INSIGHTS
SYNERGIA FOUNDATION
JUNE 2021 | EDITION III | WEEKLY


# SECURING THE CLOUD

## EXPERT INSIGHTS

**Mary Kavita Dominic**
Policy Research Associate,
Synergia Foundation

**Lt Gen Rajesh Pant**
National Cyber Security
Coordinator, GOI

**Ariel ( Eli ) Levite**
Former Israeli Deputy
National Security Advisor

**Monica Pellerano**
Research Analyst, CEIP

**Matt Carling**
Cyber Security Solutions
Architect, CISCO Systems

**Col KPM Das (Retd)**
National Cyber Security
Officer, CISCO

**Chelsea Smethurst**
Senior Security Strategist,
Microsoft

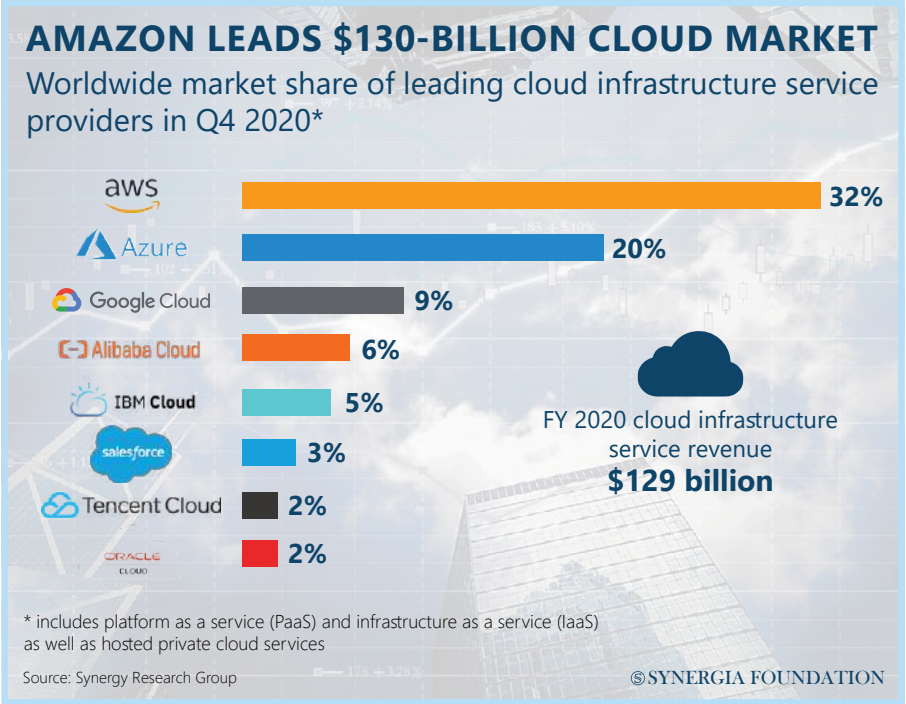
**S Chandrasekhar**
GR. Director Govt Affairs
& Public Policy, Microsoft India

SYNERGIA FOUNDATION

# THE CONCENTRATION CONUNDRUM

It is important to identify and address the systemic risks that arise from a concentration of cloud service providers

**Mary Kavita Dominic,** is a Policy Research Associate with the Synergia Foundation. She has completed her masters in law (BCL) and South Asian Studies (MSc.) from the University of Oxford.




As organisations around the world create and capture more data, there are increasing demands to employ resources provisioned over the Internet.In this veritable milieu, cloud computing has emerged as an attractive solution that facilitates a scalable online environment by offering powerful processing and storage resources. Its optimisation of infrastructure usage has reduced dependence on legacy software and 'on premises' alternatives, thereby lowering capital costs and operational expenses for businesses.

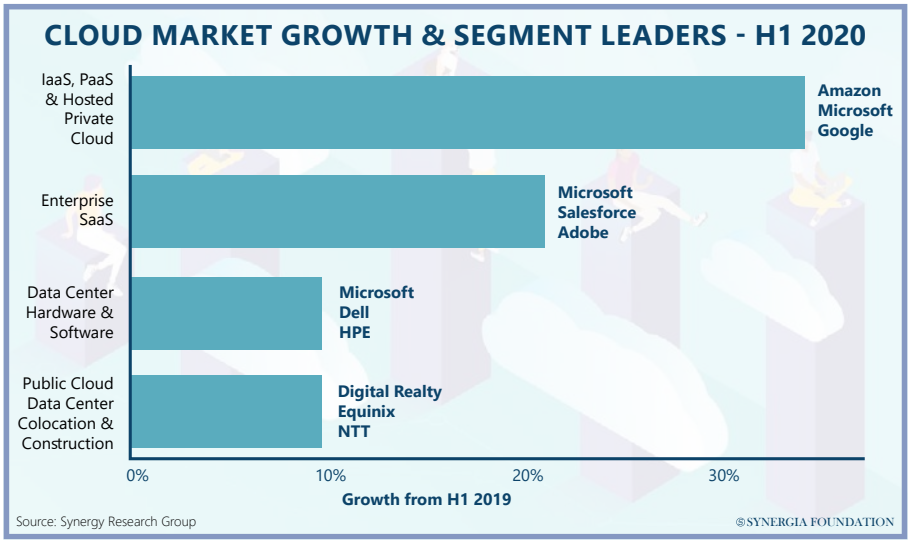
The responsibility for undertaking maintenance and updates has been shifted to the cloud service provider (CSP), with indirect overheads like power consumption by 'on-premises' hardware being eliminated. Rather than maintaining proprietary servers, enterprises can rent additional server space for a few hours at a time. This flexibility and economy of scale have been particularly expedient for small and medium-sized organisations, which lack the capacity to undertake massive investments in IT infrastructure. Moreover, the purported agility and resilience of this networked technology has accelerated the outsourcing of computer systems to cloud-based companies'. At a time when the Covid-19 pandemic has rendered remote working a norm, the cloud has afforded employees the necessary tools to operate outside a quintessential office environment.

## IMPLICATIONS FOR CRITICAL INFRASTRUCTURE

Given the unique benefits of the cloud, many critical infrastructure providers are also contemplating the migration of their workloads. Cloud computing can potentially upgrade the IT infrastructure of governments and bureaucracies, which are particularly notorious for their inefficient services and delayed response times. The scalable platforms of cloud-based companies are also useful for vital sectors like power distribution networks that handle large amounts of data computation and multi-tenant billing. Even the financial services industry is projected to be transformed by cloud computing in the next five years. Against this backdrop, it is increasingly important to configure and manage security postures. The cloud is susceptible to malware infections, data breaches, identity theft and other social engineering tactics, just like any other aspects of cyberspace. There are, however, other pressing concerns that need to be addressed in the short term, namely the risks posed by a concentration of CSPs.

## MARKET DOMINANCE

As the demand for cloud services accelerates at a rapid pace, especially in the aftermath of the Covid-19 pandemic, the markets have become more concentrated in a few key players. In 2020, it was estimated that Amazon, Microsoft, and Google accounted for nearly 71 per cent of the suppliers that offered




cloud infrastructure and platforms as services. In other words, the virtual computing systems of most businesses are predicated on a few CSPs. By heavily investing in security, maintenance as well as data centres around the world, these tech giants have secured the trust of their consumers in a manner that other CSPs struggle to compete with. Apart from possessing the processing power required for advanced analytics, they are often perceived to be superior in managing cybersecurity and technical risk mitigations. This historical path dependence has been supplemented by the network effect among users, which has effectively created an oligopoly of sorts in the cloud services industry.

## RISKS OF CONCENTRATION

Of course, such concentration of market power can have its own advantages. Apart from benefiting from operational and cost efficiencies, CSPs can leverage their technical sophistication, skilled personnel, and security protocols to offer better services for their consumers. There are, however, other risks that accompany this unique combination of ubiquity and concentration. When a single technology vendor has a large concentration of customers relying on its services, a single breach or outage can have a cascading effect. The 2017 server outage of Amazon Web Services, which disrupted a whole range of websites like Quora, Imgur, Trello, Flickr, Glassdoor and the Washington Post, is a case in point.

