Chapter 16
An Evolving Paradigm of Cybersecurity in North Eastern India

Subimal Bhattacharjee

Abstract Over the last two decades, the cyberspace has become an integral part of our lives connecting people from all over the world and creates new models for business and communication. But the process of digitization comes with the rising threat of cyberattacks on our networks. Cyberattacks threaten everything from our critical infrastructures to our personal data and given the hyper speed of digital adoption, this threat is only going to grow over time. The scale and sophistication of the attacks have been increasing with the growing power of state sponsored hacker groups. In this paper, we examine the growing menace of cyberattacks and the cybercrime in the north eastern states of India and look at ways toward creating a strong cybersecurity mechanism that will help the region tackle the growing wave of cyberattacks in the coming times with increased digitization and universal adoption of digital payment systems through strong a public–private partnership and a graded approach to security.

Keywords Cybersecurity · North eastern India · Cybersecurity strategy · Cyberattacks · Cybercrimes

16.1 Introduction

Every day brings new stories about cyberattacks and with far higher frequency than just a couple of years back. But it is not just the frequency that is growing, but also the scale and sophistication of the attacks have evolved and grown. The recent case involving a retired bank officer from Silchar in Assam losing INR 18.93 lakhs (INR 3.14 lakhs from the savings account and INR 15.79 lakhs from fixed deposits) was the biggest cyber fraud in the state of Assam and the north eastern region ever. While we will retake a look at this case later in this paper, what is an established reality is that the hackers were upping the ante in the region with more structured stories and

S. Bhattacharjee (✉)
Independent policy adviser on Cyber Issues & Editorial Board member of the Journal of Cyber Issues, Chatham House, London, UK
e-mail: subimal@subimal.in

S. Anand et al. (eds.), *Sustainable Development Goals in Northeast India*,
Advances in Geographical and Environmental Sciences,
https://doi.org/10.1007/978-981-19-6478-7_16

better coordination. The state of cyber resilience in the state is going to be tested to the highest level of stress.

The north eastern states have been luckier than the rest of the country that the absolute volume of cyberattacks has been far lesser, though that might be attributed to lower levels of digitization in the society. But the region cannot remain immune to the winds of change blowing across cyberspace as hackers across the world are hitting at any target that displays any vulnerability. The level of cyberattacks would go up proportionately in the near future as the region increases its participation in the digital economy unless serious steps are taken to shore up the cybersecurity preparedness of the states.

Before we take a look at the north eastern states of India in a focused manner, it would be pertinent to study the changing landscape of the cybersecurity mechanism in the global context, given that the last year has seen some of the most audacious cyberattacks. The SolarWind attack using vulnerabilities in its ubiquitous and very popular Orion system gained access to both federal and private networks in the US, one of the most advanced countries in digital readiness and usage. The attack was attributed to a Russian hacker group that had tacit backing from Kremlin (Temple-Raston 2021). Even before the dust settled on the hack, the world witnessed a global wave of cyberattacks when 4 zero-day exploits were found in Microsoft Exchange Server. The attack was unusual in its ferocity and has been confidently attributed to a Chinese backed hacker group known as Hafnium, and it is estimated that almost 750,000 servers were affected (Carlson 2021).

While both the above-mentioned hacks were humongous in scale, they had little impact on the common person. But then that was about to change soon with the Colonial Pipeline. Probably the costliest cyberattack in history to date, the incident brought into sharp focus that the severity and scale of cyberattacks were growing every day as critical infrastructures became more decentralized and connected. The attack on 9 May 2021 on the pipeline that catered to 45% of the energy needs of the east coast resulted in the company shutting down its operations as they grappled with the attack, resulting in a loss of almost 2.5 million barrels and pushing up Brent Crude by 1.5% and US futures by 3% (Greenberg 2021). The long lines at the gas stations were the optics that finally shook up the US administration. US President Joe Biden signed an executive order to encourage improvements in digital security standards across the private sector and better equip federal agencies with cybersecurity tools (Presidential Actions 2021).

The FBI has identified the DarkSide Group as the perpetrators, and there is enough circumstantial evidence to link this group to the intelligence community in Kremlin. But that is not enough to take on-ground action against Russia except imposing a few sanctions. As a matter of fact, the United States in April did impose sanctions against Russia for its alleged involvement in the SolarWind attack but nowhere was the response proportional (Helman 2021).

Before we look closer home, let us first delve a bit into the unique challenge we face in securing our networks, the core cybersecurity challenge.

