's defence.

In each operation, threat actors employed many of the tactics, techniques, and procedures observed before the invasion against targets inside and outside of Ukraine. These threat actors intended to destroy data and to impede the work of Ukrainian government agencies in the initial stages of the conflict. They have since sought to derail the transport of military and humanitarian assistance to Ukraine, disrupt public access to critical services and media, and steal information with longer-term economic and intelligence value for the occupying forces.

In addition to destructive cyber-attacks and cyber espionage efforts, threat actors also increasingly conduct cyber-influence operations around the world to support their efforts. State and state-affiliated actors use influence operations to shape opinion, discredit adversaries, incite fear, promote discord, and to distort reality. Falsehoods spread by nation states, both throughout the pandemic and during the conflict in Ukraine, demonstrate how cyber operations and information operations can be blended by threat actors to concurrently advance their goals. Digital technologies and the Internet give foreign influence operations a broader geographic reach, higher volume, more precise targeting, and greater speed and agility.

Russia's cyber-influence operations are focusing on four distinct audiences to support their war efforts:

- They are targeting the Russian population with the goal of sustaining public support for the war effort.
- They are targeting the Ukrainian population with the goal

of undermining confidence in their country's willingness and ability to withstand Russian attacks.

- They are targeting American and European populations with the goal of undermining Western unity and deflecting criticism of war crimes.
- They are targeting populations in nonaligned countries to sustain their support at the United Nations and in other international fora. These efforts are aided by the increasing reliance in many countries on Russian state-controlled media as a primary source for news.

Similar to the pre-positioning of malware and other software code for cyber-attacks, Russian threat actors have been pre-positioning false narratives in the public domain. After the false narrative is staged, they launch broad-based and simultaneous "reporting" from government-managed and influenced news and information sources to amplify their narratives, and they further amplify those narratives with tools designed to exploit social media platforms and users. We estimate that Russian cyber influence operations successfully increased the spread of Russian propaganda after the war began by 216 per cent in Ukraine and 82 per cent in the US. We have seen similar sophisticated efforts to spread false narratives in multiple Western countries about the COVID-19 pandemic.

Unfortunately, as the war continues, these cyber influence operations will likely be used more and more to sustain public support and fend off fatigue. However, many state cyber influence operations run for months without proper detection, analysis, or public reporting. Recognizing the possibility that such operations will increase in frequency and scale, and the significant challenges of countering a sophisticated influence operation, should add urgency to the importance of strengthening defenses against these types of foreign cyber influence attacks.

Cyber resilience and cyber norms

The scale, scope and severity of the harms described so far clearly require whole-of-society solutions. Mitigating the risks and impacts of hybrid conflict will only succeed through better coordination and implementation of cybersecurity norms for peace and security by governments, the private sector and civil society, in order to improve cyber resilience.

Currently, there are many simple ways to improve cyber resilience worldwide:

- Around 80 per cent of security incidents can be traced to just as a few missing security practices that could be addressed through modern approaches, discussed below.
- Over 90 per cent of accounts compromised via password-based attacks were not protected with strong authentication.
- According to a study on critical patch deployment, 78 per cent of devices are still at risk nine months after deployment.
- Twice as many users are employing strong authentication methods today compared to users in 2019, but that still represents just 26 per cent.

Attacks by nation state actors can be technically sophisticated and these actors have the capacity to use a wide variety of tactics. However, many of these actors use relatively low-tech means, including spear phishing emails to deliver sophisticated malware instead of developing costly customized exploits. As such, attacks can often be mitigated by good yet basic cyber hygiene, which is holistic, adaptive, and global in nature so that it can withstand the evolving threats.

Basic cyber hygiene, with endpoint detection and response tools, can help network administrators in mitigating the harms of

these nation state threats in both peacetime and during conflicts. Importantly, all of these basic cyber hygiene tactics can be best achieved at-scale and most effectively across devices and networks when digital transformation happens in the cloud. They include:

- *Protect the identities of users:* Identity protection tools, requiring multifactor authentication, and using least privileged access policies to secure sensitive and privileged accounts and systems will help prevent credential theft and account abuse.

- *Apply updates as soon as possible:* Patches and updates are critical to reducing the possible exploitation of unpatched, public-facing applications, which can breach network security.

- *Use extended detection and response anti-malware and endpoint detection solutions:* Defence-in-depth security solutions empower organizations to identify, detect, and prevent intrusions, particularly when enabling cloud-protections to identify and mitigate known and novel threats across networks at scale.

- *Enable the auditing of key resources and prepare incident response plans:* Incident responders benefit from having access to the information needed to investigate, identify, and mitigate harms when a threat is detected or when a notification of a threat is received.

However, while network administrators have a responsibility to deploy basic cyber hygiene, nation states in particular have a duty to uphold international law and norms in order to protect human rights from reckless state behaviour online. This need is clearly demonstrated in the ongoing conflict in Ukraine but has been self-evident for many years. Five years ago, Microsoft called for a "Digital Geneva Convention" to advance responsibilities and obligations across sectors to defend peace and security online. Cyberspace was already emerging as a distinct and volatile domain

of conflict and competition between states. Attacks in cyberspace were becoming increasingly common even in times of peace.

Today, the need for such a framework is even more evident. The Ukraine conflict underscores that a new frontline exists – a frontline which is fundamentally different from other domains of conflict since it is borderless and largely created, owned and operated by industry.

Since digital technologies and the Internet are increasingly becoming the gateway to the exercise of human rights, we cannot take an open, free and secure global Internet for granted. Civil society, the technology industry, and rights-respecting governments must work together towards an affirmative vision for a safe and secure cyberspace. Although that is deeply challenging, governments can take action now to preserve peace and stability in cyberspace. Specifically, governments should:

- *Cite norms, laws, and consequences in attributions:* The speed and coordination of government attributions of cyber-attacks are already improving. However, naming and shaming also needs statements that highlight which international laws or norms are being violated and the likely consequences. This will help strengthen recognition of international expectations.

- *Clarify the interpretation of international law:* Governments have agreed at the United Nations that international law applies online, including in the 2021 consensus report of the UN Group of Governmental Experts on information security, which emphasized that the principles of humanity, necessity, and proportionality must also be observed online. The Oxford Process has convened world-leading international law experts who have opined on the application of international law principles to cyberspace. If states clarify how they understand their obligations under international law they will greatly improve expectations, avoid misunderstandings, and build trust.

- *Consult other stakeholders:* International fora at the United Nations and elsewhere need sustained and substantive multistakeholder participation so that dialogues benefit from the essential expertise of civil society and industry.

- *Create a standing body to support responsible state behaviour in cyberspace:* The use of cyberspace as a domain of conflict will continue and likely worsen. A permanent UN mechanism to deal with cyberspace as a domain of conflict is our best hope for globally and authoritatively coordinated efforts.

- *Consider new norms for evolving threats:* Technology evolves exponentially while norms and regulations evolve incrementally. International norms will need to be updated as threat landscapes and technology uses change. As a first step, states should expressly commit to protect the core processes underpinning digital ecosystems that are not currently protected, including the software update process, and, as we have learned during the pandemic, norms are essential for protecting specific contexts such as healthcare.

Reflections

We recognize that the technology industry, including Microsoft, has many responsibilities, including to our customers and their data. That responsibility extends to protecting digital systems and promoting safe, secure computing for everybody, everywhere. We can only meet that responsibility by taking direct action where we can help to combat nation-state threats and cybercrime, and by fostering deep working relationships between private industry and governments.

Throughout 2022, our experience has demonstrated that early detection and disruption of potentially devastating attacks is possible when the security of systems are connected to the cloud. For example, in Ukraine, for the first time in a major cyber

event, previously identified attack patterns were used to help train machine learning with new analytics tools, broader data sets, and a growing staff of experts to track and forecast cyber threats. Our machine learning tools used behaviour detection to successfully identify and stop further attacks, even before human analysts and users were aware of the threats.

Learning from past examples, our security product teams can identify evolving threat trends by analysing the threat notifications and then focus our product protections to proactively mitigate threats to customers across our cloud services. The analysts tracking these actors combine their knowledge with geopolitical experts to understand the motivations of threat actors. That combination of technical and global analysis into the priorities of nation state threat actors highlights how the actors' motivations often mirror the political, military, and economic priorities of the nation states employing those tactics, techniques and procedures.

Act now

Now is the time to participate in global efforts to maintain peace and stability in cyberspace:

- Join the Cybersecurity Tech Accord[3]: The Cybersecurity Tech Accord fosters collaboration among over 150 global technology companies by partnering on initiatives that improve the security, stability, and resilience in cyberspace.
- Sign the Paris Call for Trust and Security in Cyberspace[4]: Signatories of the Paris Call are national governments, public agencies, civil society organizations, companies and others who work together around nine common principles to secure cyberspace.
- Demand Digital Peace Now[5]: Join over 130,000 individuals from more than 170 countries who demand that nations stop engaging in cyberwarfare and start to protect people from state sponsored cyber-attacks.

References

1 Every day, Microsoft serves billions of customers around the world. Security data is generated by a broad range of organizations and consumers using our technologies in the cloud, endpoints, and the intelligent edge, subject to choices users make on how to configure their systems. The anonymized data which Microsoft collects from users who enable our access gives Microsoft a unique vantage point to analyse a global breadth and depth of signals intelligence, and to develop defensive capabilities to protect our customers and the digital ecosystem. Between July 2021 and June 2022, the volume and diversity of signals processed by Microsoft included:

- 43 trillion signals were synthesized daily, using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.
- Over 8,500 engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, law enforcement professionals, and frontline responders operated across 77 countries.
- 37 billion email threats were blocked.
- 34.7 billion identity threats were blocked.

2 Microsoft, 2022, "Microsoft Digital Defense Report", https://microsoft.com/mddr.

3 Anonymous, 2022, "Cybersecurity Tech Accord", https://cybertechaccord.org/.

4 Anonymous, 2021, "Paris call for trust and security in cyberspace", https://pariscall.international/en/.

5 Anonymous, "Digital Peace Now", https://digitalpeacenow.org/.

The Rapid Evolution of Ransomware Tactics and What to Do About It

Steve Ledzian

Introduction

Ransomware has proven to be a gold mine for cyber criminals looking to monetize their hacking skills. With each attack, they build experience, refining their techniques and innovating along the way. The evolution has been rapid, and defenders need to keep pace with their adversaries or risk finding that those attacking them are always two steps ahead. In trying to understand ransomware, it's helpful to first consider where ransomware sits in the landscape of cybercrime.

One way to categorize and group cyber attacks is by the motivation of the attacker. Common motivations include cyber espionage, cyber crime, and hacktivism. Within the motivation of cyber crime, attackers can turn to a number of different types of techniques to achieve their goals. Some examples might include attacking Point of Sale (PoS) systems to collect credit card information, jackpotting ATMs, fraudulent money transfers by abusing interbanking communications and messaging systems, web skimming (a.k.a. formjacking) to capture credit card numbers of online shoppers, and Business Email Compromise (BEC) scams where an attacker socially engineers a victim into making what they believe is a legitimate payment into an attacker-controlled account. All these different approaches require different levels of

effort and technical expertise and can result in netting the attackers different amounts of stolen gains.

Over the past few years though, one particular technique has dominated the cyber crime landscape and has become the preferred method for cyber criminals to monetize their attacks. The problem of ransomware has grown to be so prevalent, so concerning, and so impactful that it is now considered an "urgent national security risk"[1] as it now threatens to disrupt critical infrastructure.

Understanding ransomware

Almost any definition of ransomware is likely to frame the problem in relation to malware. A belief that ransomware is "malware" may lead to a view that the best way to prevent a ransomware attack, is to have good malware prevention. Let's look carefully at why this is most likely not the case and why it may be more useful to think of the ransomware problem primarily along the lines of being a human-driven digital intrusion.

The impact of early ransomware attacks was a form of service disruption. Typically, victims were tricked into running ransomware malware on their machines, which would encrypt their files making their data inaccessible. The impact of some ransomware variants were limited to a single machine, other malware could spread beyond the initially infected machine to shared or networked drives potentially impacting entire teams instead of just an individual. The types of machines encrypted were typically end-user machines and not servers, simply because end-user machines have humans sitting behind them who can be tricked into clicking on something they should not while servers do not. As a consequence, the impact of these initial attacks, while inconvenient, was usually not catastrophic to the business and ransom demands reflected that, often only amounting in the thousands of dollars.

Attackers wanted to demand larger ransoms, and to do that, they had to attack bigger targets like corporate servers. Getting their malware to run on those servers would be no easy task because again, there was no human sitting behind the server to trick into installing the ransomware on it. Instead, the attackers would have to install the ransomware on the servers themselves and to do this, they would need to intrude into the victim network. With this idea, ransomware evolved into "post compromise ransomware." The impact of this evolution of ransomware was still a disruption, albeit a much more consequential one. Often the attack crippled multiple servers and so the attacker had greater leverage and could demand a higher ransom.

Following post compromise ransomware, attacker's tactics continued to evolve. At this point, attackers had already intruded into victim networks, finding and getting access to critical servers. Once on the servers and ready to manually deploy the ransomware, attackers realized that if they stole some of the data on the servers, which they already had access to, they could gain yet another point of leverage and demand an even higher ransom. This was a pivotal moment in the evolution of ransomware tactics as the nature of the impact of the attack changed from being a service disruption to being a data breach. Depending on the nature of the business, data breaches can be more consequential than service disruptions.

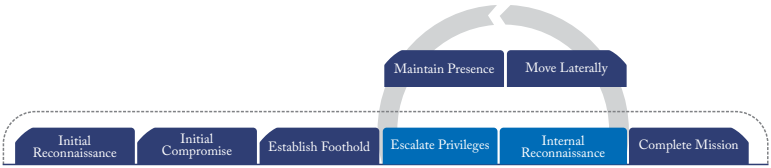
Data breaches can bear greater reputational damage, regulatory fines, and class action lawsuits. With multiple points of leverage against the victims, attackers were now asking for ransoms amounting to millions of dollars, and in some cases getting it.

Small samples of the stolen data are provided as proof that data had been exfiltrated. A threat to publish the stolen data is made to the victim organizations and those victims have to choose between seeing their customer PII, intellectual property, HR files, or whatever may have been stolen be made public, or pay the ransom/extortion. To make matters worse, many organizations had prepared for ransomware by ensuring that they had good

backups. Backups would address the issue of encrypted files, but do not help in stopping the leaking of stolen data.

With all of these evolutions, ransomware was looking less and less like the traditional problem everyone understood very well. Despite these changes, the attacks were still referred to as "ransomware attacks", and in some cases organizations address ransomware risks the way they always had, with a sound backup infrastructure. At Mandiant, we started to refer to these attacks as "Multifaceted Extortion" to more accurately reflect the changing nature, complexity, and impact of these attacks.