More recently, incidents like the SolarWinds hack have demonstrated how the compromise of multi-client providers can affect all downstream client-customers. Given that most software companies build their products on top of a larger cloud service provider, they are particularly exposed to such supply chain attacks.

Secondly, risks are also high when a single company depends on the same cloud provider for all its mission-critical tasks. In the absence of a diversified vendor portfolio, organisations can go out of business if their lone supplier is compromised or hacked. In fact, this single point of failure makes them attractive targets for numerous threat actors. While the threshold for hacking the cloud platforms of tech giants may be high, if successful, the payoff is equally rewarding.

Finally, the dominance of a few CSPs may lead to uncompetitive pricing. Owing to their proprietary technical features and market infrastructure capability, they can effectively lock in consumers, significantly impeding the latter's ability to negotiate favourable prices. Unless this power asymmetry between providers and consumers of cloud services is addressed, small-scale businesses may be disincentivised from migrating to secure cloud platforms.

**Tobby Simon**
Founder and President, Synergia Foundation

> Global Governance and fragmentation of the internet are two key challenges that will determine the future of cloud security.

## Assessment

To reduce risks, users of cloud services should aim to diversify their cloud portfolios if the technical environment is conducive. The entire supply chain should be scrutinised to ensure that all providers involved in data processing are complying with minimum security standards. Contingency plans should also be put in place to protect and retrieve data stored on cloud systems.

Meanwhile, governments can assist in the mapping of concentration risks by undertaking initials surveys of CSPs, sub-contractors and services provided under cloud models. This can help to identify 'single point' vulnerabilities that destabilise entire systems, processes, and critical sectors.

Policymakers should consider mechanisms that foster technological innovation and promote healthy competition in the cloud-based environment without compromising security standards. In fact, jurisdictions like the EU have already pledged €10bn for building their own cloud infrastructure as an alternative to U.S.-based providers.

# CLOUD SECURITY-A MACRO VIEW

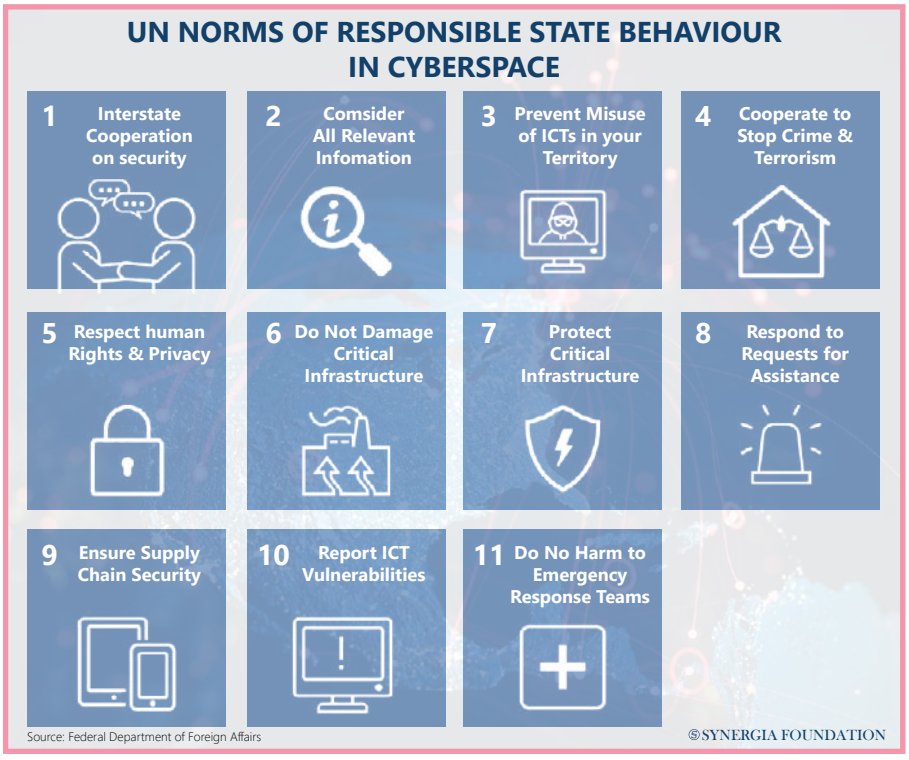
Acknowledging the cloud as 'global commons' is the prerequisite for launching a universally coordinated effort to bolster security


**Lt General (Dr) Rajesh Pant (Retd),** is the National Cyber Security Coordinator at the National Security Council Secretariat of India. He had earlier headed the Army's Cyber Training establishment. He served in the Army Signals Corps for 42 years. Post his retirement, he was the Chairman of Precision Electronics Ltd and also a Governing Council member of IETE (India). This article is based on his views at the 103rd Synergia Forum on the 'Future of Cloud Security'.

Cloud security, at the highest level of governance, must take into account two important considerations.

Firstly, cloud security can be likened to the 'global commons. It affects everyone, sees no borders or boundaries, and requires global solutions. The nature of the cloud is such that, despite the main server located within one's country, both the disaster recovery site and back-ups are likely to be positioned elsewhere.

The vastness of the field is reflected in the spectrum covered by the U.S.'s National Institute of Standards and Technology (NIST) for cloud security. Some of these elements include reference architecture, service orchestration, cloud service management, security



## PARTICIPATING COUNTRIES IN OPERATION TROJAN SHIELD

16 countries participated in a global sting operation using a secure FBI-run messaging network that led to more than 800 suspects arrested and the seizure of more than 32 tons of drugs along with 250 firearms, 55 luxury cars and more than $148 million in cash and cryptocurrencies.


Source: Europol



and privacy aspects, cloud auditor, cloud broker, and cloud carrier. However, there is a silver lining, which foregrounds the second point.

There are positive signs which indicate that the world is willing to collaborate to solve global problems concerning cybersecurity. Recently, the UN member states reached a consensus on the 11 norms for promoting responsible state behaviour in cyberspace. In fact, Trojan Shield is a recent operation undertaken against encrypted communication. The international coalition of law-enforcement agencies behind this, consisting of sixteen countries, led by the U.S. and Australia, hav arrested 800 criminals.

Digital transformation has only sped up matters for cloud security and its aspects. As a result, security architecture has been flipped on its head. However, the industry has been swift in coming up with solutions and addressing identity and access management issues, Work-from-Home, and the shift from a castle-and-moat concept to a distributed architecture.

## KEY ASPECTS

There are four critical areas of cloud security. Firstly, application security covers everything from early design and threat modelling to maintaining and defending the product application. Security must be built into the design process. Since cloud deployments are often greenfield, new opportunities can be created to engage with the security aspects.

Secondly, there is data security and encryption. The Cloud Access Security Broker (CASB) can be considered to monitor data flowing through its system and use appropriate encryption options based on the website model. One can also consider the use of provider-managed encryption and storage options. Thirdly, there is the issue of identity and access management. Here, organisations must develop comprehensive formulae, plans, and processes, for managing identities and authorisations with cloud services. When connecting to external cloud providers, federations must be employed, if possible, to extend the existing identity management. Multi-factor authentication for all external cloud accounts must also be considered, especially for privileged identities. We can also have attribute-based access control over the roll-based access control for cloud computing.

Finally, there is the matter of Security-as-a-Service (SECaaS). These providers offer security capabilities for cloud service, including dedicated SECaaS providers and packaged security features from general cloud computing providers. However, care must be taken to ensure they meet the essential NIST characteristics for cloud computing.

Cloud services imply more than just infrastructure as service, software, or platform as service. For instance, on the Amazon Web Services (AWS) website, all security features are listed, including quantum computing.