16.2 Cyberattacks and the Evolution of Network Risks

Cyberspace has this unique aspect that the attack vectors and tools are almost the same whether the attack is perpetrated on an individual, an institution, or even a national network. The attackers range from individuals to organized groups and syndicates, non-state actors, and formal militaries of various nations. Even the motive for the attacks differs from thrill-seeking to disrupting networks, causing financial losses, and destroying critical infrastructure functions. The absence of geography in carrying out these attacks gives anonymity to the attackers who today execute their sinister missions involving multiple counties at the same time (Erikson 2008).

Networks have always been attacking vectors. In conventional attacks, these are the roads, railways, naval, and air routes. In the twenty-first century, digital networks are the attack pathways. The trend has been driven by universal digitization leading to global interconnectivity that raises the risks of cyberattacks.

The term "Internet" is a truncation of "internetworking", the original label for how multiple unrelated networks interconnect to form a common whole. This interconnectedness is the inherent strength of the network connecting seven billion people on this planet. It is also the same interconnectedness that creates the vulnerabilities that allow hackers to break the system.

The reason why cybersecurity is such a complex endeavor lies in the nature of the digital landscape, which can be thought of as a digital wild west where a person with a laptop and a data connection can cause more damage than a dozen men with guns. The low entry cost has been the primary reason why the cyber battlefield has seen a constant influx of hackers ready to take down the digital pathways of the world.

Over the last three decades, as the world came to terms with cyber risks, the majority of the hackers focused on some of the other forms of social engineering (phishing) (Aiken 2016) that allowed the hacker to obtain enough information from the target, which could be used to access the targets mail or social media accounts or alternatively target the victims' financial accounts and siphon off funds. The conflict zones saw more incidents of dedicated denial of service (DDoS) which required a large number of hackers working with established tools to ping a server and overwhelm the same. More complex hacking using malware was far less common.

In the past few years, one of the more certain trends emerging is the use of ransomware by hackers. This is connected to the rise of cryptocurrency, allowing the hacker to easily receive the ransom anonymously, a task that would have been difficult a decade ago. As a matter of fact, the majority of illegitimate transactions on the dark Web are powered through crypto transactions. As any law enforcement official will tell you, the toughest bottleneck in receiving ransom is the financial drop-off. Cryptocurrency has effectively solved this problem. Remember that in most data breaches in recent times, like the Mobikwik customer data that ended up on the dark Web, the payment demanded was in bitcoins (Myre 2021).

That does not mean that the less tech-savvy financial frauds have decreased. Rather, these numbers have soared, especially after the global lockdowns were implemented, resulting in the common man spending greater time online, thus giving a

larger window of opportunity to the hackers. It is just that we see far greater degree of sophistication and technical innovation in the present-day attacks. Remember, both the Microsoft Exchange hack and the Solar Wind hack exposed multiple zero-day exploits (SolarWinds Security Advisory 2021).

Most times, the system vulnerability is due to mundane and almost silly reasons like outdated hardware, disgruntled employee, or software that has not been updated. In the case of Lal Path Labs, which found its entire data up for sale on the darknet, it was discovered that the database did not even have the rudimentary protection of a password (Jamie 2020).

The future is going to get even more complex and probably scary. Much has been said and written about the potential impact of technological advancements like 5G, machine learning, AI, quantum computing, and the Internet of things. These are the critical transformative technologies that will determine global prosperity in future. But these technologies are giving sleepless nights to the security community as the world is not yet ready to face these incremental challenges (Castagna 2021).

The fact is that the impact of many of these technologies is not known, and no practical assessment has been done so far. What though is undeniable is that with an unprecedented growth in connected devices, the possibilities of unlawful access would also be an existential threat, and the new tech has the potential to overwhelm the defenses of global network security. Just imagine the Stuxnet or Zeus or CryptoLocker powered by ML and spreading through the IoT nodes to infect every device on the network. That is what a digital apocalypse would look like.

16.3 The Rise of State-Backed Actors

Since the first Gulf War, the world has witnessed the disturbing trend, wherein hacker groups have started receiving state backing. Both China and Russia have encouraged and supported hacker groups and made such groups part of informal state policy to wage asymmetric warfare. A college system with an emphasis on mathematics and computer science means that there is no shortage of recruits.

The transparent method of thwarting cyberattacks has always been raising the cost of penetration. Thus if an organization has solid cyber defenses, the possibility is that a normal hacker would be discouraged from mounting an offensive, given that they are always looking out for low hanging fruits. This does not apply to state-backed hackers who have unlimited funds and sometimes even access to human resources on the ground to take down the defenses of the target.