Rather than getting hit by a ransomware "malware", it is better to envision a ransomware attack as human intrusion into the victim network. This intrusion spans the typical stages of the cyber attack lifecycle. These stages include : Initial Reconnaissance, Initial Compromise, Establish Foothold, Escalate Privileges, Internal Reconnaissance, Move Laterally, Maintain Presence, and Complete Mission. The actual ransomware malware only comes into play at the very last stage: Complete Mission. Defenders who focus on the malware are giving up the opportunity to stop the attack much earlier by addressing the intrusion at an earlier stage. That revelation is the key takeaway. If you want to avoid a ransomware attack, do not put your primary focus on the ransomware malware, but rather the human intrusion that precedes it.



There is one more evolution to consider now that the problem is framed in the context of this attack lifecycle. That evolution is division of labour and specialization of multiple actors across this attack lifecycle to accomplish a specific attack instance. With Ransomware as a Service (RaaS) providers, the late stages of the attack lifecycle can be outsourced to other groups who have

expertise in malware creation and shaming victims by publicly disclosing stolen data. With Initial Access Brokers, the early stages of the attack lifecycle can be outsourced to other groups who have expertise in intruding into networks. The human intrusion that precedes the ransomware deployment does not have to be done entirely by the same threat actor. There are permutations and combinations of these intrusions as different stages of the attack lifecycle are accomplished by different groups. This complicates detection of intrusions for defenders as different groups will use different techniques and the spectrum of attack building blocks that need to be mitigated becomes a wider and more difficult problem to manage.

The final takeaway from understanding all of these evolutions is to shift from thinking of ransomware attack simply as a "malware" to thinking of ransomware attacks as digital intrusions carried out by human attackers. If organizations want to be effective in stopping ransomware attacks, they must be effective in stopping intrusions. Stopping intrusions is a tall order given the variety of way actors intrude into networks.

Recommendations to mitigate modern ransomware risk

Proactivity

To intercept a ransomware attack, organizations need to have a capability to notice prevention failures that allow attackers to intrude into their network. Typically, Mandiant observes that intrusions often go unnoticed for long periods of time, and it is not possible to respond to an intrusion, which has not been detected. Mandiant's M-Trends report 2022[2] (a report of the trends and learnings of Mandiant responding to victims of cyber intrusions) tells us that cyber intrusions in APAC organizations go unnoticed for an average of 21 days. The same report highlights that ransomware threat actors can complete their movement across the

entire attack lifecycle and deploy ransomware in just nine days after achieving initial compromise. Noticing, intercepting, and mitigating successful cyber intrusions is often beyond the inhouse capability of many small organizations, and challenging even for many enterprises. Organizations who need help in this area can turn to Managed Detection & Response (MDR) services.

Auditing Security Control Effectiveness (Not Just Existence)

While addressing the intrusion that precedes the ransomware deployment is paramount, it is not to say that addressing the ransomware malware can be ignored. Typically, organizations will have many security controls such as firewalls and antivirus in place to address the malware concern. It is not enough though just to have these security controls in place, organizations also have to regularly test their effectiveness against the latest ransomware threats. Breach & Attack Simulation (BAS) solutions can help in this area.

Ensuring Business Preparedness

CEOs whose organizations have been hit by ransomware attacks often say that the decisions that they needed to make during the attack were some of the most difficult decisions of their careers. Often these decisions need to be made in the absence of a clear picture and without complete information. To make matters worse, these attacks are often the CEO's first encounter with ransomware, and they have no practice or experience to draw upon to inform that decision-making.

Many organizations are preparing by practicing this business-level decision-making with role-play scenarios. Tabletop Exercises (TTX)[3] can help in creating realistic, industry aligned attack scenarios that lets business leaders experience what they would be faced with in a real-world attack and practice decision-making, without actually impacting the business.

In a crisis, the most precious resource is time. Organizations looking for help from incident response firms are not going to want to waste that time working out agreements on the details of contracts and other legal documents. Incident response firms can be available through retainer via Incident Response Retainer Services (IRR)[4] to save precious time and increase readiness for cyber crises.

Prepare For Failure

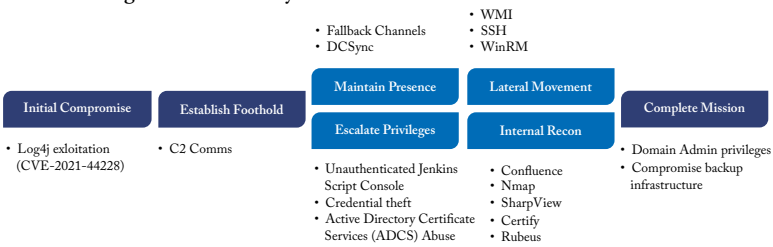
Despite defenders' best efforts, sometimes attackers will still be successful in completing all the stages of a ransomware attack and the organization will be impacted. For this reason, it's not enough to try to prevent ransomware. Organizations also need to have a plan to respond and recover from a ransomware attack should they be hit. Having a plan can help in reducing the overall impact, and the shorten the recovery time. Organizations who have a plan and would like it assessed or organizations that don't yet have a plan can consider a Ransomware Defense Assessment (RDA)[5]. The freely available M-Trends 2022 report also has an entire chapter focused on "Observations on Ransomware Recovery Operations."[3]

All The Bases Covered?

What if your organization already has all the bases covered? Once ready, an organization can test themselves with a Red Team Assessment (RT)[6] simulating a real-world ransomware attack in a no-holds-barred friendly sparring session. The organization being assessed should define the mission objectives for the red team that they hire. For example, in a ransomware scenario the mission objectives could be to acquire Domain Admin privileges and to demonstrate the capability to compromise critical backup infrastructure. The red team can then attempt to progress through the full attack lifecycle exactly as a real world attacker would while trying to defeat security defences and avoiding detection by their

target. This sort of exercise tests cyber defences systemically across people, process and technology.

Red Team Targeted Attack Lifecycle



Conclusion

A ransomware attack is not perpetrated by a malware, it is driven by an ecosystem of human criminals each with their own specializations working in concert. Looking at the full attack lifecycle of a ransomware attack gives defenders the greatest set of opportunities to identify, intercept and interrupt the attack.

Of all the incident response work that Mandiant did in Asia Pacific & Japan (APJ) in 2020 only 12.5 per cent was related to ransomware. That number grew to 38 per cent for the incident response work Mandiant did in 2021. The growth of these observed ransomware attacks is higher in APJ than anywhere else in the world.

Cyber risk should be close to the top of the business risks organizations are paying attention to. And at the top of the lists of cyber risks should be ransomware attacks. These attacks are high frequency and high impact. Fortunately, there are many ways organizations can work to prepare for and mitigate this risk, it is just a matter of taking the problem seriously, and then following up with action to address it.

References

1 Institute for Security + Technology, "RTF Report: Combating Ransomware", 2021, https://securityandtechnology.org/ransomwaretaskforce/report/.

2 Jurgen Kutscher, "M-Trends 2022: Cyber Security Metrics, Insights and Guidance From the Frontlines", Mandiant, 19 April 2022, https://www.mandiant.com/resources/m-trends-2022.

3 Mandiant, "Tabletop Exercise", https://www.mandiant.com/sites/default/files/2021-09/ds-tabletop-exercise-000005-2.pdf.

4 Mandiant, "Incident Response Retainer", https://www.mandiant.com/sites/default/files/2021-09/ds-incident-response-retainer-000038.pdf.

5 Mandiant, "Ransomware Defense Assessment", https://www.mandiant.com/services/ransomware-defense-assessment.

6 Mandiant, "Red Team Assessment", https://www.mandiant.com/services/technical-assurance/red-team-assessment.

Why Zero Knowledge is The Missing Piece in The SSI Puzzle

Team Polygon

The emergence of self-sovereign identity with privacy and trust principles

"The Internet was built without an identity layer" goes the popular quote by Kim Cameron, one of the key contributors to the early evolution of the Self-Sovereign Identity (SSI) movement. The Internet was built to solve the problem of interconnecting machines on a global scale. The human element was not at the center in the early days of the Internet. The result of this "original sin" is that Personally Identifiable Information (PII) must be re-entered by humans and stored on the servers of each individual platform we might interact with, where it could get out of sync and even rendered prone to hacks.

The self-sovereign identity movement which started around 2005, proposes a shift from the centralized and federated identity models that we live in currently (think big social media platforms and content streaming companies that exploit our data and preferences). The SSI movement moves the Internet towards a model where users are in control of their personal data and can choose to what parties they disclose this data to.

The vision behind SSI describes an ecosystem comprised of three elements:

1. Issuers (entities that issue claims or credentials, for example, governments or educational institutions)
2. Identity Holders (persons or things that hold a claim or credential)
3. Verifiers (entities interested in using the claims and credentials presented by the holders)

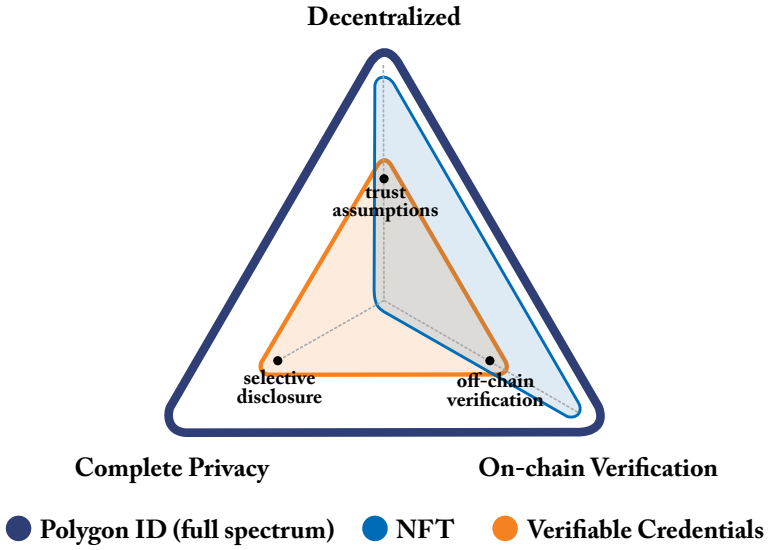
This ecosystem will allow Identity Holders to have control over their personal information and choose which credentials to reveal to the Verifiers. The World Wide Web Consortium (W3C) has led the way in SSI through the Decentralized Identifiers recommendation[1]; with more than 100 Decentralized Identity (DID) methods registered so far, the use of Verifiable Credentials and DID has become the industry de-facto standard for SSI.

Introducing Polygon ID and the Iden3 protocol

A decentralized and privacy preserving SSI solution for the future Web 3.0, Polygon ID solves some of the existing challenges in SSI adoption through its use of Zero Knowledge Proofs (ZKP) to preserve privacy and facilitate digital identity management. Polygon ID is an implementation of the Iden3 protocol, which has been in development since 2018.

Polygon ID supports the verifiable credentials standards, and has its own DID method (DID: iden3, pending registration). This combines all the benefits of a consolidated standard with the unique benefits of a Web3 native solution (decentralization, private on-chain verification, and composability). This innovation makes for better privacy for users when compared with VCs and SBTs (Soul-bound tokens or Non-transferrable NFTs).

Figure 1: Three dimensions to look at when comparing Polygon ID, SBT and VCs

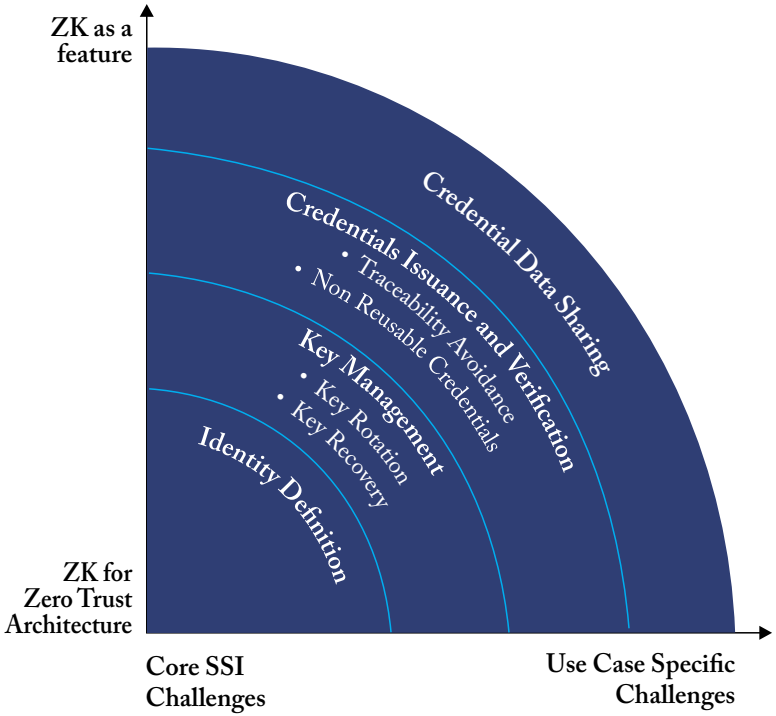


How Zero Knowledge became a pillar of SSI

To achieve the goals of decentralization and self-sovereignty, decentralized identity protocols face several challenges that are well known in the industry. Some of these challenges have their origin in the core principles of SSI, like the user-centric nature of the identity and how that becomes a burden for the identity holder. Other challenges present themselves only in certain use cases, such as when issuers or verifiers could not be trusted to behave honestly.

We will now explain how ZKP can be used to provide enhanced solutions to these challenges at different levels of the architectural design – from adding features at the user level to changing the underlying architecture of the identity protocols.

Figure 2: Areas where zero-knowledge could add innovation to the architecture of an SSI protocol



First layer: identity definition

Although some initial approaches to the implementation of decentralized identifiers assumed that a decentralized identifier is based on (and generated from) the control of one public/private key pair[2], but the more recent implementations of the DID standard assume that an identity can control multiple keys.

However, Web3 solutions that try to tackle decentralized identity challenge this understanding by using blockchain addresses as identifiers (your wallet = your identity). This is the basis of some NFT/soul bound token-based identity solutions, which assume that entire identities could be built around a single key pair and stand in contrast to the DID standards mentioned above.

As discussed earlier, Polygon ID's approach is in line with the DID and verifiable credentials standards. The standard only recommends that an identity can "control" multiple keys, but it does not prescribe any implementation in specific. Polygon ID builds on this and goes further with an innovative approach through the use of ZKP. A zero-knowledge proof allows one to prove the truth of a statement without sharing the statement's contents.[3] Using ZKP, one can prove that an identity has control over a set of keys. This mechanism decouples the identity from the keys. Identity is not a public key. An identity owns a number of keys and can be represented by a number of identifiers.

Using a new concept called "Identity State", Polygon ID is able to separate individual identities from individual key pairs. They are defined using ZKP and merkle trees. Identity States consist specifically of 3 merkle trees: claims, revocations, and previous roots. [4]

This way, the relationship between the identity (the decentralized identifier) and the cryptographic keys is added as a claim to the Claim Merkle Tree in the identity state. The ownership is proved using ZKPs. This means that the user can generate a ZKP that they know the private key corresponding to the public key claim added to the Claims Tree (a "merkle tree proof"), without revealing the claim and its position in the tree.

The details of this proof and the circuits used to generate it are available in the Iden3 protocol specification.[5] This means we can provide an anonymous proof that an identity is controlled by a specific key. In addition, the user's identity can revoke any given key by adding a leaf of the nonce of the original claim to their revocation tree. A nonce is a special unique number tied to each claim.