## CLOUD VIS-A-VIS TELECOM

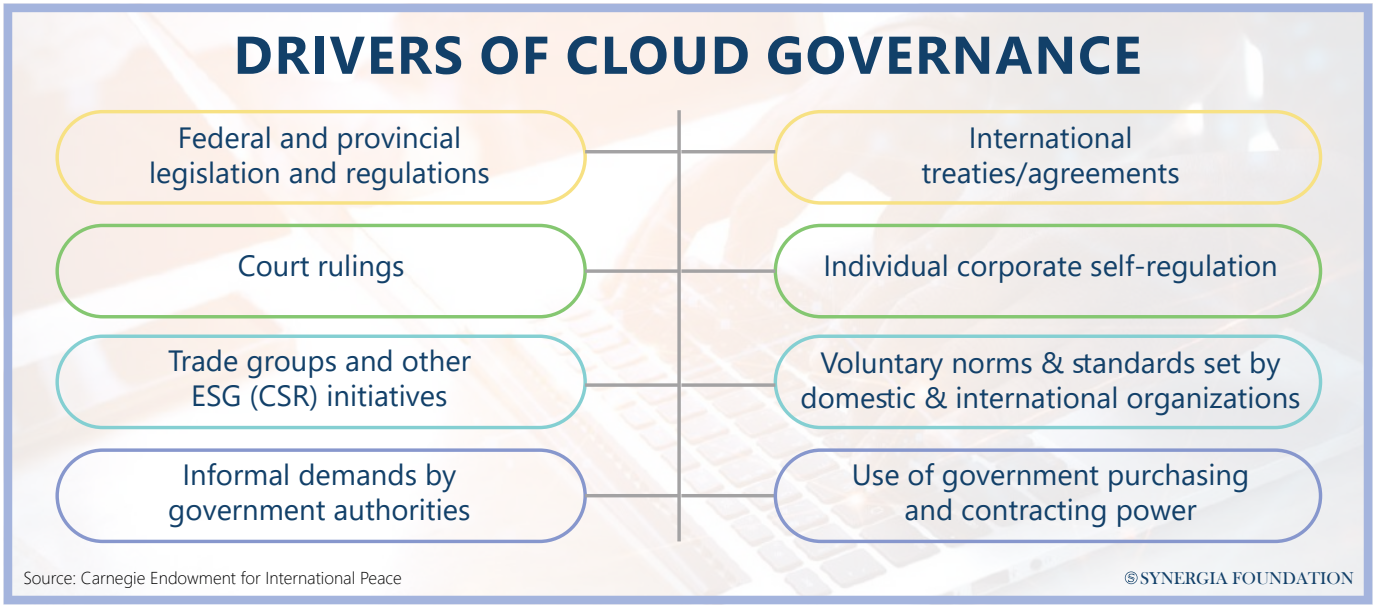
India's telecom infrastructure in the urban areas is in stark contrast to its rural counterparts. The high bandwidth and the wireline options at the backend required by the cloud are unavailable in villages.

While it is true that the cloud has democratised technology by providing an equitable distribution of services to anyone who wishes to make use of it, the question of accessibility precedes it. The government has been tirelessly working towards this infrastructure problem because Optical Fibre Cables have replaced only 25 per cent of our telecom structure.

However, the situation will undoubtedly improve five years down the line, considering the ongoing capacity-building, lessons learnt every day, and good practices that cloud service providers will follow. The newly unveiled Trusted Telecom Portal by the Government of India also promises to usher in a new era of telecom security where every product connected to our networks will be a trusted product.

# FUTURE OF CLOUD: RISKS, SECURITY AND GOVERNANCE

It is imperative to view cloud security as an integrated whole by placing equal emphasis on its non-security aspects




**Ariel (Eli) Levite,** is a non-resident Senior Fellow at the Nuclear Policy Program and Cyber Policy Initiative at the Carnegie Endowment for International Peace (CEIP). He is former Deputy Israeli National Security Advisor for Defense Policy, and also former Head of the Bureau of International Security and Arms Control, Ministry of Defense, Israel. **Monica Pellerano,** is a research analyst at CEIP. This article is based on the presentation given by them at the 103rd Synergia Forum on the 'Future of Cloud Security'.

India is fast emerging as a leading digital power with a fair amount of sophistication, thus making it imperative for Indian experts to engage with their foreign counterparts to shape cloud security. India also happens to be a governance innovator and a huge marketplace for digital services.

## UNDERSTANDING CLOUD

The wide range of characteristics peculiar to the cloud must be fully comprehended before a deeper look is taken into its security environment. The cloud represents a critical part of digital transformation, with its benefits being used universally by individuals, enterprises, and governments. Since there is a wide dependency on cloud services for both essential and non-essential services, its growth and evolution are taking place at a rapid pace. The pandemic has only contributed to this acceleration.

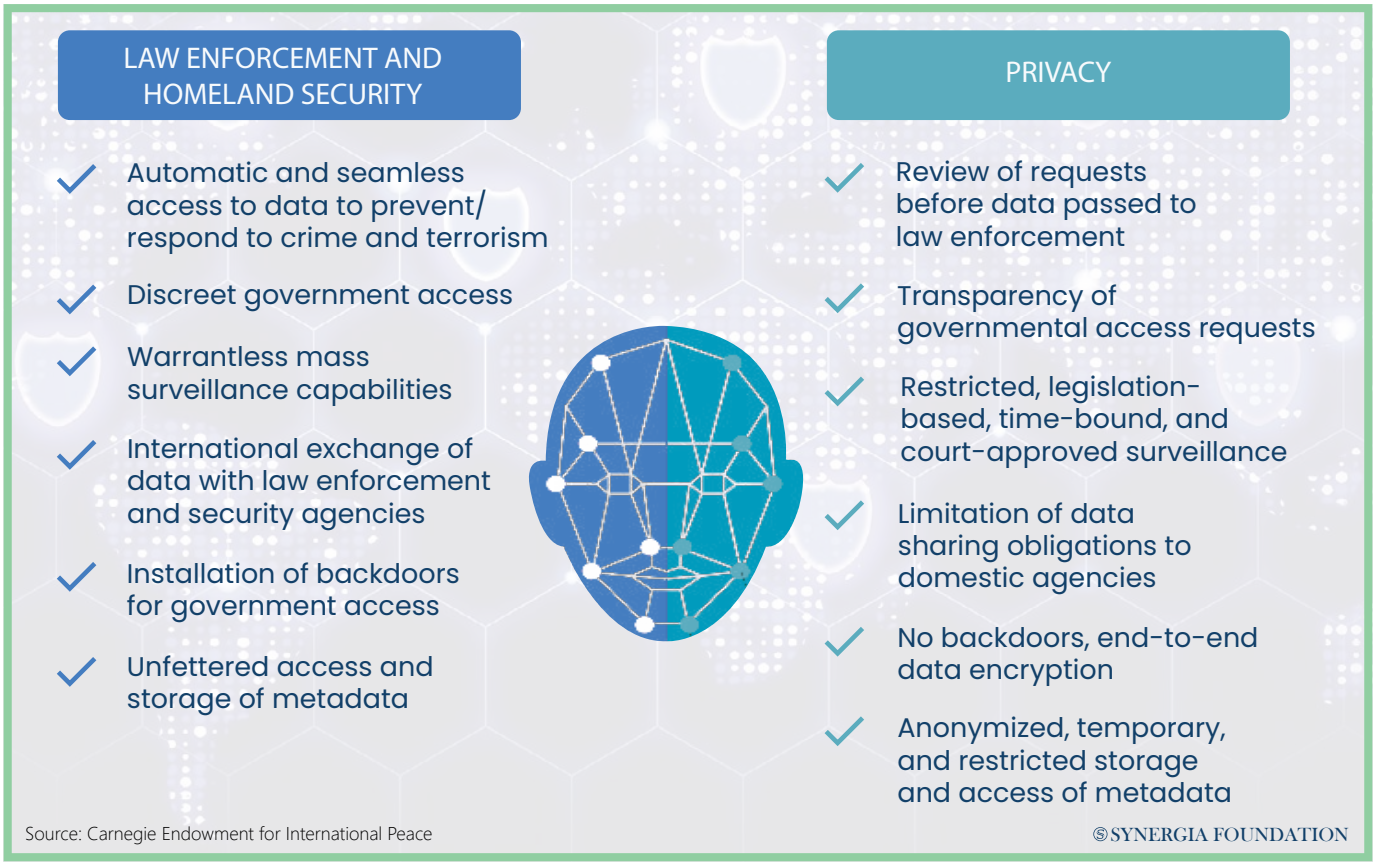
The cloud industry is mostly driven by the private sector, although in some countries, like India, it is the government that provides the requisite impetus as there are huge benefits in terms of security, growth, innovation, and efficiency.