Most of the major hacks over the last few years can be traced to state-backed hackers who are working toward implementing the states objectives. For example, the DNC hack used to target Hillary Clinton and push Trump's candidacy was supported by a well-backed social media campaign using bots and sock puppets and can be considered as one of the most successful hacks and was pulled off by hackers with the backing of Russian State (Nakashima and Harris 2018).

16.4 Critical Infrastructures in the Cross Hair

When successfully attacked by a hacker, critical infrastructures scattered by geography can have a severe cascading effect on the economy and social fabric. We witnessed a small montage of this with the Colonial Pipeline incident. In November 2020, the grid failure in Mumbai severely disrupted normal life in the city that was still reeling from the effects of the pandemic. The energy minister had stated that the grid failure was due to a cyberattack originating from China, though the Central Government did not comment on the matter. Recorded futures, a US company, had independently corroborated that Chinese malware codes were flowing through the network and had put the Chinese hacker group, Red Echo, behind the intrusion. Observers have opined that the attack if it was so was to send out a message to Government of India after the skirmishes in the Galwan Valley that led to casualties on both sides (The Print Team 2021).

The increase in the digitalization of many critical infrastructures especially in sectors such as oil, gas, and other associated industrial systems is altering the nature of cyber risks in the country. According to the Global Risks Report (2021), cybersecurity failures are among the world-attacks' top mid-term threats. Critical infrastructures are also increasingly shifting to automated control to reduce the human interactions, and control is devolved to centralized computing systems. The growth of interconnected systems and networks makes the system more vulnerable to malicious attacks. Also the use of robotics, sensors, and AI only increases the points of attack.

In February 2021, a hacker made an attempt in Florida to tamper with the chemical levels in the city's drinking water supply (Tidy 2021). The hacker had gained access to the water system with the help of a control system of the plant using a remote access program after then he tried to increase the levels of sodium hydroxide which would have invited a dangerous kind of situation. A supervisor detected the attack monitoring the computer system that reversed the chemical levels as soon the hack was detected, averting a crisis. Today, almost 80% of critical infra companies are privately owned. They are facing intrusion challenges from state-backed actors with infinite resources making the battle terribly skewed.

16.5 The India Story

India has been the second most affected nation by cyberattacks. And the pace of attacks is increasing relentlessly. In the first few months of 2021, India witnessed significant data breaches reported by Air India and Dominos, as both the two companies' databases get posted on the darknet for a price. In another bizarre incident, when Mobikwik, the payment solutions company, had a data breach with customer data, including personal data posted on the darknet,the company brazened it out by not accepting the data breach, despite overwhelming evidence to the contrary.

This was utterly contrary to accepted norms that ensured companies urgently share information of breach with the customers.

In 2020, when India came under a harsh lockdown to contain the spread of COVID-19, our digital networks started seeing an unprecedented surge of attacks, with as many as 1,158,208 attacks recorded, a 300% increase (Nanda 2021). The majority of these attacks can be confidently attributed to hackers operating out of mainland China. The reasons for the growth in cyberattacks could be the increased time spent online by the citizens, making them more vulnerable to cybercriminals and shift to the work from home model that compromised organization security protocols. Most of the attacks took the form of financial fraud, but the latter part of the year saw a growing number of major data breaches and a possible attack on the power grid in Mumbai. One of India's largest data breaches has been the Aadhaar data breach, where 1.1 billion Aadhaar details got leaked through multiple government databases (Sapkale 2019).

Cyberattacks pose a clear and present danger to the nation, both strategically as well as economically. The current digital economy comprises around 14–15% of our country's total economy and is expected to reach close to 20% by the end of 2024. India has more than 120 recognized "data centers", and it is important to mention that although India was one of the first countries to introduce cybersecurity policy in 2013 not much was done for the upgrading of a mature and coordinated cyber and its security approach.

Countries like the United States, United Kingdom, and Singapore have a single organization dealing in cybersecurity, but India on the other hand has 36 central bodies which is headed by ministries deals with cyber issues, and almost all has a different problem solving structure. The state governments have their own Computer Emergency Response Team (CERT). While CERT-IN has responded to cyber threats, it has been late in conducting security checks and has often released advisories once an attack has occurred. In the case of WhatsApp and Pegasus malware, CERT-IN only came in after others had warned of the possibility of individuals being compromised.

There are multiple agencies operating in the national cybersecurity landscape. National Technical Research Organization (NTRO) handles the technical intelligence gathering functions around various sectors including aviation, space and telecom, data management, cybersecurity functions, encryption, and software systems. The National Critical Information Infrastructure Protection Center (NCIIPC) which operates under the NTRO is the national nodal agency for critical information infrastructure protection and is now also covered under the IT Act.