Second layer: key management

The architectural decisions detailed in the first layer allow us to provide a better user experience in usually complex scenarios like key recovery and key rotation. The second layer of challenges then becomes identity management and the key lifecycle.

Key Rotation

To enable key rotation, an identity can self-issue and revoke many public key claims using the identity's claims tree mentioned earlier. To support verification of such claims, an identity state is publicly available on the blockchain. Any private key for which a corresponding claim exists in the Identity Claims Tree (and is not present in the Identity's Revocation Tree), can be used to create a ZKP of valid credentials. Such proof should pass verification by a verifier as it is able to check the latest identity state in the blockchain. In the same way, any valid and non-revoked identity private key can be used to create a valid ZKP for the Identity's State Transition Function.

Key Recovery

The idea of "Identity State" was introduced earlier. It is a data structure defining the status of the identity in terms of identifier, issued claims, revocations to issued claims, and history of past states.

For the sake of transparency, compliance, and auditability, our protocol includes a Smart Contract that validates the transition of the Identity state to a new state ("Identity state smart contract", IDSC). This smart contract checks that the changes to the identity state adhere to certain rules before publishing the new Identity state on chain. One of these requirements is that the application making these changes can prove the control of a single private key controlled by the affected identity. This makes the IDSC contract the "gate keeper" of any changes to the identity state (protecting the Identity from being taken over by someone not in control of the private keys).

Key Recovery is a known challenge in the Public Key Infrastructure. A user centric identity means that the user is responsible for keeping the private keys safe, even at the risk of losing their identity forever.

Besides the fact that our protocol allows the user to associate multiple keys to the same identity (reducing the risk of losing the control of the identity by having multiple backups), the IDSC opens the door for the implementation of multiple recovery mechanisms (through social recovery or biometrics).

By creating an alternative Transition State Smart Contract (Recovery Transition State) we can change the requirements for a change in the identity state. For example, instead of requiring the control of the private keys associated with the Identity we could ask for the signature of three trusted parties, or the proof of human identity provided by a biometric or KYC provider. This innovative recovery mechanism is not possible with other SSI protocols currently available. Since all these operations take place on-chain, the usage of ZKP is crucial to maintain the necessary levels of privacy.

Third layer: credentials issuance and verification

The third layer in the identity lifecycle is related to the interactions between the Identity Holder, the Issuers, and Verifiers. In this regard, we need to evaluate the trust that we put in these actors. In Web3 it is very common to assume a "trustless environment", where we want to minimize the trust assumptions of the system – or what is the same, we should follow an adversarial line of thinking in the design of the interactions between these three.

Following this line of thought, we want to prevent the following attack vectors:

Traceability avoidance: an issuer is capable of tracing the activities of one identity.

To avoid this, our protocol avoids any interaction (and thus traceability) with the claim Issuer in these two scenarios:

- **Claim Verification:** The Issuer signature is used to prove the provenance of the claim.
- **Claim Revocation Status Check:** Each identity has a claims tree and a separate revocations tree. The claim tree is private and only its merkle root is public, the revocation tree however is entirely public. An identity (the Issuer) can specify that a claim is no longer valid by adding the revocation nonce of the original claim as a leaf in its revocation tree. An identity (Identity Holder) that wishes to prove that a claim is valid (and thus not revoked or updated) needs to generate one ZKP about two facts. First, prove that the claim was issued at a specific time (this proof is generated once by the issuer and kept in the Identity Holder wallet). Second, prove that the claim has not been revoked (this special proof is generated by querying the issuer's revocation tree published on a decentralized storage).

Traceability avoidance: verifiers can collude to trace an identity.

In the scenario where a third party is in control of multiple verifiers (or can observe the interactions between identity holders and multiple verifiers) we want to prevent a third party from tracking the activity of the identity across multiple verifiers.

An example of this would be a government that controls both the e-government services and the e-voting infrastructure, and must not be able to break the anonymity of the vote by correlating identifiers using the e-government services data.

We achieve this with nullifiers. A nullifier is a verifier-application-specific Identifier generated by hashing the Identity Identifier and another piece of information (a nonce – that is specific to that verifier). This way, a different identifier could be offered to

each verifier application (one identifier for e-government, and a second one for voting). We use ZKP to prove that the Nullified Identifier is generated from an Identifier that is in control of the public keys used for the signature.[6]

Non reusable credentials: a malicious verifier (or an attacker with access to the ZKPs) wants to publish the ZKPs without consent of the identity holders.

By getting access to ZKPs, a third party could run a verification process (assuming the conditions checked are known) to obtain information about the Identity Holders. Another scenario is when a malicious verifier discloses the proofs without the consent of the identity holders.

We add an additional condition to the Zero Knowledge circuits that generate the proof on the Identity Holder side like this:

- Either the conditions proven by the Identity Holder are true OR the identity holder is in control of public key of the verifier.

Now, only the verifier can fully trust the results of these proofs (since the verifier is the only one with total certainty about the fact that nobody else has control of his keys).

This is an additional security measure that mitigates the following risks:

- If a malicious Verifier publishes the proofs, nobody will have total certainty about the validity of the proofs (unless the verifier shares the private keys).
- A verifier could preventively create lots of fake proofs, where the second element of the proof is True and the first element is false. Without the Verifier private keys it would be impossible for an attacker that has access to the proofs to distinguish between valid and fake proofs.

Fourth layer: credential data sharing

Finally, we have the layer dealing with the interaction between the Identity Holders, Verifiers, and Issuers. Here is where we have seen the most adoption of Zero Knowledge technology, we have various examples of how Zero Knowledge technology allows an identity to share a proof of a claim as opposed to the full or partial claim information. This is perhaps the most obvious application of ZKP – that is, prove that you are older than 18 without telling your birthday.

Using proofs instead of full data, we are able to offer an on-chain verification option for trustless and private implementations.

The impact of Zero Knowledge in common SSI use cases

In the following table we analyse the impact of Zero Knowledge in some of the best-known cases of SSIs.

Use case title	How ZK-powered SSI solutions will address these challenges
DAO governance	Provides DAOS the ability to verify membership without disclosing a member's identity (ZK proof of membership, humanity, etc.)
Reusable KYC	Provides an identity layer with re-usable KYC/ KYB that is secured and instantly verifiable, while maintaining the customer's privacy across multiple service providers (non-traceable) and for on-chain verifications.
Portable reputation and avatars	Given the decoupling between Web3 addresses, Identity and Identity Keys enabled by ZK proofs, it is possible for an individual to "segment" his/her public reputation (gaming, professional) but also to merge these segmentations when needed.

Use case title	How ZK-powered SSI solutions will address these challenges
Under-collateralized lending	ZK proofs and ZK Query Language are used to enable a private and efficient On-chain verification of the reputation, allowing for a decentralized and trustless implementation of this idea.
Health and travel Passport	ZK plays a role both at minimizing the amount of data shared and preventing unwanted traceability of the use of these credentials.
NFT provenance and UX	ZK proofs and ZK Query Language are used to enable a private and efficient On-chain verification of the reputation, allowing for a decentralized and trustless implementation of this idea.
eGovernance services	ZK plays a role both at minimizing the amount of data shared and preventing unwanted traceability of the use of these credentials. Moreover, given the critical importance of these credentials and the high level of compliance and privacy required, the simplification in the key rotation and the facilitation of identity recovery mechanisms is crucial. ZK can provide both the Sybil resistance and privacy features required by e-voting. No other technology can do that.
Digital prescriptions and medical reports	ZK plays a role both at minimizing the amount of data shared and preventing unwanted traceability of the use of these credentials. Moreover, given the critical importance of these credentials and the high level of compliance and privacy required, the simplification in the key rotation and the facilitation of identity recovery mechanisms is crucial.

Conclusion

We have described various uses of ZKP across the entire spectrum of SSI architectural layers: From the most common and known uses (sharing a proof derived from the credential's data instead of the actual data) to some of the biggest challenges in key management (key rotation and recovery). The use of Zero Knowledge in these areas has been demonstrated to improve not only the privacy of the SSI solutions but also the user experience and the scalability of the solution.

For privacy, this could mean proving your credentials without disclosing your data; preventing issuers from knowing when and how the credentials are used; or preventing verifiers from tracking the activity of an identity through multiple verifications.

In terms of user experience, this could be allowing an easy key rotation without any impact on the identity verification experience.

As far as scalability is concerned, the verification of credentials is a process that involves multiple checks, not only on the credentials, but also on the identities involved (holder, issuer), the validity of the claim (claim provenance, non-revocation, non-expiration) – and finally the conditions applied to the credential data (age > 18, country = Iran). All these checks are processed in the wallet and proven to the Smart Contract through a proof. The cost of the on-chain verification is constant and it doesn't depend on the complexity of these checks.

Considering the evidence, it seems reasonable to conclude that the use of Zero Knowledge should be considered as an architectural pillar of Self Sovereign Solutions and should guide the best practices and standards defined in this area. We hope that the contributions from Polygon ID and the Iden3 protocol will bring further adoption of SSI and verifiable credentials in a way that preserves user's privacy.

References

1 Anonymous, "DID Specification Registries", World Wide Web Consortium, https://www.w3.org/TR/did-spec-registries/.

2 Affinidi Pte. Ltd., "Role of Public Key Cryptography in Self-Sovereign Identity", 15 July 2021, https://academy.affinidi.com/role-of-public-key-cryptography-in-self-sovereign-identity-8c2d-c37a2bf3.

3 Ethereum, "What are zero-knowledge proofs?", https://ethereum.org/en/zero-knowledge-proofs/.

4 For details, see Anonymous, "Iden3 Protocol Specifications", https://docs.iden3.io/protocol/spec/#definitions.

5 Ibid.

6 This approach presents some challenges when Sybil Resistance is needed by the verifier. We are currently researching new solutions (based on ZKP) to solve this scenario.

Security and Trust in The Post-Quantum Era

Sunil Gupta

Over the last couple of years we have seen accelerated digital business transformation. The amount of data generated and stored in the cloud and on-premise as part of this transformation has, and will continue to make organizations faster, and more intelligent and efficient. Unfortunately, it will also result in more challenges as breaches persist in sustained attempts to access these valuable enterprise data stores. More advanced data protection that empowers business operations is desperately needed, and the current solutions could be inadequate for the task at hand.

As devices and systems in our critical infrastructures become ever more interconnected, it is becoming increasingly important to ensure that they have adequate cryptographic protections. This is particularly challenging – yet even more essential – given the potential scalability of the attack vectors in this hyper-connected world. Action is required now, both to ensure security in the present context, and to prepare for future technology advances.

Systems and assets have developed into a networked Internet of Things, where machines talk to machines and devices to devices without human interaction. Examples include electricity grid, smart grids, and train networks, where commands could now be sent over open transmission networks using IP-based protocols such as Multiprotocol Label Switching; the connections to

smart meters deployed in millions of homes; to the devices underpinning smart cities; or, in the future to the millions of smart cars driving autonomously on our roads which depend on embedded IoT devices.

Such hyper-interconnected infrastructures present a whole new set of security challenges. Rapid advancements in technology will add new attack vectors which were not conceived of, or which were not feasible at the time devices were originally deployed – especially given the long lifetimes of critical infrastructure devices in the field. The scalability of the attack vectors is unprecedented, where a single successful hack could affect millions of devices. In the world of ubiquitous IoT, if a hack can cause an entire smart city infrastructure to fail, or the entire self-driving car or rail network to go down, then it could easily spiral into a national security issue.

Many of the core requirements for the security of modern critical infrastructures depend on cryptographic primitives. Therefore, we must consider the implications of the emergence of new quantum technologies on cryptographic primitives – both in the context of creating new threat vectors, as well as providing security solutions. Cryptography is fundamentally crucial – if the underlying crypto primitives fail, then the security of the device(s) and the network fails as well.

All cryptographic algorithms currently in use are subject to security decay over time; mainly due to the steady increase in available computational power. Considering the rise of quantum computers especially, as soon as sufficiently strong quantum computers come into existence, established asymmetric schemes like RSA, DSA, and ECDH will be broken in no time. The timelines for this may not be very clear at the moment but it is inevitable.

The very prospect of quantum computers has led to a new approach to attack, called "Harvest Now, Decrypt Later". Hackers in this case are copying and storing large volumes of encrypted critical data, to be decrypted later using quantum algorithms

such as Shor's algorithm on scalable quantum computers. This essentially means data that is encrypted and cryptographically secure today, will not be secure in the post-quantum era and will possibly lead to a "Data apocalypse".

In order to protect most of the existing encrypted data, which uses public key cryptography, two promising solutions have emerged that are expected to provide forward security in the post-quantum era. While the symmetric encryption algorithm AES 256 is expected to be safe even against large quantum computers, the asymmetric encryption algorithms used to generate session keys remain highly vulnerable, and are certain to be broken with large quantum computers. Thus, the focus needs to be on a solution that can keep encryption keys secure against attacks leveraging the sheer power of quantum computers.

The first such solution is called Quantum cryptography, which uses the principles of quantum physics ("Heisenberg uncertainty principle" and "No cloning" theorem). This solution generates a pair of secret keys across two nodes connected through optical fiber, without sharing any key information on the network. Any man-in-the-middle attack on optical fiber perturbs the quantum state of photons on the quantum channel and it is detected by the Quantum Key Distribution (QKD) hardware, which immediately stops generating the key thus protecting the key from falling into the hands of the attacker. This solution requires the deployment of a pair of specialized hardware boxes at two ends connected through a dark fiber. Moreover, it works for a limited distance of up to 150 km point to point, but using Trusted Node technology multiple QKD boxes could be connected in a daisy chain configuration to extend the range to longer distances.

The other solution is Post Quantum Cryptography (PQC), which offers quantum-resistant security and uses advanced mathematics (lattice code, multivariate, hash, etc.) based algorithms to generate session keys. These algorithms are based on tough problems, which can't be broken by any known quantum

algorithms, even when run on a large quantum computer. However, this is not assured as new quantum algorithms might emerge in the future, which can break PQC algorithms. That makes PQC weaker compared to QKD. Since PQC adopts a software-based approach, it does not have the limitations of media and distance as in the case of QKD, and thus it is advised to be used to offer advanced security for Internet protocols.

Recently, the National Institute of Standards and Technology (NIST) of the US Department of Commerce has identified the first group of quantum-resistant cryptographic algorithms that are designed to withstand the assault of a future quantum computer. These four cryptographic algorithms will become a part of NIST's post-quantum cryptographic standard, which is expected to be finalized in about two years.

These algorithms are designed for two main tasks for which encryption is typically used: to protect information exchanged across a public network, and digital signatures which are used for identity authentication. All four of the algorithms were created by experts collaborating from multiple countries and institutions.

For general encryption, used when we access secure websites, NIST has selected the CRYSTALS-Kyber algorithm. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation. For digital signatures, often used when we need to verify identities during a digital transaction or to sign a document remotely, NIST has selected the three algorithms: CRYSTALS-Dilithium, FALCON and SPHINCS+.