A worrying trait of the cloud is that today the infrastructure is largely concentrated in the hands of a few hyper-scale cloud service providers (CSPs) who are positioned beyond national borders. To tackle this concern, a global solution is necessary.

## GOVERNANCE RISKS

The governance challenges in a cloud environment include direct risks such as severe disruptions in cloud services, either malicious (cyber-attacks) or non-malicious (natural disasters) or indirect risks rooted in dislocation and adjustments made in response to cloud dependency and bundling of services.

Another critical challenge is to develop a global regulatory framework without stifling innovation. This framework should be able to reduce the opaqueness caused by the complexity of the cloud, which makes risk modelling challenging, as also reduce the CSP oligopoly where one is overly dependent on a few providers. Most importantly, the regulations




must devise a comprehensive responsibility framework to deal with both security and resilience to potential risks and attacks.

## FIVE BASKETS OF GOOD GOVERNANCE

The governance issues can best be understood in five 'baskets'.

1) Security and Robustness: This represents the need to safeguard against both malicious and non-malicious triggers. This coupling will seem like a heavy proposition due to various government mandates, geographic and national locations. Cloud security goes much beyond traditional ideas of cybersecurity and is closely tied to various other non-malicious variables. This would mean developing a responsibility matrix and regulatory oversight, coordinating response effectively against incidents, sharing information and inter-governmental intelligence, moderation of cloud misuse, facilitating localisation requirements and cross-border data transfer arrangements etc.

2) Resilience: This is the ability to recover from mainly non-malicious triggers through maintaining data retrievability and back-ups, facilitating portability, interoperability, and multi-cloud arrangements. There must be a degree of assurance that the government steps in and takes over in case of extremities, ensuring provider and insurance carrier solvency and by investigating significant security breaches.

3) Consumer Protection: This basket deals with issues that flow from the power asymmetry between the providers of cloud services and the consumers. It also considers the dynamics when the government is also a consumer of these services. This should be done by preventing bias against consumers in services and application, informing and rewarding users for utilisation of their data, offsetting CSP market concentration and by informing the users of compromises made and thereby working to redress these compromises.

4) Prosperity and Sustainability: The challenges that the cloud can have on national well-being and development can be mitigated by the government. The state has a major role to play by supporting the development, dissemination, and operation of cloud infrastructure. It can promote its growth by extending its services via the cloud, establishing widespread broadband access and creating strict environmental standards on energy efficiency and emissions.

5) Human and Civil rights: The cloud hosts a large amount of private and sensitive data of its users as well as various essential services. To protect these assets, the access to cloud databases containing citizen's identity and vital information should be restricted. As a human right concern, equitable access to the cloud must be mandated while concurrently, cloud services must be curtailed to known human rights abusers.

These baskets are designed to identify key stakeholders' perspectives, expose the deficiency in current arrangements as well as the possible incongruities in the various stakeholder perspectives. All of them intertwine at various points to illustrate concepts like digital sovereignty and how content moderation overlap and entangle, making it necessary that we develop integrated and holistic approaches to cloud security.


## GOVERNANCE TEMPLATES

The Integrated Responsibility Model aims to develop an integrated approach to adjudicate responsibility for cloud security, robustness and resilience between providers, consumers and governments across all sectors and functions.

The prominent challenges this model aims to overcome are the various disagreements between stakeholders on how to share responsibility, the dynamics of the government being both a consumer and provider of cloud or cloud-based services, the mandates and jurisdictional limits which deter trans-national problem-solving mechanisms and the variations in the characteristics of the cloud services and models which hinder uniform solutions.

There is no clear separation in the division of labour and responsibility, which makes developing and maintaining systems of trust difficult.

This model has been developed on the information collected from the survey on the shared responsibility model made available by cloud providers and cloud-based service providers, as well as from the deductions made by the Carnegie Foundation.

The role of governments (including government services such as certification), providers and customers overlap. The responsibilities shared by all are mainly taking steps to manage cyber risks and responding to incidents that threaten security. The responsibilities shared by providers and consumers include complying with norms and standards, facilitating recovery of data and security if compromised, changing management if necessary, as well as identity and access management.

The customer-only responsibilities are relatively less when compared to providers and governments. It is mainly to manage their data efficiently and to properly understand third-party dependencies. The provider-only responsibility is to protect cloud products, be it the physical infrastructure, network, or hard/software. The government's only responsibilities are mainly ensuring international norm-setting, certification, law enforcement, ensuring equitable access to cloud services and intelligence sharing.

The second governance template is to understand the anxieties arising with Cloud Security being deemed Critical Infrastructure (CI). As the world is growing dependant on cloud and cloud-based services, several governments have started thinking about designating cloud security as a critical infrastructure. The challenges here are mainly to understand risk prioritisation, raising many pertinent questions.

What is vital enough to be CI certified? How does one disaggregate between the cloud services and functions? Will this CI certification effectively give the government excessive control over the cloud? Would excessive certification and red taping of the cloud as different entities stifle innovation?

The designation of cloud as CI can only be looked at holistically in intersection with other policy issues such as consumer protection, resilience, prosperity and sustainability and human rights.

## DELINEATION OF RESPONSIBILITY

Therefore, the new regulatory approach is to leave it to the providers and make the government establish performance-based requirements. The government should define and segment high-level surety requirements along three main tangents, which are confidentiality, the type of services offered and sectorial criticality. The

# THE IMPERATIVE OF GLOBAL CLOUD GOVERNANCE


**Samuel Barnett and Mónica Pellerano ,** are research analysts with the Cyber Policy Initiative at the Carnegie Endowment for International Peace.

The development, adoption, and expansion of the cloud has been breath-taking in both pace and scale – representing the apex of a digital transformation that is upending how humans live, work, fight, govern, and do business.

But with the enormous benefits of this technology comes an ever-expanding and ever-more-complicated set of risks and policy challenges, from cascading cyber threats to implications for critical infrastructure and basic government functioning to effects on equitable economic development and human rights. Harnessing and unleashing the potential of the cloud will require its many stakeholders – including policymakers providers, and publics – to recognize these cross-cutting challenges and embrace optimized and coherent solutions. Failure to do so will result in either catastrophic risk – as the cloud is subjected to greater threats from malicious and non-malicious triggers alike – and/or an inevitable wave of counterproductive, unsophisticated, or ill-conceived regulation that dampens the promise that this technology has for global prosperity, interconnectedness, and human flourishing.

Indeed, the cloud's growing ubiquity ought to induce such a broad recognition of its challenges, as well as catalyse a harmonized effort to manage them.

providers, in turn, should commit to honour them, educate the customers on their responsibility, develop an internal system of auditing, provide transparency and so on. The providers can be given incentives to comply, such as insurance coverage, operational licenses etc. In parallel to cloud governance, there should be a process to understand cloud risk management. Cloud risk management can be undertaken by enhancing the understanding of cloud risks and modelling their consequences through an identification of the critical chokepoints that risk security. It is then imperative to diminish the probability of their occurrence and develop a proper responsibility matrix. The prime factor in promoting risk management efforts is to develop a working formula for government and private sector burden-sharing in risk channelling and management. Even high-scale private companies will find it hard to deal with large-scale security attacks if not backed by the government and its resources.

## Expert Q&A

**Q Synergia: Over the coming years, what are the practical roadblocks in evolving and implementing a model for cloud security? Are fragmented laws and country-specific systems going to be a key challenge?**

**A Ariel Levite:** The primary challenge is in the absence of progress in defining expectations. Many cloud providers are amenable to such exercises. They should, therefore, be given the opportunity to engage in a dialogue. Governments have a huge role in specifying their requirements and expectations, which can then act as the basis for reliability or surety standards. Once these have been clearly laid out, the onus is on the providers of business practices and technological development. They need to figure out these practical aspects and make sure they are on the same page. A transparency model can be effective in adjudicating between the two sides.