CERT-In is the premier agency that is responsible for the overall cybersecurity mechanism for the nation. This was the agency that had for the first time flagged security concerns for Android Jelly Bean and Kit Kat. Being the nodal agency, CERT-In receives operational intelligence from its situational awareness and threat intelligence systems. Whenever a breach or malware is discovered, the organization issues an advisory to the concerned parties. It also forecasts and alerts of cybersecurity incidents, provides emergency measures for handling cybersecurity incidents, and coordinates cyber incident response activities.

16.6 North Eastern India and Cyber Risk Evaluation

Looking at the complex challenges of cybersecurity and juxtaposing them on the north eastern region presents a unique set of challenges. The NFHS-5 survey has thrown up some very disturbing figures with Meghalaya (42.1%) and Assam (42.3%) at the bottom of the Internet usage chart in the country. Against that Sikkim and Mizoram are at the top of the charts with almost three quarters of the population online (NFHS-5 2021; see also, Chari et al. 2020). But these numbers are slated to rise diametrically. While we will go into the sustainable development program and its focus on cybersecurity a little later, it is essential to mention that of the 17 goals under the SDG program, 13 rely heavily on digitization and delivering governance through cyberspace (The 17 Goals n.d). This alone will probably increase the number of netizens in the north eastern region by 50% in a short space of time.

On the other hand, a quick look at the incidence of cyber frauds gives us a bleak picture. According to the report released by the National Crime Records Bureau (NCRB) in (2018), the rate of cybercrimes in the state of Assam is 6.5 (defined as the number of crime per one hundred thousand population), the third-highest in the list of all states and union territories. The potential explosion in cybercrimes can be well imagined by the fact that even with the second-lowest internet usage across the nation, the state ranks near the top in the rate of cybercrime.

A cybersecurity think tank had conducted several surveys in October 2020 in the state of Assam to figure out the public awareness with respect to cybersecurity and cyberattacks. Similar surveys were conducted in the other neighboring states, including Meghalaya. The data generated was hugely worrying as the majority of the respondents had not filed a police complaint despite facing some form of cyberattack, while only a meager 12% decided to approach the police (The Shillong Times 2021). Interestingly enough, almost 73% of the respondents stated that they faced some form of cyberattack. These are numbers that should give the law enforcement officials sleepless nights as that means the absolute number of cybercrimes happening in the state would be almost five times more than the reported number of cases. The other worrying fact is that the response mechanism has time and again failed the victim.

The recent case reported in Silchar involved an SBI officer losing INR 314,000 to cybercriminals as the officer was asked to pay a sum of INR 11 to bsnl.rechargecube in the process reveals his net banking details (Barakbulletin 2021). The victim was immediately locked out of his account, and despite rushing to the police station immediately to lodge a complaint, INR 3.14 lakhs had been siphoned off to two bank accounts and one PayTM account. The incident was newsworthy primarily because an ex-bank official ended up losing money and that too, a lot of money. But the aftermath of the story is what makes the case really interesting. Three days after the incident, the victim's wife checking on her husband's account realized that despite reporting the hack, the bank (SBI) had not restricted the victims net banking account resulting in an additional INR 1.579 million withdrawn from the fixed deposit accounts in the form of overdraft. This incident illustrates the level of apathy that becomes a boon for the cybercriminals allowing them to flourish. Of course, as per

the RBI circular released in 2017, a bank customer will have zero liability from the moment he has reported the incident, which means the victim in this case will not lose his life's savings, but that does not absolve the bank of gross negligence.

The region has also been witnessing a veritable explosion of QR code frauds. The eastern states in the country are witnessing high levels of online frauds through payment apps and online marketplaces. TrustCheckr, a software company, located in Bengaluru reported that states like West Bengal, Odisha, Bihar, Jammu and Kashmir, Himachal Pradesh along with all the north eastern states are facing frauds in KYC, cash-back offers, false digital wallets, fake-selling, QR codes, UPI phishing, and lottery scams. About 20% of the QR Code scams originate from the north eastern state Assam. In QR code frauds, most fraudsters posed themselves as a defense person selling. TrustCheckr identified over 1 million frauds in B2B and B2C, and the majority of the scams are around fraud in KYC, fraudulent cash-back, digital wallet theft, counterfeit, QR codes, UPI phishing, lottery threats, and money laundering on social networking sites. Most scams involved people purportedly from the armed forces advertising goods on electronic marketplaces. In the last 15 months, about 25% of scams have taken place in the know your customer (KYC) and 20% in QR codes, while the B2B scams were largely accomplished with 25% synthetic identity frauds and 30% fake identities (Sentinel Digital Desk 2021).