The great news for India is that it has its own quantum-safe and quantum-resistant technology-based solutions, which could be used today to protect our critical infrastructure and ensure future security against quantum computers. Given the seriousness of quantum computer attacks that can disrupt or suspend a critical infrastructure, the adoption and application of quantum security

in defence, intelligence, telecom, banking, nuclear installations, airports and railway networks, etc. must be taken up as one of the top priorities.

Another important aspect to be considered in the post-quantum era is the ease of upgrading to new algorithms without disrupting business. Crypto-agility describes the feasibility of replacing and adapting cryptographic schemes in software, hardware and infrastructures without any major changes to the underlying cryptographic infrastructure. For example, in recent years, the transition from SHA-1 to SHA-256 took more than five years. While the specifications and implementation were done quickly, updating software and hardware products by vendors, providers, or administrators took a long time. Crypto-agile solutions would make this task easier and faster, and thus crypto-agility will become a cornerstone of the migration strategy.

Globally a lot of research initiatives are attempting to extend QKD networks through satellites. Many academic and industry players have carried out successful experiments to achieve this objective. Extensive research effort is focused on building single-photon detectors, which are a critical part of QKD. Some efforts have also picked pace in the area of integrated photonics to miniaturize the technology to a chip scale so that it could be embedded in IoT devices, mobile phones, laptops and other edge devices. Post-quantum era is inevitable and a number of initiatives across the world are seeking to prepare the technology, platforms and standards to implement the technology in an easy and seamless manner.

Part 3

Future of Digital ++

Digital Human Rights

Vakul Sharma

"On the roads banyan trees were caused to be planted by me, (in order that) they might afford shade to cattle and men, (and) mango-groves were caused to be planted. And (at intervals) of eight kos wells were caused to be dug by me, and flights of steps (for descending into the water) were caused to be built. Numerous drinking-places were caused to be established by me, here and there, for the enjoyment of cattle and men." – *Ashoka [Major Pillar Edict No. 7]*[1]

One of the earliest examples of observing human rights manifested in the form of providing comfort as little as a shade of banyan tree, flight of stairs or drinking water, Emperor Ashok [BCE 268 – 232 BCE] through its edicts created a grammar of human rights.

The concept of human rights has evolved over centuries of civilization struggle and turmoil from tribes to Greek city-states to the modern state, thanks to religious sutras/sermons/codes to philosophical and political writings. Every influential thinker has always ideated human rights as a struggle between the State and the Man.

State versus man

The human right is an inalienable right available to all irrespective of their status in the social strata. It is not constitutional rights or guarantees, but rights which are part of individual's

existence from "cradle to grave" – a state has to recognize this and often it is bundled as the fundamental rights (inalienable rights) under the Constitution or rule of law that governs the existence of the state. This rule of law has manifested itself in various forms: fundamental rights to duties to guarantees. The first struggle to enshrine human rights as constitutional guarantees met with success when the rule of law guaranteed fundamental rights to every citizen. The fundamental rights guaranteeing right to speech and expression, and right to life have become energy sources to nurture civil society. However, the second struggle of effective implementation of the fundamental rights by the state and its organs still continues.

"Let them eat cake" is attributed to Marie Antoinette, the Queen of France during the French Revolution. It is alleged to be the queen's response upon being told that her starving peasant subjects had no bread. Likewise, nation states without providing basic human rights to their citizens have started granting them the Digital Human Rights (DHRs). It is an exercise in deception as without meaningful access to Human Right (HRs) in physical space, DHRs are being offered, and that too based on the same HR template. There is dearth of innovative thinking. If HRs are subject to reasonable restrictions in the form of laws, then their digital version, DHRs, are also witnessing similar restrictions, or could be even more.

State v digital man

The United Nations Secretary General's Roadmap for Digital Cooperation speaks about ensuring the protection of human rights. It has the following components[2]:

1. *PLACE HUMAN RIGHTS AT THE CENTRE of regulatory frameworks and legislation on digital technologies*
2. *GREATER GUIDANCE ON THE APPLICATION OF HUMAN RIGHTS STANDARDS in the digital age*

3. *ADDRESS PROTECTION GAPS CREATED BY EVOLVING DIGITAL TECHNOLOGIES*
4. *DISCOURAGE BLANKET INTERNET SHUTDOWNS and generic blocking and filtering of services*
5. *HUMAN RIGHTS-BASED DOMESTIC LAWS and practices for the protection of data privacy*
6. *CLEAR, COMPANY-SPECIFIC ACTIONS TO PROTECT PRIVACY RIGHTS and other human rights*
7. *ADOPT AND ENHANCE SAFEGUARDS RELATED TO DIGITAL IDENTITY*
8. *PROTECT PEOPLE FROM UNLAWFUL OR UNNECESSARY SURVEILLANCE*
9. *HUMAN-RIGHTS BASED LAWS AND APPROACHES to address illegal and harmful online content*
10. *TO ENSURE ONLINE SAFE SPACES, TRANSPARENT AND ACCOUNTABLE CONTENT GOVERNANCE FRAMEWORKS that protect freedom of expression, avoid overly restrictive practices and protect the most vulnerable*
11. *UNITED NATIONS SYSTEMWIDE GUIDANCE ON HUMAN RIGHTS due diligence and impact assessments in use of new technologies*

This roadmap has highlighted areas to strengthen the extent of human rights in the digital age. The primary focus is to have an open, safe, secure and accountable digital ecosystem, supported by the rule of law, so as to remove any arbitrariness or inconsistency in decision making. This roadmap is about regulating the processes and not technologies. It considers technology as a fait accompli. In other words, the focus is to regulate human actions.

A critique of the United Nations approach

The United Nations in its roadmap has taken technology out of the digital human rights equation. It is human action that is to be made responsible and must conform to the technology template. This essentially means "Human standards" are supposed to follow "Technology standards" or protocols. Is it an abject surrender to the technology and an admission that the technology cannot be regulated? In a way, it has negated the centuries of struggle to give primacy to the human rights. Now what we are witnessing is primacy of technology over human rights, and the latter being made a sub-set of technology. Digital human rights are not inalienable rights. The fundamental rights granted to a citizen are now subject to technology advancement.

Thus, the very first objective as articulated above states: "PLACE HUMAN RIGHTS AT THE CENTRE of regulatory frameworks and legislation on digital technologies" can be restated as: "PLACE HUMAN RIGHTS ALONG WITH DIGITAL TECHNOLOGIES AT THE CENTRE of regulatory frameworks and legislation."

Digital Human Rights design

Digital human rights model presently available to the citizens is primarily based on legacy Human Rights. It comes with a heavy dose of regulations. If we compare DHRs with legacy Human Rights, one will find regulation of HRs in the digital realm arbitrary, whimsical, and unreasonable. Such regulations are often in the form of vague laws, and such laws may trap the innocent by not providing fair warning. Second, if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them. A vague law impermissibly delegates basic policy matters to policemen, judges and juries for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application.

The pertinent question is why vague laws are being framed? The answer lies in the fact that the basic policy matters, especially related to the issues which are part of the DHRs ecosystem never received any inputs from the fields of "digital sociology"[3], or "digital anthropology"[4], or neural sciences. The result is the expertise available in terms of cogent digital data is rarely being utilized. It is therefore prudent that while designing basic policy matters related to DHR, inputs from other fields of study are sought and considered.

DHRs in the Indian context

The development of DHRs in India as a policy and regulatory framework may be seen in the context of the Information Technology Act, 2000[5] (IT Act). It laid down the concept of functional equivalent approach, meaning that law does not discriminate between the "physical form" and its functional equivalent, the "electronic form". Over the last 20 years, the IT Act did influence the concept of DHRs, but there has not been any formal declaration, directive or policy document envisioning a roadmap for the digital human rights in India.

Shreya Singhal v Union of India[6]

Shreya Singhal v Union of India is a landmark judgment that must be hailed as the first step towards protecting the digital human rights as tested/ adjudged by the Supreme Court on the touchstone of the principles of the Constitution of India. A Division Bench of Supreme Court comprising Justice J. Chelameswar and Justice R.F. Nariman struck down[7] Section 66A of the IT Act as unconstitutional, as it is violative of Article 19(1)(a) and not saved under Article 19(2) of the Constitution related to the right to freedom of speech and expression. The said section read:

Section 66A. Punishment for sending offensive messages through communication service, etc.—Any person who sends, by means of a

computer resource or a communication device,—

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device; or

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

The Supreme Court held that:

"Chilling Effect and Overbreadth Information" *that may be grossly offensive or which causes annoyance or inconvenience are undefined terms which take into the net a very large amount of protected and innocent speech. A person may discuss or even advocate by means of writing disseminated over the internet information that may be a view or point of view pertaining to governmental, literary, scientific or other matters which may be unpalatable to certain sections of society. It is obvious that an expression of a view on any matter may cause annoyance, inconvenience or may be grossly offensive to some. A few examples will suffice. A certain section of a particular community may be grossly offended or annoyed by communications over the internet by "liberal views" – such as the emancipation of women or the abolition of the caste system or whether certain members of a non proselytising religion should be allowed to bring persons within their fold who are otherwise outside the fold. Each one of these things may be grossly offensive, annoying, inconvenient, insulting or injurious to large sections of particular communities and would fall within the net cast by section 66A. In point of fact, Section 66A is cast so widely that*

virtually any opinion on any subject would be covered by it, as any serious opinion dissenting with the mores of the day would be caught within its net. ***Such is the reach of the Section and if it is to withstand the test of constitutionality, the chilling effect on free speech would be total."***

Interestingly, the above judgment made a humongous impact, but nevertheless across India there have been large number of instances wherein Section 66A of the IT Act was used by the police authorities to prosecute the citizens even after Shreya Singhal's judgment. This led to another intervention by the Supreme Court to safeguard citizens' digital rights in no uncertain terms. In People's Union of Civil Liberties v Union of India & Ors,[8] the Supreme Court directed:

"The information given in tabular form shows that despite the issue regarding validity of Section 66A of the 2000 Act having been pronounced upon by this Court, number of crimes and criminal proceedings still reflect and rely upon the provisions of Section 66A of the 2000 Act and citizens are still facing prosecution for the alleged violation of Section 66A of the 2000 Act.

Such criminal proceedings, in our view, are directly in the teeth of the directions issued by this Court in Shreya Singhal (supra). Consequently, we issue following directions:

(a) It needs no reiteration that Section 66A of the 2000 Act has been found by this Court in Shreya Singhal (supra) to be violative of the Constitution of India and as such no citizen can be prosecuted for alleged violation of offence under Section 66A of the 2000 Act.

(b) In all those case where alleged violation of Section 66A of the 2000 Act has been projected and citizens are facing prosecution for such alleged violation, the reference to Section 66A of the 2000 Act from all these crimes or criminal proceedings shall stand deleted.

(c) We direct all the Directors General of Police as well as Home Secretaries of the States and Competent Officers in Union Territories to instruct the entire police force in their respective States/Union Territories not to register any complaint or crime with respect to alleged violation of Section 66A of the 2000 Act.

(d) * * * * * *

(e) Whenever any publication, whether Government, Semi Government or Private, about Information Technology Act is made and Section 66A is quoted, the readers must adequately be informed about the fact that the provisions of Section 66A of the 2000 Act have already been found by this Court to be violative of the Constitution of India."

It is imperative to note that not only did the Supreme Court champion the civil liberties in the digital realm as enshrined in the Constitution, but also proactively placed onus on the entire citizenry to be informed and vigilant. Similarly, courts are not shying away from using technology equipment as an aid to protect human rights. In *Paramvir Singh Saini v Baljit Singh & Ors*[9], the Supreme Court directed installation of CCTV cameras across all police stations in India to purchase, install, maintain and preserve CCTV footage, so as to check for any human rights violation that may have occurred inside the police stations but went unreported. A part of the order is reproduced below:

16. The State and Union Territory Governments should ensure that CCTV cameras are installed in each and every Police Station functioning in the respective State and/or Union Territory. Further, in order to ensure that no part of a Police Station is left uncovered, it is imperative to ensure that CCTV cameras are installed at all entry and exit points; main gate of the police station; all lock-ups; all corridors; lobby/the reception area; all verandas/outhouses, Inspector's room; Sub-Inspector's room; areas outside the lock-up room; station hall; in front of

the police station compound; outside (not inside) washrooms/ toilets; Duty Officer's room; back part of the police station etc.

17. *CCTV systems that have to be installed must be equipped with night vision and must necessarily consist of audio as well as video footage. In areas in which there is either no electricity and/or internet, it shall be the duty of the States/Union Territories to provide the same as expeditiously as possible using any mode of providing electricity, including solar/wind power.*

The aforesaid order(s) are being used as a template by various High Courts[10] and the subordinate courts to further the cause of human rights in India.

DHRs – citizen at the core

It is the core, that is, the citizen, which needs to come to the forefront and seek intervention of the courts whenever it feels violated of constitutional guarantees. The right to privacy emerged from the shadows of *Aadhaar case*.

On 24 August 2017, a Constitutional Bench of nine judges of the Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v UOI*[11] upheld that Privacy is a Fundamental Right, which is entrenched in Article 21 [Right to Life & Liberty]. All the judges expressed their opinions on the subject (running into 574 pages), which are being crystalized herein below:

1. Privacy is one of the most important rights to be protected both against state and non-state actors (body corporates), however it is not an absolute right and is subject to certain reasonable restrictions, which the state is entitled to impose on the basis of social, moral and compelling public interest in accordance with the law.

2. Privacy is not just a common law right, but a fundamental right.

3. The right to privacy is claimed qua the state and non-state actors. Recognition and enforcement of claims qua non-state actors may require legislative intervention by the state.

4. A robust privacy regime is necessary to ensure fulfilment of a three-fold requirement. These three requirements apply to all restraints on privacy (not just informational privacy). The first requirement is that there must be a law in existence to justify an encroachment on privacy. Second, the requirement of a need, in terms of a legitimate state aim, ensures that the nature and content of the law, which imposes the restriction falls within the zone of reasonableness, which is a guarantee against arbitrary state action. The pursuit of a legitimate state aim ensures that the law does not suffer from manifest arbitrariness. The third requirement ensures that the means adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law. Hence, the three-fold requirement for a valid law arises out of the mutual inter-dependence between the fundamental guarantees against arbitrariness on the one hand and the protection of life and personal liberty on the other.

5. The balance between data regulation and individual privacy raises complex issues requiring delicate balances to be drawn between the legitimate concerns of the state on the one hand and individual interest in the protection of privacy on the other.

6. Privacy has both positive and negative content. The negative content restrains the state from committing an

intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual.

7. Restrictions of the right to privacy may be justifiable in the following circumstances subject to the principle of proportionality:

   (a) The right to privacy must be considered in relation to its function in society and be balanced against other fundamental rights.

   (b) Legitimate national security interests.

   (c) Public interest including scientific or historical research purposes or statistical purposes.

   (d) The need of the competent authorities for prevention investigation, prosecution of criminal offences including safeguards against threat to public security.

   (e) The unidentifiable data.

8. Data protection rules need to be according to the objectives of the processing. There may, however, be processing, which is compatible for the purposes for which it is initially collected. The state must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed.