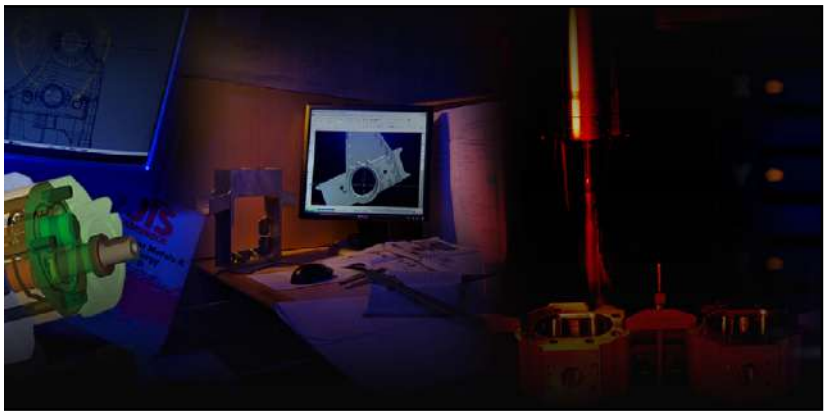
**A Lt. General (Dr) Rajesh Pant (Retd):** Today, the world is faced with technological bipolarity. On one hand, countries like the U.S. have embraced a clean path, clean network, clean undersea cable as well as a coalition for 5G. On the other hand, there is an Eastern lobby that has approached the International Telecommunication Union (ITU) with a new internet protocol and a new initiative for data security.

The world will have to function within this geopolitical reality. Secondly, ransomware is emerging as a serious cyber security problem. In fact, India is one of the worst-affected countries that give pay-outs for ransomware. When one looks at the numbers, the figures have gone up by three times between 2020 and 2021.

When the cloud is involved, the confusion is even more, and cyber insurance alone cannot make up for these losses. Despite the increasing ubiquity of cloud services, cyber laws have not kept up with the rapid proliferation of cloud services. Moreover, establishing a trusted chain of evidence in a court of law is proving to be difficult. Other areas that need more deliberation include the use of Artificial Intelligence as well as the concept of cyber audits in a distributed environment.

DYNAMATIC TECHNOLOGIES LIMITED

# MAKING A **DIFFERENCE** THROUGH **PASSION & TECHNOLOGY**



**HYDRAULICS**

**AEROSPACE**

**AUTOMOTIVE & METALLURGY**

**MEDICAL**

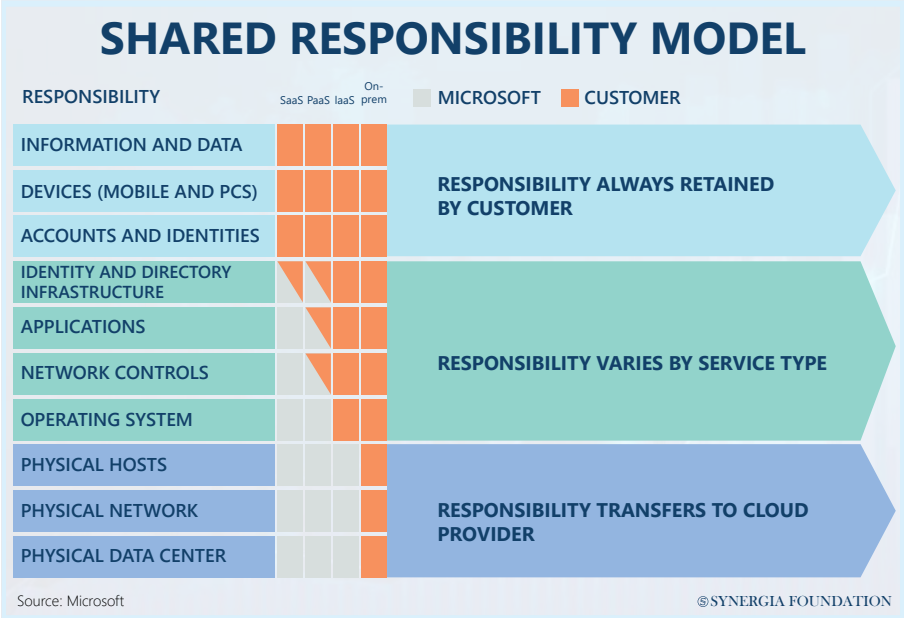
**Dynamatic Technologies Limited**
Dynamatic Park Peenya Bangalore 560058 India
Tel : +91 80 2839 4933/34/35
Email: ajay.g@dynamatics.net

www.dynamatics.com

# AN ALL-PERVASIVE PRESENCE

By allocating shared responsibilities for risk mitigation, the cloud affords a better baseline for security

**Matt Carling,** is a Cyber Security Solutions Architect at Cisco Systems. This article is based on his views at the 103rd Synergia Forum on the 'Future of Cloud Security'.



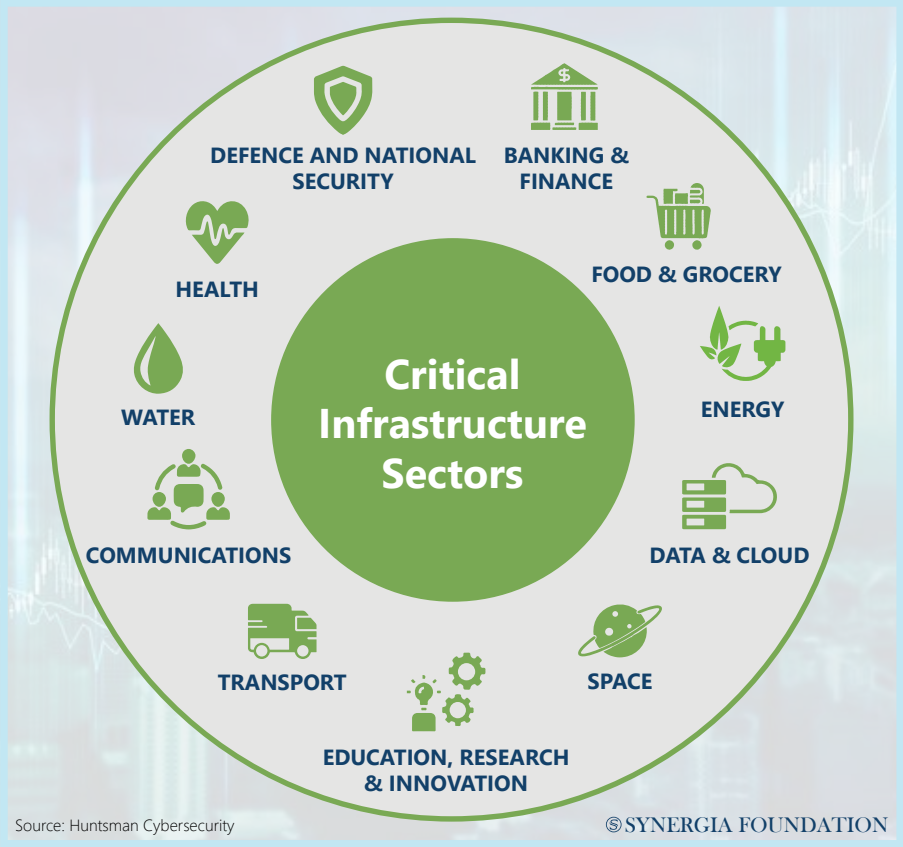

Facilitating conversations on the future of cloud security is exceedingly important. As of today, there is growing awareness of the vital role played by this industry in critical infrastructure as well as businesses. Over the coming years, policy decisions and actions will be driven by better risk sentience.

## CRITICAL INFRASTRUCTURE

While identifying cloud services and platforms that qualify as critical infrastructure, it is important not to cast the net too wide.

Many jurisdictions like Australia, India and the U.S. have similar definitions of critical infrastructure that seek to address any disruption to societal well-being, national security, or the ordinary lives of citizens. Such nuanced characterisations are essential to prevent every cloud application from being designated as 'critical'.

In many cases, cloud providers inherit their criticality from customers. For example, consider the case of clean water providers. These providers must rely on technology like water pumps or filtration systems which, in turn, may use Information Technology (IT) systems or cloud platforms for their




operations.