All indications are that the north eastern states are fast growing into hotspots for financial cyberattacks, and the law enforcement agencies are in a tizzy trying to figure out a way to control the spread of financial frauds through phishing (Hadnagy 2018). The problem is that cybercriminals are fast reinventing themselves and creating better and better scenarios. For instance, in the middle of the pandemic and the central vaccination drive, people started receiving OTPs ostensibly for vaccine appointments despite not having registered on the COWIN site. While no actual case has been discovered of a data breach or financial loss, the fluidity in creating new plays by the hackers should be of concern.

Apart from the usual financial frauds, some of the other major hacks in the region have been:

1. Manipur Government's Manipur.gov.in was infected with Japanese Keyword Malware as reported on February 2021. It was spamming Japanese scripts on the official site and had the ability to hijack all the key search results of the site.
2. In August 2020, the Nagaland Government's E-commerce Platform "Invest and Development Authority of Nagaland" was also infected by malware, redirecting the visitors to unwanted pop-ups and links. The Nagaland State Biodiversity Board Website was hacked in the same year, and the hackers displayed the Pakistan Army Zindabad message on the page.
3. In 2012, Mizoram Government's site Dpar.Mizoram.gov.in was hacked and defaced.
4. In January and February 2021, a series of Websites of the popular educational institutes in Barak Valley of Assam was hacked.
5. In February 2021, Gauhati University's Website was hacked, and a Valentine Message was displayed on the screen.

Most of these events have not involved deep penetration attacks using ransomwares or malwares and have been reasonably simple from a technological perspective. However, that does not reduce the concerns that are being witnessed in the region due to cyberattacks.

Financial frauds aside, the other area of concern is the spread of online misinformation in a structured fashion, intended to disturb the peace. The north eastern region of India comprising of the eight states—Assam, Nagaland, Manipur, Arunachal Pradesh, Mizoram, Tripura, and Sikkim had its issues around identity and conflicts. Many of the insurgency movements in the region have been resolved recently and as the government wants to bring lasting peace to the region by solving the remaining ones including the Naga insurgency movement, which started in the 1950s. The reasons for the respective conflicts are wide-ranging from separatist movements to inter-community, communal, and inter-ethnic conflicts (Bhattacharyya 2018, 2019; Bhattacharyya and Pulla 2020a, b). To add to the several problems of the region, malicious interference by Chinese backed actors has been constantly targeted at the region, which includes carrying out online misinformation campaigns to disrupt the local peace. The north eastern region of India happens to be one of the most violent regions in the country (Bhattacharyya 2018, 2019; Bhattacharyya and Pulla 2020a, b), and a concerted campaign of misinformation can cause severe repercussions in the region.

The spurt of violence in north eastern states after the Citizenship Amendment Bill was enacted as a law in December 2019 saw a huge misinformation (ANI 2019; Sarma and Bhattacharyya 2021) campaign authored by groups that probably had allegiance to international players, which aimed to exacerbate the situation. The indigenous population of the region were concerned about losing out elements of their culture due to the influx of outsiders while the so-called "outsiders" were worried about the violent ramifications of the new law. The spread of misinformation was targeted at both groups that raised fears and fueled further violence. The situation deteriorated fast, prompting the army to issue an official advisory to the citizens to be cautious of spreading fake news (ANI 2019).

Another long-running urban legend being pushed via social media and instant messaging apps is that a small group of outsiders are roaming the region and looking to kidnap small children (please see, Bhattacharyya 2017) for nefarious purposes. The fake news has already claimed two young lives in 2017 through mob lynching in Assam (Karmakar 2018), but similar stories are still getting circulated. The region is even now sitting on a power keg, with almost 1.9 million people being left out of the National Registrar of Citizens (Sarma and Bhattacharyya 2021); a concerted misinformation campaign can rekindle the insurgency in the region. The new Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules have aimed to target the origin of such news as the cybercriminals behind these insidious campaigns have long hidden behind the veil stitched by the anonymity of end to end encryption. The need for attribution trumps the need for privacy, given that lives are being lost due to the spread of fake news.