9. The Judgment endorsed the principles of consent, choice, purpose, collection, disclosure, retention, proportionality, and legitimacy.

The privacy judgment once again established citizen at "the core" and by establishing the contours in the form of principles, the Supreme Court made it clear that every "byte" of personal data is sacrosanct. This spirit has been exhibited by a group of academicians and researchers who have approached the Supreme

Court in Ram Ramaswamy & Ors. v Union of India[12] and sought restrain over the entirely unguided power exercised by investigative agencies to take control of devices that "contain much if not all of a citizen's personal and professional life, requires to be civilized by way of directives from Supreme Court."

They have prayed for the framing of guidelines to govern investigative agencies in the country with respect to seizure, examination and preservation of personal digital and electronic devices and their contents. Similarly, in Shri Rahul Bajaj v Practo Technologies & Ors.[13], the complaint was filed before the Court of Chief Commissioner for Persons with Disabilities against the private company which has developed an app named "Practo" that provides a platform where medical services are available for anyone who intends to use the app. The complainant, being 100 per cent visually impaired, had alleged that he was unable to effectively access the Practo iOS application due to various accessibility barriers. Further, it was also alleged that the company did not comply with the provisions of Section 46 of the Rights of Persons with Disabilities Act, 2016. The Court made the following observations:

"[The company] shall make necessary modifications within 6 months and not later than 9 months from receiving the copy of this Recommendation-Order, to its app and other Information & Communication Technology platforms to make such platforms accessible for divyangjan. Further this Court recommends that Respondent No. 2, Director General of Health Services, M/o Health & Family Welfare shall fulfill its duty under Rule 15(2) and ensure that the platforms of Respondent No. I are accessible for divyangian."

It is imperative to note that the Indian Government websites and mobile apps must conform to compliance-matrix.[14] There also exist Web Content Accessibility Guidelines 2.0 (WCAG). This is a process of inclusion to make technology work for the people and would bring DHRs closer to reality. Afterall, accessibility is an inalienable right.

Implementation of DHRs – time to sensitize technology

One of key instruments to effectively implement DHRs is to make technology accessible to all. Technology knows no barriers. In fact, barriers are introduced by us. For example, use of Artificial Intelligence has the potential to enable millions enjoy basic civil liberties. We have to just connect the dots across the multiple databases existing in silos to set free those hundreds and thousands, who are still languishing inside the jails for years even after securing bails. A recent order of the Supreme Court[15] says it all: *"At the inception, we flag the issue of under trial prisoners who continue to be in custody despite having been granted benefit of bail on account of their inability to fulfill the conditions of bail. In order to have a realistic estimate of it, each jail authority would be required to convey to the State Government the data in this behalf and the State Government would then have to send it to NALSA[16] so that a scheme can be worked out in this behalf."*

It only shows that we have not yet sensitized the technology to our civil liberties!

References

1 Hultzsch, Eugen (1925), *Inscriptions of Asoka*, Oxford: Clarendon Press.

2 United Nations, "Ensuring the protection of human rights", https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/Digital_Human_Rights_Summary_PDF.pdf.

3 Study of contemporary social problems using digital data.

4 Study of social and cultural dimensions of digital technologies and practices.

5 Enforceable with effect from October 17, 2000.

6 Writ Petition (Crl.) 167/2012.

7 On March 24, 2015.

8 Writ Petition (Crl.) 199/2013. Order dated October 12, 2022.

9 Special Leave Petition (Crl.) 3543 of 2020. Order dated December 2, 2020.

10 *Kaushal v State of Haryana* [CRM-M-43672 of 2021]. Order dated January 7, 2022 [High Court of Punjab & Haryana].

11 *Justice K.S. Puttaswamy (Retd.) v UOI*, Writ Petition No. 494 of 2012, decided on August 25, 2017.

12 Writ Petition (Crl.) No. 138/2021. Presently pending before the court.

13 Case No. 13205/1102/2022, dated August 24, 2022.

14 *See* https://guidelines.india.gov.in/compliance-matrix/.

15 *Sonadhar v The State of Chhattisgarh* [Special Leave Petition (Crl.) No. 529/2021 & SMWP (Crl.) No. 4/2021. Order dated November 29, 2022.

16 National Legal Services Authority.

Building Trust and Confidence in Digital Health

Sangita Reddy

The turn of the century saw technology changing every aspect of our lives. With the increasing democratization of data, the number of people with access to the Internet and using digital technology has seen a huge jump. While the number of people using the Internet globally was only around 413 million in the year 2000[1], today the number of active internet users just in India far surpasses this figure at 692 million and is projected to grow to 900 million by 2025.[2] Healthcare has not been left untouched by the magic of the digital wand and has seen digitization and the Internet driving the evolution of the technology used for treatment and care delivery.

Health 4.0

The Fourth Industrial Revolution or Industry 4.0 has seen convergence between the digital, physical, and biological environments. The concept of Health 4.0 inherits this evolution of technology to not just improve but also trigger a paradigm shift in healthcare delivery. Digital health is a very important aspect of this along with the application of artificial intelligence, data mining, machine learning, augmented and virtual reality and the internet of Medical Technologies. While automation has been predicted to lead to a reduction in jobs in the manufacturing and related industries, health-related fields stand apart with an increase in employment[3] that makes healthcare delivery accessible

and omnipresent with a strong focus on clinical quality, patient safety and extremely delightful clinical outcomes.

The changing world of digital health

The slow and steady pace of growth in digital health in the years prior to the pandemic saw a major boost over the last two years as the world fought the COVID-19 pandemic. Today, we are witnessing a transformation to a new "digital normal" that is driven by anywhere-anytime access to healthcare through telemedicine, and artificial intelligence enabling digital therapeutics and personalized medicine that underscore the quality and high sense of the reliability of service. This in short is High Tech-enabled High Touch that brings the confluence of the art and science of medicine at accessibility levels that are 24x7. Technology has the advantage of creating a healthcare ecosystem that is sustainable and scalable.

The disruption induced by technology is an opportunity to improve health systems, making them more affordable, efficient, strongly aligned to quality outcomes and more easily scalable. Technology is making healthcare better, safer, reliable and more efficient.

Digital health was an important part of the global response to the COVID-19 pandemic with symptoms and contact tracing apps helping understand the progression of the pandemic and to devise the appropriate response. These provide insights into the many symptoms associated with COVID-19 facilitating a response to any flare-up of infections, all in near real-time. This demonstrated that digital health was capable of delivering solutions at scale with exceptional accuracy and precision.

The gamut of digital health extends far beyond telemedicine. By way of example, digitally enabled risk scores are helping identify individuals and population groups at a higher risk for certain health conditions at an early stage. These enable effective

early intervention strategies, which could be as simple as diet and lifestyle modifications for the early onset of any disease or to open up a horizon of clinical treatment plans that not just reverse the condition but also ensure the quality of life does not degrade in the future.

The integration of AI and ML technologies leveraging Big Data is leading to personalized medicine in clinical practice with AI-enabled clinical modules guiding the decision of the most suitable treatment plan. Smart wearables with data analytics promote healthy actions through real-time feedback from a voice assistant or a digital health coach. ICUs and telementoring for surgeons are other advantages the world of digital health brings to the healthcare ecosystem.

But while we embrace digital health, it is important to address the challenges in terms of building trust and confidence at the various touchpoints that patients have in their interactions with the healthcare ecosystem. It is only then that we will be able to fully build trust and earn patients' confidence in digital health. We also need to reimagine security as we confront and address critical aspects such as data accuracy, data security and privacy protection.

A global strategy on digital health

In March 2019, the World Health Organization (WHO) launched the consultative process that led to the release of the Global Strategy on Digital Health 2020–2025, which was endorsed by the Seventy-third World Health Assembly. This supports the 2030 Agenda for Sustainable Development that emphasizes the importance of information and communications technology in accelerating human progress and bridging the digital divide.[4]

The Global Strategy recognizes the importance of health data in helping improve the processes and outcomes of health services, building a knowledge base for effective research, and developing and validating AI tools. Setting out a framework for a person-

centric digital health ecosystem, the Global Strategy emphasized the need for encouraging sharing of health data with the patient's consent in a manner that builds trust, protects privacy, secures digital systems, and protects them against inappropriate use.

The importance of trust

Trust is the key to a healthy doctor-patient-health system relationship. Trust is a factor that contributes to successful interactions in many societal institutions, including healthcare. Trust as a factor includes both trust in healthcare providers and trust in the healthcare system as a whole. This trust is fundamentally guided by effective processes that are the DNA of an organization and wholly guided by a functional ethics-based governance system. Such a governance system ensures continuous benchmarking of the process and procedures of the organization against the best in class and regular audits to ensure seamless functioning and consistent sustainability.

Trust has been found to have an impact on treatment outcomes with high levels of trust leading to patients seeking timely medical intervention and adhering to treatment with a beneficial effect on patient safety.[5] It is important to build trust as high levels of trust can develop into positive feedback loops where trust is continually strengthened, while the opposite with low levels of trust has its own risks.

It is trust that leads to a patient opening up and sharing intimate details with a doctor they may have met for the first time. Transferring this interaction to a virtual setting places difficulties in conveying empathy that comes through in a face-to-face consultation. In a virtual setting, interpersonal relationships depend on communication skills of the healthcare providers, affecting patients' perceptions of whether their complaints are being taken seriously or not.

There is no doubt that trust is central to the vision of deriving maximum benefits from digital health to all the sections of our society.

Trust among healthcare recipients

Gaining the trust of patients is fundamental to the successful rollout of digital health. However, as healthcare increasingly integrates digital technology, from promotion to prevention and from diagnosis to treatment, the challenge remains to get patients to trust the system. Among the many factors affecting trust and confidence are questions over safety, efficacy, equity and sustainability. Regular media reports on database hacks, misuse of personal data, and the spread of misinformation are adding to the existing distrust in technology. This is instigating people to question many aspects when it comes to the adoption of digital health.

These include doubts about whether the chatbot that an individual interacts with is optimized to recreate an interaction with a real doctor? Are the claims of the benefits of an AI-based predictive algorithm truly tested? Whether the electronically stored health data is protected from unauthorized access? And is an individual's video and audio data, which is sensitive information, safeguarded from unscrupulous use? Will private information be used by insurance companies to deny coverage?

Digital health generates massive amounts of data and the future will see exponential growth in the volume of data, running into zettabytes or even yottabytes.[6] This will emanate not just from telehealth but also from genome sequencing, imaging, proteomics and other studies of the human body. To deal with this data, transparency and communication must be open along with collaboration between stakeholders across disciplines.

Patients need to be guided to develop trust in the tools to protect private information and work in their best interests. It

is these tools and technologies that can be leveraged to enhance trust by ensuring transparency, ethical practices, and data privacy and security. Organizations must demonstrate beyond doubt the security and privacy measures being deployed and their effectiveness in a consistent, repeatable and pervasive manner. This requires strong process enablement and governance and a high degree of accountability. It necessarily calls for a constructive environment of governing laws that protects the interests of the entire ecosystem, is well balanced for all the stakeholders and is uncompromising on the fundamentals of ethics that healthcare delivery always demands.

Trust among healthcare providers

Trust has to be ubiquitous across all the levels of the healthcare ecosystem. While building trust and confidence in digital health among patients is important, it is also critical that the healthcare providers who deliver care also have an equal amount of trust in the capabilities of digital health to augment their own expertise.

Trust builds up over time and takes immense effort to maintain. Healthcare providers need to be communicated about the benefits of digital health. An example is its use in Robotics and Augmented Reality and Virtual Reality, which could help skill development. Digital health will also support our efforts to promote Heal in India and Heal by India with digital health platforms driving robust growth in Medical Value Travel.

Need for regulatory and legal clarity

A case from 2017 is indicative of the problems that could occur with patient data. A collaboration of National Health Service (NHS) of the United Kingdom with Google's DeepMind gave access to 1.6 identifiable million patient records for developing applications that would support patients with kidney disease. An investigation later found that the agreement between NHS and DeepMind was not legally sound.[7]

This case highlights the need for clear guidance from governments over regulations pertaining to data sharing as well as research in and testing of new technologies so that there is no ambiguity in the derivation of the public good. Norms and standards that ensure a balance between safety and development are important to ensure that technological development takes place in an open and transparent fashion.

There should be a legal and ethical framework that assures patient privacy, data security, appropriate use of health data, and protection of intellectual property rights. Governance has to be strengthened especially in the area of the use of health data in technologies such as artificial intelligence and big data analytics.

Winning trust

Surveys have shown that just 20 per cent of patients express high confidence in their data being used responsibly and in their best interest.[8] Hence, transparent communication on how the data is intended to be used, taking consent, and handling patient data responsibly and in the patient's best interest is important.

To build trust, we must work to create an experience for the patient that demonstrates how digital health and the use of their data enhances the care that is delivered to them. Personalization helps create customized experiences for each patient and increases trust by showing that the digital health platform looks at each user as a unique patient. It will result in effective and near-real-time responses to health events through medical devices and digital tools backed by IoT and 5G.

Feedback is an important component of the process of building trust among patients. A feedback loop allows patients to connect with the digital health system and remain invested in the outcomes.

Trust through hybrid care – the human touch

Even with the most advanced technology being used in healthcare delivery, health remains a deeply personal human experience. Digital health necessarily needs to have elements that bring human experience to the digital space for patients to develop trust and confidence in the use of digital platforms. It is here that the human touch works to promote trust in care delivery by the digital health ecosystem.

For doctors and nurses delivering care, the integration of digital and human aspects allows nurses and practitioners to focus on the "human" elements of care while allowing digital technology to deal with routine administrative work. This helps in giving patients the confidence that their care is being done in a meaningful way. It gives them the confidence that digital health will be able to see them through any challenges.

When patients develop trust and confidence in digital health, it also gives them the resources to take charge of their health. It will ensure that the patient is integral to the digital health ecosystem and give patients the autonomy with the opportunity to participate in their own treatment. This will certainly be the ultimate measure of their trust and confidence in digital health.

References

1 Max Roser, Hannah Ritchie and Esteban Ortiz-Ospina, "Internet", https://ourworldindata.org/internet.

2 Staff, "India to have around 900 million internet users by 2025: Report", *Mint*, 29 July 2022, https://www.livemint.com/news/india-to-have-around-900-million-internet-users-by-2025-report-11659063114684.html.

3 Juliano Marcal Lopes, Patrícia Marrone, Sergio Luiz Pereira and Eduardo Mario Dias, "Health 4.0: Challenges for an Orderly and Inclusive Innovation [Commentary]," in IEEE Technology and Society Magazine, vol. 38, no. 3, pp. 17-19, Sept. 2019, doi: 10.1109/MTS.2019.2930265.

4 WHO, "Global strategy on digital health 2020-2025", World Health Organization, 2021, https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf.

5 Sara Belfrage, Gert Helgesson and Niels Lynøe, "Trust and digital privacy in healthcare: a cross-sectional descriptive study of trust and attitudes towards uses of electronic health data among the general public in Sweden", in *BMC Med Ethics* 23, 19, 2022, doi: 10.1186/s12910-022-00758-z.