Therefore, it is possible to trace an element of criticality in the cloud environment from its foundational source.

## RISK ACCOUNTING

On comparing the cloud to private data centres, it could be argued that the technology stack is largely consistent. Both have elements of storage, networking, and computer applications. What is different, however, is their emphasis on models of shared responsibility.

Irrespective of whether one is running the cloud, consuming the cloud, or engaging in 'on-premises' IT, the cloud system provides for better accountability on the part of every stakeholder.

The responsibility to treat risks is not solely vested in the service provider. By highlighting the importance of identity and access control, it accords equal importance to responsibilities that reside with a consumer.

## AVOIDING DUPLICATION

For cloud providers, the recognition of international standards, certifications and audits will be important for scaling up their security frameworks and satisfying the demands of governments and consumers. If every country devises a bespoke certification or security regime, many of them may tend to overlap. From a purely technical control perspective, such duplication of efforts needs to be avoided.

For example, in Australia, lawmakers are currently in the process of updating the Critical Infrastructure Bill.

By virtue of this legislation, the number of critical infrastructure sectors is slated to increase from three to eleven.

In this context, one of the primary challenges for cloud providers will be to ensure that eleven different regulators do not develop their own risk assessment frameworks.

To avoid such duplication, it is important to evaluate the default native infrastructure of cloud providers against existing standards like ISO or SOC 2 audits. If governments and regulators can map the extent to which these frameworks have already addressed some of their security concerns, then future risk assessment protocols and security standards can be formulated accordingly.

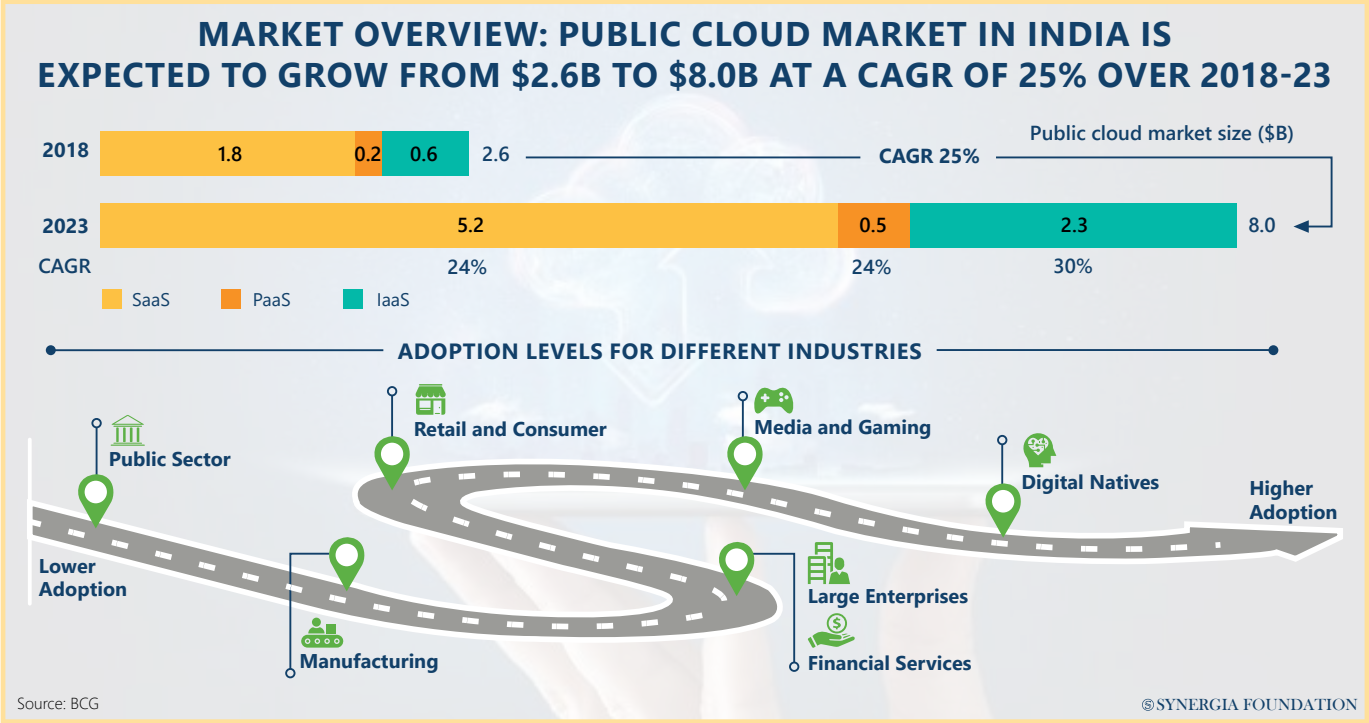
At the end of the day, however, the future of cloud security looks positive, with policy engines and infrastructure codes promising to place the industry in a better spot than before.

| STANDARD | TYPE | STRENGTH | SPONSORING ORGANIZATION |
|---|---|---|---|
| Service Organization Control (SOC) 2 | Audit for outsourced services | Technology neutral | American Institute of CPAs |
| ISO 27001 and 27002 | Traditional security audit | Technology neutral | ISO |
| NIST 800-53 rev. 4 | Federal government audit | Technology neutral | National Institute of Standards and Technology |
| Cloud Security Alliance (CSA) | Cloud-specific audit | Dedicated to cloud security auditing | CSA |
| Payment Card Industry (PCI) Data Security Standard (DSS) | PCI Qualified Security Assessor cloud supplement | Cloud specific and provides guidance | PCI DSS |

Source: IEEE Security & Privacy Magazine
SYNERGIA FOUNDATION

# INDIA: OPPORTUNITIES AND CHALLENGES

India has a huge potential in the cloud market, both as a consumer as well as a service provider and business innovator




**Col KPM Das (Retd),** is the National Cyber Security Officer at CISCO. Prior to tenures in the IT industry, KPM was with the Indian Army for 25 years.

While talking about the 'global commons', it is important to add a more orthogonal perspective, vis-à-vis India and the other members of the emerging countries. In this context, it is necessary to accord due regard to global practices and global standards, on which so much work is being done, albeit in fragments.

Geopolitics governs much of the sovereign pressures today, and in that, there is a tendency for people to look inward and strengthen their defences. But one can do this, even while absorbing global best practices and building on existing standards.