Coming back to the Chinese interests in the region, we must remember that the Doklam crisis was the Chinese creeping closer to the Siliguri Corridor, a long-term objective to cut off the north eastern states from the mainland. China has also continued to claim Arunachal Pradesh as Chinese territory. As a matter of state policy, China has over the years kept the insurgency in the region alive by supplying the insurgent groups with arms and financial aid (Bhalla 2016). With growing digitization in the region, including ramped up digitization of the oil pipelines and power grids, the region is becoming hugely vulnerable to asymmetric warfare conducted by external hacker groups based out of Chinese soil.

The problem is that no independent assessment has been made of the vulnerabilities in the region's critical infrastructure, thus making any kind of predictions irrelevant. While most significant states facing organized cyberattacks have a state CERT, Assam and the other north eastern states are an exception. Given the region's strategic importance, local state CERTs or a common north eastern CERT must be set up to tackle the growing problem of cyberattacks and act as the regional nodal body to author the appropriate response. The Cyberdome project (Radhakrishna 2019) of the Assam government is a good initiative, but it has to be well structured to undertake CERT functions and do threat mitigation and train law enforcement authorities on cyber investigations and forensics. With almost 75% of the regional population expected to be online by 2025, the region can expect to start reaping the benefits of digitization, but it cannot be accomplished without developing strong cyber resilience as that would leave the region vulnerable to the worst of the worst cyberattacks. The region needs to develop a graded risk approach along with vulnerability testing to address the problem at hand.

16.7 The Current Response Model

The National Cyber Security Policy announced in the year 2013 was devised to give an umbrella approach for ensuring a safe and secure cyber experience to individuals and businesses alike and also help in capacity building around the overall cyber security ecosystem as well as fostering economic opportunities among youngsters and start-ups. Cybersecurity management was the key focus of the policy. It is this policy directive that determines our response to incidents in cyberspace.

The model has multiple lacunas, the primary being the communication between the public and private bodies. We must remember that the majority of institutions hit by cyberattacks are private organizations that most times do not even know who to call and report the breach. These private organizations are battling hackers with the backing of enemy states with almost infinite resources. And that is a battle that cannot be won. The security of our networks is too important to leave in the hands of the private industry.

In the north eastern states, the majority of the cyberattacks are directed at individuals or small mom and pop outlets and take the form of financial frauds. In this context, the greatest enemy is lack of awareness. The survey undertaken by the

Cyber Peace Foundation (PTI 2020) has clearly demonstrated that a majority of the population are unaware of online financial frauds through phishing. Even when the individual is aware of cyber frauds and the need to protect personal data, they are not very comfortable going to the law enforcement to report an act of data breach. This might also stem from the fact that local law enforcement in India does not actively investigate cybercrimes other than lodge a complaint unless the case is in the media's eye.

The other major problem with individual users is that they do not update their applications or apply security patches on a regular basis. Adobe Acrobat has been regularly releasing software patches, but most people using the Adobe softwares do not apply these patches regularly, resulting in intrusions through the software, a common occurrence in most small communication agencies. Obsolete hardware and software remain one of the most significant causes for the data breach.

The COVID-19 pandemic has driven people to work from home, resulting in an explosion of cyberattacks as the basics of cybersecurity are thrown to the winds. At the same time, the pandemic spurred the use of digital payments, which has also been a factor behind the increase in cyberattacks (Parent 2020).

It is also high time that cybersecurity compliance is made mandatory and regulations to handle data breaches. The passage of the Personal Data Protection Bill 2019 currently with a select parliamentary committee will address these issues. Take the case of Mobikwik (The Hindu BusinessLine 2021), who should have informed its customers about the data breach to enable the said customer to take protective action. Instead, the company has maintained innocence, probably as they are in the process of coming out with an initial public offering. CERT-In could has pushed through a third-party audit, but strangely that has not been ordered.

16.8 Cybersecurity Response Model for the Future

India faces one of its toughest challenges as we are subject to persistent and sophisticated malicious cyberattacks that threaten our institutions. North eastern states in particular will face the growing menace of cyberattacks as the government will look toward achieving universal digitization to improve the delivery of governance to the citizens. That will be accompanied by increasing risks. What we must realize is that the digital world has completely metamorphosed over the last seven years. The cyber threats today are far more complex, and this complexity will only grow with time. It is time to take bold decisions if we are to win this asymmetric war that has been fostered on us. Incremental changes will just not do. To tackle this menace, a structured approach and an institutional rethink are necessary. Here, I will try and list down some broad approaches that will help better respond in this digital battlefield as far as north eastern India is concerned.