6 Afua Adjekum, Marcello Ienca and Effy Vayena, "What Is Trust? Ethics and Risk Governance in Precision Medicine and Predictive Analytics", in *OMICS: A Journal of Integrative Biology*, December 2017, pp. 704-710, doi: 10.1089/omi.2017.0156.

7 Alex Hern, "Google DeepMind 1.6m patient record deal 'inappropriate'", *The Guardian*, 16 May 2017, https://www.theguardian.com/technology/2017/may/16/google-deepmind-16m-patient-record-deal-inappropriate-data-guardian-royal-free.

8 Anonymous, n.d., "How Digital Health Can Improve Patient Trust", Medisafe, https://www.medisafe.com/how-digital-health-can-improve-patient-trust/.

Challenges of Cyberspace Diplomacy

Syed Akbaruddin

Cyberspace quintessentially transcends boundaries in scope. It epitomizes seamless connectivity across boundaries and has become intrinsic to communication, commerce, trade, economic development, research, knowledge, and social interlinkages. The burgeoning role of cyberspace in our day-to-day lives is widely acknowledged. A highly regarded study has projected that the global Internet traffic in 2022 will exceed all such traffic from inception in 1984 to 2016.[1] Cyberspace is integral to all fast-evolving digital technologies. Data analytics, artificial intelligence (AI), blockchain, cloud computing, and other Internet-based services depend heavily on cyber-enabled connectivity. These services, in turn, have considerable potential to shape our collective destinies.

Notwithstanding its growing centrality and significance, cyberspace still has a nebulous diplomatic status. It is not like "outer space," described as "the province of all mankind" in the Outer Space Treaty.[2] Nor is it like the "area" of the seabed and ocean floor and subsoil thereof, beyond the limits of national jurisdiction, designated as the "common heritage of mankind" in the United Nations Convention on the Law of the Seas.[3] These natural domains are "global commons." No such global agreement governs the diplomatic understanding of cyberspace.

Cyberspace was born on the initiative of one state – the United States of America. It grew manifoldly and came of age,

while other states largely remained spectators. States, who are usually the primary actors in the diplomatic sphere, have been "latecomers" in joining the cyberspace bandwagon. In the case of other "ungoverned" spaces – such as outer space and the high seas – they were primary actors from very early in the game. The surge of states' interest in cyberspace followed the onset of many other stakeholders, including the academia, research community, and industry, which had the first mover's advantage and distinctive interests before states gained a firm foothold.

Cyberspace governance transitioned from the custodianship of the US government to various multi-stakeholder forums under US tutelage. These platforms include several constituencies – states represented by their governments, business, and civil society. They are distinct from multilateral arrangements where other state representatives are the sole players. For example, matters related to the virtual infrastructure are managed mainly through non-profit groups like the Internet Corporation for Assigned Names and Numbers, which administers IP addresses, autonomous system numbers, domain name system, and protocols (technical standards that enable data transmission on the internet). Such an arrangement provides a peripheral role to states, and same is the case with Regional Internet Registries and the Internet Engineering Task Force – an organization primarily responsible for the development of technical standards for the Internet.

Even the efforts led by the United Nations – quintessentially a multilateral forum – led to the World Summit on the Information Society in 2003 in Geneva and 2005 in Tunis and the subsequent formation of the Internet Governance Forum. All these are multi-stakeholder policy dialogues drawing representation from governments, the private sector, and civil society, including the technical and academic community, through an open and inclusive process. Cyberspace epitomizes the multi-stakeholder model, gaining salience in a world where inter-state cooperation was the dominant mode of international cooperation.

The multi-stakeholder model tends to be seen as more inclusive, providing space for more entities with a stake in the process and decision making than the multilateral model. The multiplicity of stakeholders though does not translate into equality for all the stakeholders. The dominance of non-state actors is quite visible. The cardinal role of industry as the driver of this engine is perceptible. Besides, the active participation of large corporate entities from the Global North and the limited influence of entities of all sizes from the Global South is glaring too.

Since the late 2000s, the digital transformation of societies and their economies has led to the cyber domain impacting states in many more ways. Since cyberspace is critical to the generation, dissemination, collection, and use of data in the present day and age, it has numerous public policy imperatives for the states to consider addressing cyber issues in ways quite different or divergent from the past. They range from economic development objectives to national security and improved commercial services and industrialization to the protection of intellectual property, privacy, and human rights and civil liberties. As the canvas of cyberspace expanded, states have pressed on for more significant role for themselves. It has stemmed mainly from states prioritizing national policy objectives beyond the technical and operational needs of interoperability and connectivity that were predominant earlier.

The rapidly transforming cyber environment is generating demand for governance and state intervention. The ramping up of regulatory capacity and adopting policies on data flows according to governmental priorities in the form of economic, social, political, institutional, and cultural values, has dragged states into new rivalries with geoeconomic and geopolitical overtones. For example, the United States is in favour of "free flow of data and information", with data being controlled by private corporations who gather it. That many of the present-day technology giants are US companies is not without significance in such an approach. China and the Russian Federation advocate the "cyber sovereignty

model" with state in the control of data. The European Union is not aligned with the United States data governance model and provides space for individual choices and some forms of regulation. India is working out a model for digital economic development and data regulation that is likely to be distinctive from the others, aligned with its interests and priorities.

Surprisingly, the fear of a cyber "Pearl Harbour," predicted for long, has not materialized so far. However, ransomware attacks, interference in electoral processes, industrial espionage, threats to critical infrastructure, and efforts at disrupting social order have increased by leaps and bounds. Growing insecurity emanating from the cyberspace has resulted in states exerting greater control over cyber activities to counter malicious actions. State responses take the form of increased data localization initiatives and attempts to moderate online content and stem cyber-enabled influence campaigns. States have progressively moved from the periphery to a more distinctive place, if not to the center stage, in matters relating to cybersecurity. As states' worries grow, they are refining the tools to address security concerns and changing the rules about their use.

Once the roles of states manifested in oversight at the national level, discussions have spawned in multilateral fora. These include the United Nations Commission on Science and Technology for Development; the Office of the United Nations High Commissioner for Human Rights; the United Nations Commission on International Trade Law; the United Nations Educational, Scientific and Cultural Organization; the International Telecommunication Union; the United Nations General Assembly; and the United Nations Security Council. Due to specific national and regional policies, the evolving landscape of the approach to cross-border cyber flows [global cyber affairs/ global governance of cyberspace] is now a patchwork of different national policies, which leads to a fragmented international approach towards various aspects of cyberspace.

The UN Secretary-General has for long tried to facilitate congruence of different approaches. Since 2004, he has appointed experts who function in their individual capacities and submit consensual outcomes on cybersecurity through the Group of Governmental Experts (GGE) process. The UN General Assembly has endorsed a set of voluntary, non-binding, and anodyne international norms based on the recommendations of the GGE. There is now an Open-Ended Working Group pursuing, in an inclusive manner, the development of rules and norms for responsible behaviour of States in the cyberspace.

The UN Secretary-General also appointed a high-level panel on Digital Cooperation headed by Melinda Gates and Jack Ma. The group submitted its report "The Age of Digital Interdependence"[4] in 2019 and made several recommendations to foster greater international cooperation. However, it did not make much headway.

Undaunted by this setback, in September 2021, the UN Secretary-General came up with a report titled "Our Common Agenda".[5] The recommendations included a proposal for a Global Digital Compact to be agreed upon at the Summit of the Future. The deliberations will involve diverse stakeholders such as governments, the private sector (including tech companies), civil society, grass-roots organizations, academia, and individuals, including youth, apart from UN system entities. The long road targets September 2024 as the timeline for the culmination of "A Pact for the Future".[6]

To summarize, despite a lot of diplomatic activism and dialogues of various hues, we are still in the phase of declaratory statements and non-binding resolutions on most cyber issues. The unique nature of the cyber-domain includes "the erosion of distance (oceans no longer provide protection), the speed of interaction (much faster than rockets in space), the low cost (which reduces barriers to entry), and the difficulty of attribution (which

promotes deniability and slows responses),"[7] making a legally binding treaty on cyber security extremely difficult to achieve.

Other factors are now in play too. Owing to differing concerns of states because of diverse priorities based on fairly evolved national approaches and the complexities of the geopolitical dynamics, international cooperation has given way to competition and conflict. Hence, while there is a strong case for a global governance framework that complements other levels of governance for cyber security, in reality, the existing institutional frameworks at the international level are inadequate in addressing the needs of global cyber governance.[8]

Achieving common ground and globally acceptable solutions will not be an easy task. With populism being the primary flavour in many states and anti-globalization and competing vested interests associated with the capture of rents from the use of digital technologies and data gaining momentum, addressing cyber issues appears to be a daunting prospect. These problems are not amenable to merely technical solutions. Nevertheless, if unaddressed, they could lead to the splintering of cyberspace into multiple spheres, spawning a chaotic situation. The value that can accrue from these technologies and the innovative use of the associated data could severely diminish. In addition, substantial harms related to privacy, cybersecurity, and other risks could accrue.

Cyber insecurity is a symptom, not a disease. Beneath it are broader geopolitical and geoeconomic problems that demand a new global institutional framework that all stakeholders can live with. The old models of multi-stakeholder approaches with secondary roles for states will not do. Cyberspace today is not an isolated realm of its own. The return of the role of the state in the digital world needs to be seen as part of a solution rather than being viewed from the traditional prism of being a problem. It can open pathways for multilateral, multi-stakeholder, and multidisciplinary engagement of a different kind at an inclusive platform. Cyber-realism needs the industry and civil society to

understand that the circumstances have changed. Technical and commercially oriented actors have enabled the dramatic growth of cyberspace, but we have moved past that era.

The state, with all its shortcomings, is back in play. It is time for actors from the industry and technology to cede space, albeit carefully. However, there is no guarantee of outcomes except by gradually building up accepted norms and implementing them over time. Public policy choices are never easy. They can at best be sub-optimal. The alternative to accommodating the return of the state with uncertain outcomes is worse. It is a contentious cyberspace that will be a tool of weaponization in everyone's arsenal, where the prospects of digital compacts are not viable, and where any hope of agreeing upon "digital commons" is non-existent. Cyber-realism demands a new accommodation between states, industry, civil society, and also among key states. The old order has ended, and the new one remains in the making, based entirely on the choices we make.

References

1 Michael Conley, "Cisco predicts nearly 5 zettabytes of IP traffic per year by 2022", Network World Asia, 28 November 2018, https://www.networkworld.com/article/3323063/cisco-predicts-nearly-5-zettabytes-of-ip-traffic-per-year-by-2022.html.

2 Article 1 of Treaty on principles governing the activities of states in the exploration and use of outer space, including the moon and other celestial bodies. https://www.unoosa.org/oosa/en/ourwork/spacela/treaties/outerspacetreaty.html.

3 United Nations Convention on the Law of the Sea, https://treaties.un.org/doc/publication/unts/volume%201833/volume-1833-a-31363-english.pdf.

4 UN, "The age of digital interdependence: report of the UN Secretary-General's High-Level Panel on Digital Cooperation", 2019, https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf.

5 UN, "Our Common Agenda: report of the Secretary General", 2021, https://www.un.org/en/content/common-agenda-report/.

6 UN, "Modalities for the Summit of the Future", 2022, https://www.un.org/pga/76/wp-content/uploads/sites/101/2022/09/Summit-of-the-Future-modalities-resolution-Rev-3-silence-proccedure-06092022.pdf.

7 Joseph Nye, "The End of Cyber-Anarchy?", *Foreign Affairs*, Jan-Feb 2022, https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy.

8 UNCTAD, "Digital Economy Report", 2021, https://unctad.org/system/files/official-document/der2021_en.pdf.

Slow Progress on Cyber Norms

Arvind Gupta

The cyberspace underpins every aspect of security and socio-economic development. Regrettably, it is also open to misuse by state as well as non-state actors. Presently, there are few norms of responsible state behaviour prescribed for the cyberspace although the issue has been discussed at the UN for more than two decades.

In the Ukraine war, cyber offensive has come of age. Although, relatively few dramatic attacks on critical infrastructure have been reported, cyber "armies" supported by the states on both sides have reportedly been extremely active. In addition, well known private technology companies have also gotten involved in cyber warfare directly or indirectly. This has raised the question whether such activities by states are in accordance with their responsibilities under international law. The issue of state responsibility in cyberspace has assumed even greater urgency as geopolitical uncertainties deepen.

Background

The concerns about the misuse for Information and Computing Technologies (ICT) began to be raised in the nineties. In 1999, Russia sponsored a resolution (53/70) in the UNGA on the issue of "misuse of information and computing technologies"[1]. Thus began the UN's involvement in cyber issues. It was realized that ICTs were a double-edged sword. On the one hand, they

provided immense benefits, on the other, their misuse posed grave danger to individuals, societies, nations and international security. Particularly worrisome is the potential of misuse of ICTs by states, their proxies and non-state actors. The borderless nature of the cyberspace, the relative anonymity that it provides to the users, makes it a unique domain. As technologies have grown and the cyberspace has expanded, the scope of the misuse of ICTs has also grown exponentially. The destabilizing potential of the ICTs is no less serious than that of the Weapons of Mass Destruction (WMDs). While there are conventions and treaties to contain WMDs and their use, no such multilateral instruments are available to reduce the threat arising from the misuse of ICTs. The cyberspace continues to be disorderly.

In the course of time, the United Nations Secretary General (UNSG) set up a Group of Governmental Experts (UNGGE) to study the issue of the responsible behaviour of state in cyberspace and make suggestions. The first UNGGE was set up in 2004. Since then, the UNGGE process has intensified. So far, six UNGGEs have debated the issue and made certain recommendations. The norms debate has been contentious and quite often the Group of Governmental Experts (GGEs) were unable to produce consensus reports. While they discussed and debated dos and don'ts of state behaviour in cyberspace, technology has leap frogged and given rise to newer concerns regarding the misuse of cyberspace by state and non-state actors.

A key finding of the 2013 UNGGE was that the principles of international law, particularly the UN Charter apply to the cyberspace also. This is an extremely important point as it implies that all countries are obliged to comply with the principles of international law in cyberspace also. No new principles of international law are needed for the cyberspace. Thus, the principles of state sovereignty, non-interference, state responsibility, compliance with human rights, etc. apply to the cyberspace too. However, the vital issue is how to ensure the implementation of such norms in cyberspace given its unique

attributes of borderlessness and lack of attribution. Cyberspace provides relative anonymity and deniability to the actors.

The UNGGEs managed to produce consensus reports only in 2010, 2013, 2015, and 2021. Building on the UNGGE 2013 report, UNGGE (2015) identified eleven non-binding norms of responsible state behaviours. According to these norms, states should not allow their territory to be used for wrongful acts involving ICTs; they should not conduct or knowingly support ICT activities that damage critical infrastructure, and they should take appropriate measures to protect their own critical infrastructure from ICT threats. An important norm recommended by the UNGGE was that states should not harm the information systems of "Authorised Emergency Response Teams" nor use such entities for malicious international activities. The states were also urged to take steps to prevent harmful ICT practices and cooperate to exchange information and assist each other in addressing threats related to ICT.[2]

These norms got the stamp of approval from the UNGA through a consensus resolution (70/237), which stipulated that the state should be guided by the norms recommended by 2015 GGE.[3] The next GGE (2016-17) looked at the implementation aspects of the recommended norms but failed to produce a consensus report.