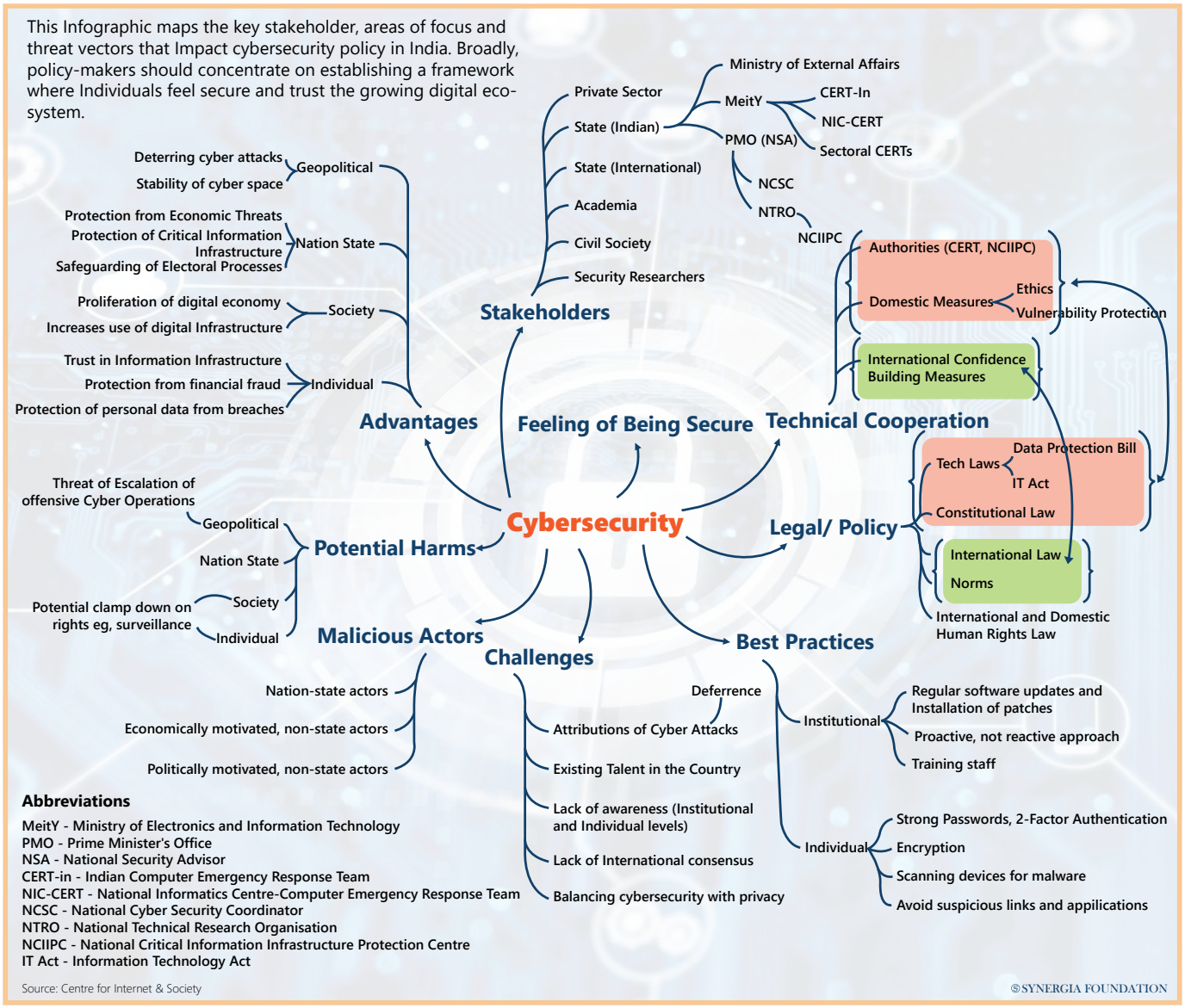
## RISKS & CHALLENGES

Those who grew in the late 1980's client-server times may observe that cloud is actually no different from setting up novel networks. In a way, one must go back to those basics of 'extensibility, scalability, resilience, responsiveness, and the ability to manage'. Moreover, there is a felt need for some degree of control – similar to that of a control plan in some of these networks – and fully appreciate it. While the governance mechanism needs it, it is important to keep in mind the dichotomy here and the need for a fine balance. If the controls move to one end, then all the advantages of being in the cloud are lost, and it raises uncertainty of its security. Because the cloud is not all of it, it eventually delivers services at the endpoints.

The second challenge is in the whole movement from 'quality of service' to 'quality of experience'. It may not matter as much for a citizen in New York or London, but it matters to a villager in India who is going to consume through the Digital India stack application. The goal is to provide the same experience as in Rajeev Chowk in Delhi to a village in Jharkhand. This inequity/equity problem is a clear challenge. For countries like India, Brazil, or South Africa, this 'middle mile' problem is challenging and needs to be addressed.

## COMING TO GRIPS

Given the ambitious objectives set by the Indian government, it is important to highlight the need to improve the talent pool – we are




talking about half a million cyber professionals by the year 2025. The data from CISCO's 'NETACAD' shows that India has the largest and fastest-growing, cyber-hungry demographic in the world. It is an area of concern if India does not get cyber-professionals or the talent aspect in place. It could be compared to the Y2K moment for India – which was a tipping point to take India into hundreds of billions of dollars of IT cells – all over again. The next tipping point for India is to be known as the 'cybersecurity services capital' of the world.

The country needs security operation centres, level one and level two personnel, and cyber analysis. It is also worth mentioning that everything comes with a cost. And there are no better people to understand this than those at the bottom of the pyramid today who wants to get into digital India or the digital world without a laptop, without a server – into the cloud. While India, Brazil, South Africa and Indonesia may be the best countries to come together and develop this model, there is a lot of investment in innovation required. Enabling bottom-up high design security, which is intrinsic to everything, ensures this. So, there will no longer be security engineers, rather just engineers who understand security. This is crucial to address due to the frequency of this issue faced in the market daily. Forty per cent of India's business is potentially waiting to be digitally enabled if security at near-zero cost can be provided.

Lastly, enhancing private-public sector cooperation is equally important. Countries that lead the pack in the maturity graph of cloud services are those that have innovated their private-public working model beyond strategy and policy.

What India lacks is monthly or once-in-three months meetings between teams with senior representation on both sides, putting away their company or department insignias and coming together to develop a collective good for their country.

To this, S Chandrasekhar from Microsoft responded that such private-public partnerships are already happening. He points out that they have collaborated with Data Security Council of India (DSCI) and also with the Office of Dr Pant. Additionally, Microsoft also runs a program called Cyber Siksha aimed at increasing cyber security awareness among government officials. Around 1200 officers have been trained till date.

# LEVERAGING THE CLOUD

As critical infrastructures undergo digital transformation, cloud services will play a vital role in their secure functionality

**Chelsea Smethurst,** is a Senior Security Strategist at Microsoft.


It is important to examine how the cloud can be leveraged to enhance security in sectors like critical infrastructure. This is an important issue, not just from a security point of view, but also from an operational resiliency perspective. Is it possible for critical services like energy or water to derive benefits from a 'global commons' like the cloud?

Irrespective of the nature of critical services or industries, the possibility of arriving at a common security baseline must be explored. Standards like the ISO may serve as valuable inputs in this regard. Once this has been achieved, the nuances can subsequently be worked out.

In any case, the fact that critical entities and infrastructure are undergoing digital transformation is a positive trend. Against this backdrop, the enhancement and encouraging of cloud services will only add further value to this exercise.

## TRANSPARENCY AND VISIBILITY

As critical sectors migrate to the cloud, it is important to identify and assess the interests of policymakers and regulators. Most of them place emphasis on the norms of transparency and visibility, as they wish to be reassured about the security of cloud infrastructures. Apart from scrutinising the security practices and policies that a cloud provider affords to critical infrastructure, they seek to obtain guarantees on the management of resiliency capabilities. Most large-scale services, platform infrastructure and hyperscale providers on the cloud inherit their security and resiliency requirements from customers and clients.

In this context, it might be useful to evaluate whether there are any commonalities across different sectors, which form an overarching umbrella for cloud service providers. Alternately, it must be examined whether it is easier to designate or apply specific standards for individual cloud providers.