1. ***Public Private Partnership***: Cybersecurity is too important and complex to be left to the private organizations. In the absence of a Personal Data Protection

Act in place, the companies have no real incentive to push for cybersecurity in their networks except for compliance. That has to change and change fast. The organizations have to be incentivized to consider cybersecurity as a key parameter of evaluation. That means either put punitive penalties for data breaches or the possibility of monetizing the data held by an organization. Today, organizational databases are sold for huge sums of money on the darknet but do not even have notional value when the same data is registered on the balance sheet. Secondly, we need an apex response body for cyber incidents, but the same body must have private members to eschew better coordination and communication. It is also extremely urgent that the law enforcement agencies work with various private and not for profit bodies to build awareness among the public on the nature and quantum of cyber risks and ways to negate the same. And this has to become an ongoing exercise if we want the citizens to be genuinely prepared to tackle the cyber threats.

2. ***Money, Money, Money***: Battles are won with resources and that takes money. The problem is that most organizations and even the government will pay lip service to data security but when it comes to actually doing something, monetary restrictions will crop up. On the other hand, the hackers at the other end have humongous resources and all the time in the world. This is a battle that can be won only with huge sums of money. The government made a start this year by allocating INR 1500 million to cybersecurity in the Union Budget (Union Budget 2021; see also, Mali 2021), but the sum is too insignificant to really make a difference. A budget has to be set aside for cybersecurity and network upgradation to tackle obsolescence at the state levels.
3. ***Weakest Link***: The commercial networks and public networks operate in an interconnected world as no network in the twenty-first century can be truly standalone. Therein lays the opportunity for the hacker who looks to target the weakest link in the chain. In the case of the SolarWind hack, the weakest link in the chain was the Orion system which could have been identified and protected better if the users could have done an honest analysis of the weakest chain. As work from home becomes an accepted part of life in the north eastern region, individual connections will need to be analyzed and strategies designed to lower risks.
4. ***Securing the Telecommunication Link***: In one of the most significant attacks of its kind in 2016, malware took control of the computing power of millions of video cameras connected to the Internet. These networked computing devices were harnessed to mount a massive DDOS attack and take down large parts of the Internet. The telecommunication chain is the most vulnerable part of the Internet. Huawei is not a part of the 5G test rollout because the company has often been referred to as an arm of the Chinese Communist Party and has been accused of using its devices to act as listening posts. But just removing Huawei from 5G rollout is not enough. The telecom link is often the most used node for entry into a system. Securing the chain is an important element of cybersecurity. Last year, the Department of Telecommunications in a bid to boost indigenization as well as improve the network security ruled that for future telecom supply, only trusted vendors whose list would be released by the government would be

acceptable (BS Web Team 2020). But this precluded existing contracts. Given the strategic nature of the north eastern states, it would be imperative to vet all existing contracts and secure the telecommunication chain at the earliest.

5. ***Data Protection Bill***: Without a legislative framework for personal data protection which penalizes data breaches, we cannot create a resilient cybersecurity model. It is indeed worrying that the Parliamentary Panel has still not approved the final bill to be tabled in the Parliament (PTI 2021). Delay in this matter can be calamitous.
6. ***Graded Approach***: The north eastern states need to apply the same graded approach to cybersecurity that is the accepted practice nationally. That means critical infrastructures will be at the top of the list of priorities. A complete evaluation of cyber risks should be at the top of the regional agenda to better prepare for the stormy times ahead.

16.9 Conclusion

The fast changing digital landscape is continuously throwing new challenges at network security, and both India as well as the narrow north eastern region will be targeted in future. If we do not prepare now, we will be putting our nation at grave risk. With the adoption of the Sustainable Development Goals (SDG) for 2030 as one of the key indicators, cyber capacity building and systematically linking these efforts with its development cooperation funds will become a key imperative. In the cybersecurity sector, the desired impact and the overall objective are to provide the citizens of the north eastern region an open, free, secure, resilient, and peaceful cyberspace. Reference to this can be found as a target under SDG 9 which states to "build resilient infrastructure, promote inclusive and sustainable industrialization, and foster innovation", as well as under SDG 4 which states the introduction of "quality education", SDG 8 backs on "decent work and economic growth" and SDG 16 on "peace, justice, and strong institutions" (The 17 Goals n.d). Given the focus on SDGs in determining growth parameters, cybersecurity has to now take the center-stage. That will go a long way in ensuring a safe and resilient digital society in north eastern region.