The GGE process, though important, has also been restrictive. Only a few countries took part in the discussions although the composition was changed from time to time. The experts participated in the discussion in their private capacity although they were backed by their respective governments. The GGE process was marked by acute tensions as the countries took divergent positions driven by their ideologies and national agendas. Several fault lines ran through the GGE discussions. The Russians, Chinese, Cubans wanted the government to have greater control over the cyberspace while the Western countries led by the US, UK, EU and others pushed for an open internet. The integrity of the internet has been hotly debated.

The possibility of its fragmentation is real as states shield their networks from the global network. Several countries, notably China, have isolated their networks from the global internet. The private sector, which owns the bulk of the internet, resents government controls and regulations. The overwhelming preponderance of the Western companies in the underlying hardware of the internet has been a cause of deep concern for many countries as they fear that they can be cut off from the internet on the whims of the West. The problem is that an overwhelming majority of the root servers on which the entire internet depends, are located in the US and a few in other Western countries. This causes disquiet in many countries. These fears have been aggravated by recent developments like the Russia-Ukraine war. Some private entities have come out openly in support of Ukraine in the ongoing Russia-Ukraine war.

One can argue the that private sector has got involved in the war on one side or the other thereby losing the protection civilians are entitled to during wars. Russia and China were also concerned about the internet being used to destabilize their societies in the name of openness. Ironically, it is the US that has accused Russia of interference in the presidential elections and China of stealing sensitive private information and patent information. Cyber security and cyber have become critical issues in US-Russia and US-China relations.

UNGGE and OEWG reports of 2021

In 2019, tensions amongst the contending parties came out in the open. The UN set up a two-track process of discussions. While it continued with the UNGGE process by setting up a new GGE, it also established an Open Ended Working Group (OEWG), a new forum for discussions. Both had a similar mandate but the difference was that the OEWG was an inclusive forum in which every country could participate. The setting up of OEWG was a welcome step. In 2021, the new UNGGE as well as OEWG submitted their much anticipated reports. The UN has also

extended the tenure of the OEWG to 2025. OEWG-2 is in the process of firming up its agenda.

The 2021 UNGGE's report reviewed the existing and emerging threats in cyberspace and recommended that "additional norms" should be developed overtime and binding obligation could be considered in the future. It also sought to deepen the understanding of the eleven voluntarily norms recommended by the UNGGE 2015.

There has been a debate, not fully resolved yet, whether the International Humanitarian Law (IHL) should apply to the cyberspace. Essentially, IHL is embodied in Geneva Conventions and Additional Protocols. It lays down the responsibilities of combatants in a war. At the time of war, combatants are obliged to follow certain norms such as not attacking civilians and civilian infrastructure and treat the prisoners of wars in a humane way. The IHL focuses on proportionality, distinction and humanity. These are sacrosanct principles of warfare that the states are obliged to follow. If not complied with, states and their agents can be hauled up for war crimes.

The UNGGE clarified that International Humanitarian law is applicable only "in [a] situation of armed conflict." This means that civilian websites and portals databases and platforms should not be attacked. But the problem is that in the cyberspace, it is very difficult to distinguish civilians from military targets. The group recommended further studies to understand how international legal principles including the principles of humanity, necessity, proportionality and distinction apply to cyber warfare. The UNGGE also elaborated on Confidence Building Measures (CBMs) and capacity building and suggested deepening of international cooperation and assistance in the area of implementation of national ICT policies.

In international law, the use of force (*Jus ad bellum*) has to be in accordance with certain criteria. Likewise, the conduct of war (*jus in bello*) is also governed by strict rules. These laws were

developed over centuries. New technologies and the emergence of cyberspace as a domain of warfare has changed the way wars are fought. Cyber warfare has been an intense area of study. In 2007, following a barrage of cyber-attacks on public and private utilities in Estonia, NATO established a Cyber Defense Centre of Excellence (CDCOE) in Tallinn to develop cyber defence methodologies and build capacities. In due course, CDCOE set up a group of international experts to study the applicability of international law in the event of cyber war and cyber conflicts. The group of experts, narrowly drawn from some western think tanks and universities, deliberated over the issue and in 2013 produced a document called Tallinn Manual 1.0, which went into details of how international law would apply in the case of a cyber war. They sought to examine the applicability of legal notions like sovereignty, jurisdiction, due diligence, human rights, etc. in the context of their applicability to the cyberspace.

A few years later, in 2017, the expert group produced yet another document, known as the Tallinn Manual 2.0, which looked at the applicability of international law not just during cyber conflicts but also in peacetime. Although produced by a relatively smaller group of international experts, these are two useful documents, which seek to give some precision to the concepts of international law as they apply to the cyber domain. It enumerated ninety-five "black-letter rules" governing cyber conflicts. Tallinn Manual 2.0, broadened the scope and covered harmful cyber operations that are routinely conducted below the threshold of war. Tallinn Manual 2.0 enumerated 154 "rules" that would apply to such cyber operations. The two manuals provide a base for further discussions on the knotty subject of state responsibility in the cyberspace.

OEWG

The Open-Ended Working Group (OEWG) also submitted its report in 2021. It discussed a variety of issues, which have been under discussion for a long time. The recommendations touched upon rules, norms and principles of responsible state behaviours,

applicability of international law to cyberspace, confidence building measures, capacity building, and regular institutional dialogue and multi stakeholder participations. The Chairman of the OEWG also issued a detailed summary. The OEWG report has made only modest progress. It does not seem to break fresh ground. The goal of attaining a peaceful ICT environment is still far away. The question of rules, norms and behaviours is a complex issue with a variety of perspectives of the various stakeholders.

The norms suggested by the UNGGE and OEWG are important but very basic. The implementation of the norms remains a key issue. Further, norms are voluntary in nature. They do not have the status of a binding convention.

Internet governance

Discussions at the UN have been limited to state responsibilities in the cyberspace. The remit of the UNGGE and OEWG has been limited. The reality is that the internet impinges on the fundamentals of governance. Internet governance is a much larger issue as it involves the question of ownership of the internet, the relationship between states and non-state actors, cross border transfer of data, data sovereignty, data privacy, freedom of expression versus disinformation, gender equality, cybercrime, technology neutrality, man and machine interface, and a host of issues impinging on our daily lives. The question of rights and responsibilities goes beyond merely the responsible behaviour of states.

The debate about the role of multiple stakeholders in internet governance has sharpened over the years. States are not the only stakeholders in the internet. Non-government stakeholders have also been clamouring for a greater role in the shaping up of internet governance. The UNGGE process has a limited mandate of ensuring responsible behaviour by states only. Internet governance issues are much broader but they do impinge upon state behaviour.

Adding to the layer of complexity in the cyberspace is the role of big technology companies. Their influence on internet governance is huge as they control standards, software and hardware. Software companies, by designing specific softwares, set the direction of future developments in the internet. Ordinary users have no control over the functioning of the big tech companies. Consumer behaviour is influenced by the tech companies in subtle and not so subtle ways. They are compelled to accept what is offered to them in the form of products and services. The privacy of the consumer is often compromised as they share personal data with these companies.

The tension between governments and tech companies is palpable and often boils over into mutual recriminations and disputes, court cases and fines. Tech companies and platforms have clashed with governments repeatedly over a variety of issues. Artificial intelligence and machine learning algorithms also introduce biases that undermine sovereignty as well as human rights. The safety and security of supply chains is equally important. Technology is not neutral. It can undermine democracy. It can reduce the big tech companies and make them reluctant to subject themselves to national and international regulation, supervision and control.

Some of these companies, for instance Microsoft, have emphasized the need for closer participation of private sector in developing norms and underlined the responsibility of global IT providers to enhance consumer trust by protecting their interest. Microsoft, for instance, has argued "…companies must be clear that they will neither permit backdoors in products nor withhold patches, either of which would leave technology users exposed. They will also have to address attacks, whatever their source, to protect customers."[4] This is a positive attitude but how many companies can be trusted? In the recent years, several Chinese ICT companies have been banned by different countries because they cannot be trusted.

Cyber norms have received the attention of diverse groups besides the UNGGE and OEWG. For instance, in 2018, President Macron, speaking at the meeting of Internet Governance Forum supported the Paris Call, which enumerates nine principles for enhancing trust and ensuring a secure cyberspace.[5] Presently, Paris Call is supported by 81 states, 36 public authorities, 39 civil society organizations and 706 private companies. The principles are focused on providing safe, secure and stable cyber space, and the prevention of malicious activity in the cyberspace.

The World Summit of Information Society (WSIS) was convened by the UN in 2001. In 2015, a WSIS+10 review was taken up by the General Assembly after the adoption of the Sustainable Development Goals. The Secretary General was mandated to set up a Global Internet Governance Forum to facilitate a multi stakeholder policy dialogue. Internet governance is a broad area covering a wide variety of issues including public policy, technology, best practices, etc. The first meeting of the IGF was held in 2006. The IGF brings together a variety of stakeholders to talk about good policies and practices concerning the internet and internet technologies. The IGF has held many meetings. Thousands of people participated in the meetings.

IGF is not a decision making body but it fosters a common understanding of the emerging challenges and opportunities in the area of internet governance. It also helps promote capacity building and skill developments, which is one of the key norms recommended by the UNGGE. The discussions held at IGF 2021 in Poland covered a large number of themes including economic and social inclusion and human rights, universal access and meaningful connectivity, regulation, environmental sustainability and climate change, inclusive internet ecosystems and digital cooperation, trust, security, and stability.

Cybercrime

Cybercrime is emerging as a major issue in international security. A study estimated that cybercrimes cost the world USD 6 trillion in 2021 and are likely to grow at 15 percent per year to reach USD 10.5 trillion per annum by 2025. The Budapest Convention (2001), promoted by the Council of Europe, is the first multilateral treaty on cybercrime. Although some non-European countries have joined the convention, it has not become universal as several countries have misgivings about some of its provisions, which are considered intrusive and violative of state sovereignty. India has kept away from the Budapest Convention.

It is the duty of every state to deal with the growing menace of cybercrime. Cybercrime cannot be tackled without effective international cooperation. Intelligence sharing, capacity building, Public Private Partnership and agreements on extradition of cyber criminals are critical for effective international cooperation. The eighth UN Congress on the Prevention of Crime and the treatment of offenders (1990) had suggested that the UN Committee on Crime Prevention and Control should develop guidelines and standards for states to deal with computer related crimes. The cooperation amongst Law Enforcement Agency of different countries is critical for dealing with cybercrimes in its various dimensions, namely, investigation, forensic analysis, evidence collection and extradition agreement.

In July 2021, the Russian Federation presented a draft entitled the "United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" to the Chair of the *UN Ad Hoc Committee*, currently formulating a UN treaty on cybercrime. The proposal has been criticized for failing to adopt a "proportional framework needed to capture the inherently complex issues raised by cybercrime."[6]

India has supported the UN initiative to evolve a comprehensive UN convention on cybercrime. Lending its support to the

drafting of an international convention on cybercrime, the Indian government representative said at the UN Ad Hoc committee meeting in February 2022: "an effective convention" would

> foster international cooperation, contribute to Member States' capacity building, integrate with relevant international and regional organizations, include effective response mechanisms for Member States, guide in improvising existing cybercrime procedures, build a common understanding and keep upgrading itself to meet the aspirations of the international community. Towards that end, India is ready to engage constructively in these deliberations.[7]

The way ahead

The cyber threat landscape has changed dramatically over the last few years. With the emergence of new technologies, modes of cyberattacks have expanded. During the Covid pandemic, cyber technologies proved to be a saviour. At the same time, cyber-attacks registered a steep rise. Health systems and facilities, which are now getting rapidly digitalized, have become favourite targets for cyber attackers. The digitalization of economy provides more targets for cyber attackers. Cyber-attacks are now becoming more organized. Criminal gangs operate with impunity in the dark web. It is no wonder that incidents of cybercrime have witnessed an exponential rise.

The ongoing Russia-Ukraine war will provide lessons on how ICT can be used in the time of a war. Presently, the cyber norms debate is progressing in a zig-zag fashion. There is a lot of rhetoric but the actual situation is that cyberspace remains a wild domain. The way forward is to have inclusive discussions between the various stakeholder at different fora, both at the UN and outside it. Public awareness about the nature of the internet should be enhanced. The state should pay greater attention to the protection of the privacy also subjecting the big companies to some standard of behaviour.

References

1 UNGA resolution A/RES/53/70, dated 4 January 1999 on "Developments in the field of information and telecommunications in the context of international security" https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement.

2 UNGA, A/70/174, Norms, rules and principles for the responsible behaviour of States, UN, 22 July 2015. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.

The eleven norms are:

- States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent harmful ICT practices;
- In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;
- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats;
- States to guarantee full respect for human rights, including the right to freedom of expression;
- A State should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure;
- States should take appropriate measures to protect their critical infrastructure from ICT threats;
- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts;

- States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
- States should encourage responsible reporting of ICT vulnerabilities and share associated information;
- States should not conduct or knowingly support activity to harm the information systems of the stacking teams. A State should not use authorized emergency response teams to engage in malicious international activity.

3 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

4 "The case for international cybersecurity norms" https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REY05.

5 https://pariscall.international/en/call, accessed. Briefly, the nine principles of the Paris Call are:

- Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure;
- Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet;
- Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities;
- Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information;
- Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm;
- Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain;
- Support efforts to strengthen advanced cyber hygiene for all actors;

- Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors;

- Promote the widespread acceptance and implementation of international norms of responsible behaviour as well as confidence-building measures in cyberspace.

6 "Russia: Proposed UN Cybercrime Convention must uphold free speech", https://www.article19.org/resources/russia-proposed-un-cybercrime-convention-must-uphold-free-speech/#:~:text=In20July%202021%2C%20the%20Russian,Criminal%20Purposes%20(the%20Proposal).

7 Statement by Joint Secretary (Cyber Diplomacy) at the 1st Session of UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes, February 28, 2022, https://www.mea.gov.in/Speeches-Statements.htm?dtl/34917/Statement_by_Joint_Secretary_Cyber_Diplomacy_at_the_1st_Session_of_UN_Ad_Hoc_Committee_to_Elaborate_a_Comprehensive_International_Convention_on_Counte.

The Way Forward

Digital++ and its contours for the decade ahead is still evolving and new themes, facets and issues will continue to emerge as the academia and industry push the boundaries of digital innovation. Finding direct answers to the number of issues brought to the fore by the contributors is at this point a far cry. However, in our view the following lessons can be drawn from the contributions:

- Unlocking the true potential of digital technologies for India and meeting the ambitious target of a trillion-dollar digital economy rests entirely on the ability of stakeholders to collaborate and drive technology-led innovation across different verticals of the economy and take the benefits to all sections of the society.

- India@75 has a new place in the world order, and its vision and plans for digital-led development over the next 25 years should place citizens at the centre stage. This essentially entails reinforcing trust of the citizens in a safe online experience for them.