## RISK-BASED APPROACH

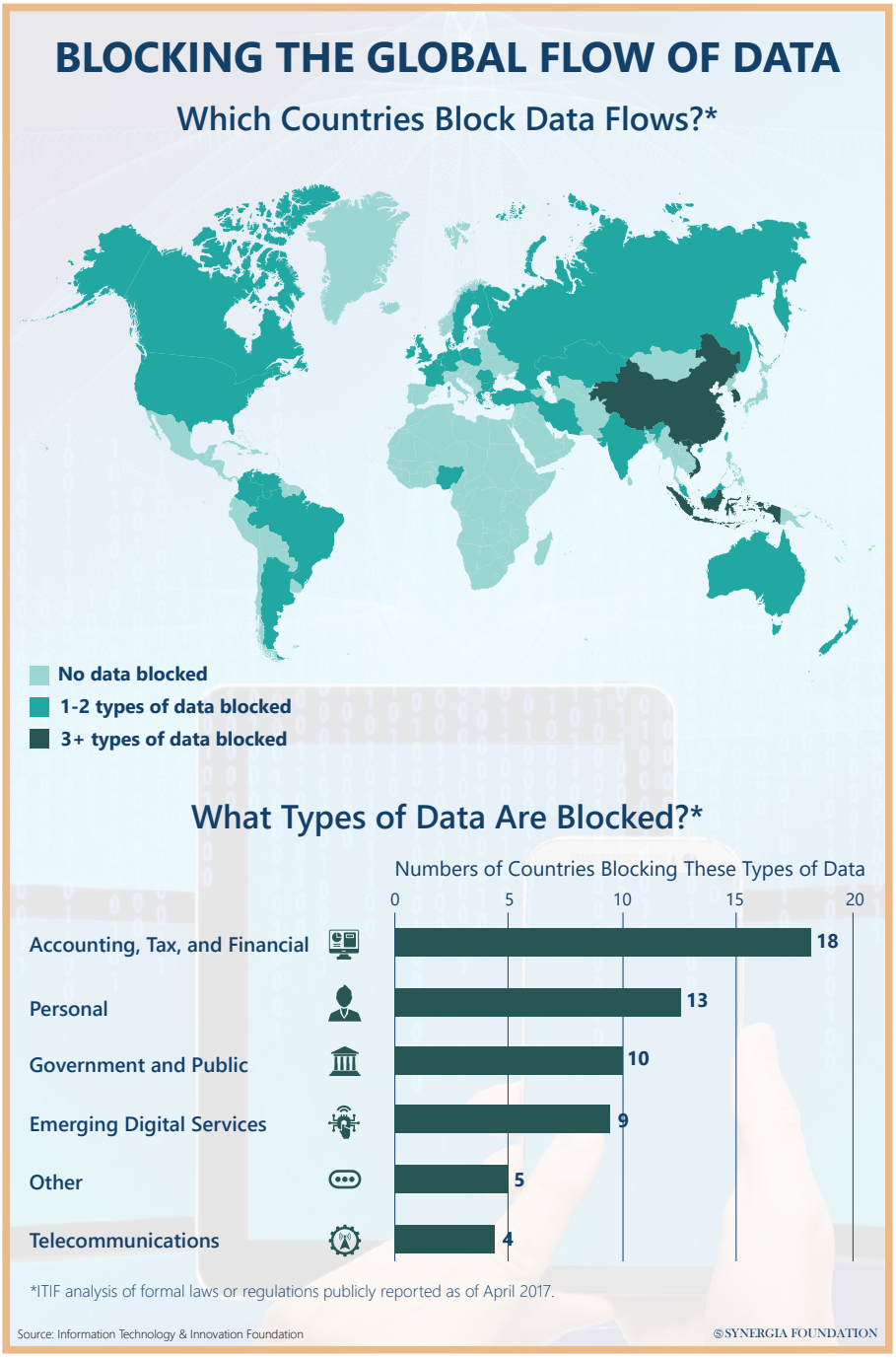
Ultimately, these questions need to be assessed through a risk-based lens. It is important to identify critical services and then apply risk-based assessments to these sectors. Based on the outcomes, one can assess the specific areas that need additional resources or efforts.

Governments and policymakers can play a crucial role in tracking the risk exposure across different critical sectors. As most industries transition to the cloud, it is important to have a risk-based, cross-sectoral view that foresees a spill-over of threats into vital entities. In grappling with these interconnected problems, the importance of public-private partnerships should not be underestimated. The tapping and harnessing of talent in cyber security should also be encouraged. For a company such as Microsoft, it is exceedingly critical to foster talent pools across the world.

# AN EVOLVING GLOBAL FABRIC

Restricting the free flow of data, which is critical to the cloud's functioning, is likely to create a more fragmented system

**S. Chandrasekhar,** is the Group Director of Government Affairs & Public Policy at Microsoft India.




The cloud, as a concept, does not connote server virtualisation alone. Today, there are hyperscale clouds that stretch across the world like a fabric, thereby creating ambient intelligence and ubiquitous computing. However, this fabric and its entire construct are under threat for a number of reasons.

Firstly, there are nationalist forces around the world, which are keen on exercising more control over data and strategic cloud assets. This makes it difficult to manage identity and access issues on a global level.

Secondly, the issue of data protection has become a pressing concern in all parts of the world. As a result, the free flow of data, which is required under the cloud's global framework, has come under challenge. Numerous restrictions are being put up in various jurisdictions under the garb of data protection.

Thirdly, global trends indicate that data has become the 'new oil'. As nation-states become unwilling to allow the free flow of data and exercise more control over it, the concept of a 'ubiquitous cloud' will be affected.

Finally, as the cloud becomes a part of the critical information infrastructure, it will acquire the status of a strategic asset. In such cases, there will be a need to carefully control and protect the same.

In devising these regulatory frameworks, there are a number of questions that need to be addressed. Does the cloud serve as an app that rides on other infrastructure? Alternately, is it a more fundamental service? If it is the former, it would probably lie outside the remit of ordinary telecom regulations.

On the other hand, if it is viewed as critical infrastructure, then the regulator might adopt a different approach.

Over the coming years, therefore, the possibility of fragmentation is likely to increase, even as the cloud grows more ubiquitous. In the context, Ariel E Levite stressed the importance of developing a generic framework, based on international harmonisation, with adjustments being made for local circumstances.

## Expert Q&A

**Q Synergia: When reliable cloud infrastructure is concentrated in a few dominant players like Google, Amazon, and Microsoft, does it create an asymmetric relationship between the consumer and provider of cloud services? What can be done to strengthen the user's hands to demand better security or data protection measures from their cloud providers?**

**A Ariel Levite:** Firstly, it is essential to acknowledge that there are some benefits to concentration. This cannot be denied in any way, shape, or form. Dominant cloud providers are endowed with good resources, technical sophistication, experience as well as global spread. However, other disadvantages need to be addressed. Any service disruption due to technical or human error, natural disasters or foul play can have profound ripple effects. Only recently, there was a service disruption in the entire Eastern Coast of the United States. Therefore, it is crucial to maintain a delicate balance that minimises the risks and maximise the benefits. The real challenge is to facilitate governance by cloud providers that afford a certain level of assurance. Meanwhile, governments also need to possess the technical ability to assess the same. In this regard, Carnegie has suggested a model that minimises the role of the government without compromising the standards they have set for their expectations. There are two ways to achieve this. Firstly, the government can lay down comprehensive standards of reliability, which require cloud platforms to provide assurance on every possible scenario that involves a disruption of service. In other words, cloud providers will have to adhere to a certain level of transparency. Alternately, there can be intermediaries like insurance companies that assist the government by assessing the reliability of cloud platforms. Finally, the government should also look at cloud providers wholistically. For example, if most of them are geographically co-located or use the same type of technology, disruption to one of them can have a cascading effect on others.

## Expert Q&A

**C.S Rao ,** is the Chairman and Co-Founder of QUADGEN Wireless Solutions Inc.


**Q CS Rao: Is there a robust and solid cybersecurity framework in India for critical infrastructures like the power grid, metro rail, transport, and air traffic control for civil aviation?**

**A Lt. General (Dr) Rajesh Pant (Retd):** TIn January 2014, the Indian government had created an organisation called the National Critical Information Infrastructure Protection Centre (NCIIPC), which serves as the nodal agency for protected systems. This includes particular components of critical infrastructure that, if compromised, can have a debilitating effect on national security.
Within this framework, there are several verticals along which the critical sectors have been divided like transportation, energy, banking and financial services.
As far as the power sector is concerned, it has been recently revamped. However, recognising its special importance for all other sectors, the government has constituted sectoral security operation centres (SOCs) along verticals like generation, transmission, and distribution. These SOCS converse with the Computer Emergency Response Team (CERT) and the NCIIPC to better protect this sector.

**Q Synergia: What are the key lessons learnt from previous cyber incidents like the Colonial Pipeline case and the SolarWinds hack?**

**A Chelsea Smethurst:** There is a lot of narrative in the cyber-world about zero-trust architecture. If there is one thing that can be improved upon, it is the deployment of these principles. Better awareness and education about shared responsibilities like identity management, data security and network architecture can also go a long way in enhancing cloud protection.

**A Mónica Pellerano:** There is a need to remove barriers to real-time information sharing between public and private sectors. Secondly, the development of centralised incident response and reporting agencies is essential for coordinating cloud security efforts.

SYNERGIA FOUNDATION

SYNERGIA FOUNDATION

34, Vittal Mallya Road, Bengaluru, Karnataka 560001, India
+91 80 4197 1000
info@synergiagroup.in

@SynergiaFoundation
@SynergiaImpact
www.synergiafoundation.org
www.synergiaconclave.org