- Technology enterprises, including start-ups, should lead the way and design digital products and solutions on the pillars of trust and security. This demands secure-by-design and privacy-by-design ingrained into digital products, services and systems, and the cognitive burden shifts left from user to provider. India specially has an unprecedented opportunity to reinforce its position as a preferred trusted destination with the emerging geopolitical dynamics and "friends-shoring" strategy.

- India's experiences with digital transformation and the models thereof have global applicability. Investing

time and resources to ensure accountability, security and equitable access will make India's models a viable alternative globally.

- Development of standards is one of the prime areas to focus on in Digital++. India's experience with the digital platforms for identity, payments, and healthcare provide both the experience and credentials for constructive engagement at standards-setting bodies to help shape the future of global digital commons.

- Digital technologies continue to change the world and impact our lives for the better, but gearing up to deal with their dark side and the fallouts of undesirable outcomes is equally important. Such developments have the potential to exacerbate the risks of miscalculation and escalation in the cyberspace.

- The shared responsibility of governments, industry and academia does not end with the development of ethical guidelines and strategies for trusted, safe and inclusive use of emerging digital technologies. It rather extends to the implementation of these and integration with business processes and design philosophies. The technology industry will be held to greater scrutiny both by governments and users to build trusted platforms and products, and therefore the companies and their workforce need to rise to meet these expectations.

- Industry and academia should collectively build platforms and fora that facilitate candid discussions over the issues highlighted in the volume, and beyond those, to ensure that Digital++ promotes human-technology symbiosis, and ingrains inclusiveness, fairness, transparency, safety, accountability, and privacy.

- Technology development in the digital space tends to outpace regulation. The traditional approaches to regulate

digital technology and markets may be counterproductive or may stifle innovation. Regulation in Digital++ therefore needs to be agile, with a wide spectrum of techniques available to regulators to manage the risks and disruption.

- The success of new age businesses and ventures in Digital++ would rest to a great extent on certainty in regulatory frameworks. Uncertainly in terms of rules, regulations, and interpretations of emerging digital technologies may drive innovators, and the value they create, to the jurisdictions offering supportive and predictable regulatory environment.
- As states are increasingly resorting to the exercise of cyber option in support of their geopolitical goals, the private sector needs to work much more closely with the government to mitigate threats. Identifying tactics, techniques and procedures would require combining technical expertise with geopolitical analysis.

We strongly believe that open dialogue among stakeholders with diverse interests is vital to effective policymaking, and it is all the more important in the intricate domain of digital. The DSCI team will endeavour to enable discourse and deliberations on the optimal ways to tackle the issues taken up in this volume, with the objective of securing India's digital future. In closing, we are extremely positive of harnessing the potential of digital and that the industry would rise to the challenge of meeting the security and trust expectations of their users.

Contributors

Arundhati Bhattacharya

Chairperson and CEO, Salesforce India

Arundhati Bhattacharya is the Chief Executive Officer at Salesforce India. In this role, her focus is on expanding Salesforce reach/footprint in the local market and strengthening the India story; she is also responsible for projecting the next wave of growth for Salesforce in India by identifying key focus areas and building business with key customers, ecosystem partners and the industry.

Prior to Salesforce, Arundhati Bhattacharya was the first woman chairperson at SBI, where she was credited with ushering in the digital transformation era at SBI, which in turn resulted in creating new opportunities for the BFSI sector in India. Under her leadership, SBI went on to be voted as one of India's top 3 best places to work in India.

With 40+ years of rich experience in India's financial sector, working across varied roles and diverse national and international locations, Arundhati has also earned a string of accolades such as "The World's 100 Most Powerful Women" by Forbes, "Top 50 globally most powerful women in business" and "World's 50 Greatest Leaders list" by Fortune to name a few.

Dr Arvind Gupta

Director, Vivekananda International Foundation

Dr Arvind Gupta is the Director of the Vivekananda Foundation, New Delhi. He was the Deputy National Security Adviser and Secretary, National Security Council, Government of India during 2014-17. Earlier, he was Director-General of the Institute for Defence Studies and Analyses, Ministry of Defence, New Delhi during 2012-2014. A former career diplomat, he has served in the Ministry of External Affairs and Indian missions abroad.

He speaks regularly at various Indian universities, military, para-military, police, and diplomatic academies on foreign policy and national security issues. He has guided research students at premier educational institutions. He is a member of the Board of Studies of the School of International Studies at Jawaharlal Nehru University and has honorary academic positions at Punjab University and Andhra University.

Author of five books, his last book *Opportunity for India in a Changing World* was published by KW Publishers Pvt Ltd in 2021. His book *How India Manages Its National Security* was published by Penguin Random House India in 2018. In 2020, Sage India published a coedited (with Anil Wadhwa) volume titled *India's Foreign Policy: Surviving in a Turbulent World*. He also co-edited with Arpita Mitra, a volume, *Vasudhaiva Kutumbakam: The Relevance of India's Ancient Thinking to Contemporary Strategic Reality*, (Aryan Book International, New Delhi).

Bojana Bellamy

President, Centre for Information Policy Leadership

Bojana is the President of Hunton Andrews Kurth LLP's Centre for Information Policy Leadership (CIPL), a preeminent global privacy and data policy think tank located in Washington, DC, London and Brussels. Bojana works with global business and technology leaders, regulators, policy and law makers to shape global data policy and practice and develop thought leadership and best practices for responsible and trusted use of data in the fourth Industrial Revolution. With more than 25 years of experience and deep knowledge of global data privacy and cybersecurity law, compliance and policy, Bojana has a proven industry record in designing strategy, and building and managing data privacy compliance programs. She was one of the 20 privacy experts to participate in the transatlantic "Privacy Bridge Project" from 2014-2015 that sought to develop practical solutions to bridge the gap between European and US privacy regimes. Bojana was also the recipient of the 2019 International Association of Privacy Professionals' (IAPP) Vanguard Award, which recognizes privacy professionals for outstanding leadership, knowledge and creativity in the field of privacy and data protection.

Currently, Bojana sits on a number of industry and regulatory advisory boards and panels. She was recently selected as a member of the UK Government's International Data Transfers Expert Council and the Global Privacy Assembly Reference Panel. She participates in many industry groups and is a regular speaker at international privacy, data and cybersecurity conferences.

Prior to joining CIPL, Bojana served for 12 years as the Global Director of Data Privacy at Accenture.

Daisy Chittilapilly

President, Cisco India & SAARC

Daisy Chittilapilly is the President of Cisco's India and SAARC theatre. As President, Daisy is responsible for strategy and sales, operations, and investments to drive long-term growth in the region.

With over 25 years of experience in the technology industry, including 18 years of leadership experience at Cisco, Daisy has a proven track record of transforming operations and cultures to drive growth at scale.

Daisy most recently held the position of Managing Director for Cisco's Digital Transformation Office, where she worked with customers to capitalize on opportunities emerging in the digital world. In addition, as the leader of Software & Services Sales, she worked with partners to accelerate Cisco's transition towards software and subscription-based offerings. Previously, she held leadership positions within Cisco's Enterprise & Commercial businesses, Strategy & Operations, and Partner Organization.

Before joining Cisco, Daisy worked with Wipro Limited across multiple sales management roles. She also serves as Co-Chair on the FICCI National Committee for Artificial Intelligence and Digital Transformation and is an advisory board member of the non-profit, Dragonflies Everywhere.

Daisy holds a BTech (College of Engineering, Trivandrum) and holds a Post Graduate Certificate in General Management (XLRI, Jamshedpur). She is passionate about empowering youth to join the technology space and mentoring start-ups to innovate technology solutions for the most urgent social challenges.

R. Jesse McWaters
Senior Vice President, Mastercard

R. Jesse McWaters is a Senior Vice President at Mastercard and a Fellow with the Mastercard Policy Center for the Digital Economy. He leads Mastercard's global public policy strategy for digital issues, advising Mastercard's senior leadership on emerging digital trends and developing thought leadership across a range of issues, including AI, central bank digital currencies, blockchain, and IoT. Previously, Jesse served as Head of Financial Technology and Innovation at the World Economic Forum.

Anand Raghuraman
Director, Mastercard

Anand Raghuraman is a Director at Mastercard, responsible for shaping global public policy and thought leadership at the intersection of geopolitics, trade, and technology. He is also a Fellow with the Mastercard Policy Center for the Digital Economy. Previously, Anand was a Vice President at the international consulting firm, The Asia Group, where he advised multinational technology companies expanding in India and across South Asia.

Rahul Matthan

Partner, Trilegal

Rahul Matthan is a partner with Trilegal and heads its technology, media, and telecommunications practice. He serves on the board of the firm. He is also a fellow with the Takshashila Institution's Technology and Policy Research Program. He advises domestic and international corporations on a wide range of regulatory issues. Matthan has been involved in a number of policy initiatives including assisting the Indian government in preparing the country's privacy law as well as its unique ID law. He was a member of the Reserve Bank of India's Committee on Household Finance and was part of the committee of experts on nonpersonal data regulation.

Shreya Ramann

Consultant, Trilegal

Shreya Ramann is a consultant at Trilegal and works with the technology, media, and telecommunications practice. She has worked with domestic and international clients to provide legal structuring and advisory services across multiple domains including privacy, e-commerce, media, healthcare and payments. She has also advised the government on key policy reforms in relation to personal and non-personal data, telecom, cybersecurity, geospatial data, and intellectual property, among others.

Dr Sangita Reddy

Joint Managing Director,
Apollo Hospitals Enterprise Limited

Dr Sangita Reddy is a Global Healthcare Influencer, Healthcare Technocrat, Social Entrepreneur and Humanitarian. Passionately committed to transforming healthcare system through technological advancements, she is accelerating positive transformation for effective healthcare service delivery. She has been conferred with an Honorary Doctorate by the Macquarie University, Australia, in recognition of her untiring efforts and resolute commitment to bringing transformative changes in healthcare, development of Health IT and championing manifold initiatives both in India and abroad. She is an Honorary Consul of Brazil in Hyderabad, appointed by the Govternment of India.

Dr Sangita Reddy is a member of the World Economic Forum. She was the President of the industry chamber, FICCI for 2019-2020. Reddy has been nominated by the Government of India as a Member of the Technology Development Board, Department of Science and Technology. She is an Executive Member at NASSCOM and was on the Board for Development Institute, USA and GAVI.Org. She was an elected Member of the Steering Committee on Health for the Twelfth Five Year Plan (2012-2017) by the Planning Commission, Government of India. She has been a recipient of numerous prestigious awards for business and leadership.

Steve Ledzian

Vice President, Chief Technology Officer, Asia Pacific & Japan

In his role as Vice President and Chief Technology Officer for Asia Pacific & Japan, Steve Ledzian advises organizations across the region on approaches to implementing modern, mature security postures. He has spent half of his 25-year career in IT focused on cyber security in Asia.

Steve is a prolific public speaker and has delivered keynotes at security events across the APJ region on a broad range of security topics. He specializes in presenting highly technical subject matter in plain language easily understood by nontechnical executives and has been featured as a TEDx speaker.

Prior to FireEye, Steve managed the security sales engineering team in Asia at Cisco Systems. Before relocating to Asia, he worked for Silicon Valley startups for over 10 years.

Steve holds bachelor's and master's degrees in computer science from Rutgers University.

Sunil Gupta

Co-Founder and CEO, QNu Labs

As CEO at QNu, Sunil is responsible for building vision, strategy of the company and create a highly passionate team of "EnterpreNerds". He has vast experience in leading R&D, Product Development, Business Development and Sales functions, playing multitude of roles as CTO, COO and CEO. Sunil Gupta is obsessed with new technologies and has successfully taken products and solutions in several cutting-edge technologies to the market and this passion has led to the data security and privacy company, QNu Labs, the only firm in the country to have successfully developed Quantum cyber-security products. Sunil has been a hardcore sportsperson from his school days and even now finds time to actively engage in multiple sports such as badminton, table tennis and cricket. Sunil holds a B. Tech in Computer Science from NIT-Trichy, Madras University, India.

Syed Akbaruddin

Dean, Kautilya School of Public Policy (former permanent representative of India to the UN)

Syed Akbaruddin is currently Dean of the Kautilya School of Public Policy in Hyderabad. He is a former diplomat who served as India's Permanent Representative to the United Nations and also worked as an international civil servant with the International Atomic Energy Agency.

Team Polygon

Polygon is a decentralized Ethereum scaling platform that enables developers to build scalable user-friendly dApps with low transaction fees without ever sacrificing on security.

Ravikant Agrawal
Vice President of Strategy, Polygon

Sebastian Rodriguez
Product Manager, Polygon ID

Otto Mora
Business Development Americas, Polygon ID

Oleksandr Brezhniev
Technical Leader, Polygon ID

Tom Burt

Corporate Vice President, Customer Security & Trust, Microsoft

Tom leads a cross-disciplinary team that works to improve customer trust in the safety and security of the digital ecosystem by advocating for international law and norms for responsible state behaviour in cyberspace and global cybersecurity policy, partnering with public agencies and private enterprises to disrupt nation-state cyberattacks and support deterrence efforts, and combatting cybercrime.

Vakul Sharma

Managing Partner, Vakul Corporate Advisory

Vakul Sharma is the Managing Partner of Vakul Corporate Advisory, a Law Firm that primarily deals with Information Technology issues, including Data Protection, Privacy, Surveillance, Encryption, Electronic evidence and Cyber-crimes and Cybersecurity.

He also practices law at the Supreme Court and various high courts. He has regularly been nominated by the Government of India to high powered committees, working groups to draft legislations, subordinate legislations, policy framework, guidelines, etc.

Editors

Rama Vedashree
Former CEO,
Data Security Council of India

With a rich thirty-five plus years in the technology industry, Rama had been the CEO of DSCI for over six years. She has had long stints at NIIT Technologies, and was the Director, Microsoft Global Services, Vice President of GE India and NASSCOM. She has also served on several committees of the Government of India and is currently on the Advisory Board Member at IIT Mumbai Trust Lab.

Dr Munish Sharma

Munish Sharma was a former Senior Consultant with DSCI and part of this initiative. He comes with 11 years of work experience spanning software industry and policy research. He has been a consultant with the Institute for Defence Studies and Analyses and a fellow with the Ministry of External Affairs. His inquisitiveness lies at the intersection of technology and geopolitics. Munish received his doctorate from Jawaharlal Nehru University in 2021. He is a UK Next Generation Scholar and a Chevening Cyber Security Fellow.

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by NASSCOM®, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

For more information, visit www.dsci.in.

Anand Raghuraman
Arundhati Bhattacharya
Arvind Gupta
Bojana Bellamy
Daisy Chittilapilly
R. Jesse McWaters
Rahul Matthan
Sangita Reddy

Shreya Ramann
Steve Ledzian
Sunil Gupta
Syed Akbaruddin
Team Polygon
Tom Burt
Vakul Sharma

DATA SECURITY COUNCIL OF INDIA
4th Floor, NASSCOM Campus, Plot No. 7-10, Sector 126, Noida, UP -201303
+91-120-4990253 info@dsci.in www.dsci.in