References

Aiken M (2016) The cyber effect: a pioneering cyberpsychologist explains how human behavior changes online. John Murray Press, London

ANI (2019) CAA protests: army issues advisory against fake news, disinformation, 14 Dec. https://www.aninews.in/news/national/general-news/caa-protests-army-issues-advisory-against-fake-news-disinformation20191214102622/

Barakbulletin (2021) An analysis on the biggest cyber fraud in Barak Valley's history; "matter under investigation". SP Cachar, 30 May. https://www.barakbulletin.com/en_US/an-analysis-on-the-biggest-cyber-fraud-in-barak-valleys-history-matter-under-investigation-sp-cachar/

Bhalla D (2016) Strategic significance of North East India. IMR Media Pvt Ltd
Bhattacharyya R (2017) Sociologies of India's missing children. Asian Soc Work Policy Rev 11(1):90–101. https://doi.org/10.1111/aswp.12116
Bhattacharyya R (2018) Living with Armed Forces Special Powers Act (AFSPA) as everyday life. GeoJournal 83(1):31–48. https://doi.org/10.1007/s10708-016-9752-9
Bhattacharyya R (2019) Chapter six: did India's partition lead to segregation of North East India? In: Ranjan A (ed) Partition of India: postcolonial legacies. Routledge, London, pp 105–131
Bhattacharyya R, Pulla V (2020a) Nagas: a bitter past—from British period to Nehru. In: Pulla VR, Bhattacharyya R, Bhatt S (eds) Discrimination, challenge and response: people of North East India. Palgrave Macmillan, pp 115–140. http://doi.org/10.1007/978-3-030-46251-2_7
Bhattacharyya R, Pulla V (2020b) The Nagas Saga and an uncertain future? Nagas after Nehru to Modi. In: Pulla VR, Bhattacharyya R, Bhatt S (eds) Discrimination, challenge and response: people of North East India. Palgrave Macmillan, pp 141–159. http://doi.org/10.1007/978-3-030-46251-2_8
BS Web Team (2020) India to name 'trusted telecom sources', may blacklist Chinese vendors. Business Standard, 16 Dec. https://www.business-standard.com/article/economy-policy/india-to-set-up-national-security-panel-on-trusted-telecom-sources-devices-120121600742_1.html
Carlson B (2021) The Microsoft exchange server hack: a timeline. CSO, 6 May. https://www.csoonline.com/article/3616699/the-microsoft-exchange-server-hack-a-timeline.html
Castagna R (2021) AI ups the ante for IoT cybersecurity. IoT World Today, 10 Feb. https://www.iotworldtoday.com/2021/02/10/ai-ups-the-ante-for-iot-cybersecurity/
Chari H, Bahadur B, Kumar V (2020) NFHS-5: how did Indian states fare in the internet usage question? Down To Earth, 30 Dec. https://www.downtoearth.org.in/blog/science-technology/nfhs-5-how-did-indian-states-fare-in-the-internet-usage-question--74843
Erikson J (2008) Hacking: the art of exploitation, 2nd edn. No Starch Press, USA
Global Risks Report (2021) World Economic Forum. https://www.weforum.org/reports/the-global-risks-report-2021
Greenberg A (2021) The colonial pipeline hack is a new extreme for ransomware. Wired, 08 May. https://www.wired.com/story/colonial-pipeline-ransomware-attack/
Hadnagy C (2018) Social engineering: the science of human hacking. Wiley, Hoboken
Helman C (2021) FBI: colonial pipeline hacked by 'Apolitical' group darkside. Forbes, 10 May. https://www.forbes.com/sites/christopherhelman/2021/05/10/fbi-colonial-pipeline-hacked-by-apolitical-group-darkside/?sh=662f60fa441821
Jamie P (2020) India's Dr. Lal Path Labs allegedly exposes millions of patients' data while using Amazon with no password. Tech Times, 08 Oct. https://www.techtimes.com/articles/253186/20201008/indias-dr-lal-pathlabs-allegedly-exposes-millions-patients-data-using.htm
Mali K (2021) Budget 2021: reactions from the technology & cybersecurity industry. Techgraph, 3 Feb. https://techgraph.co/budget-2021/budget-2021-reactions-from-the-technology-cybersecurity-industry/
Myre G (2021) How bitcoin has fueled ransomware attacks. NPR, 10 June. https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks
Nakashima E, Harris S (2018) How the Russians hacked the DNC and passed its emails to Wikileaks. Washington Post, 14 July. https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html
Nanda PK (2021) Cyberattacks surged 3-fold to 1.16 mn last year in India. Mint, 23 Mar. https://www.livemint.com/news/india/as-tech-adoption-grew-india-faced-11-58-lakh-cyberattacks-in-2020-11616492755651.html
National Crime Records Bureau (NCRB) (2018) Crime in India. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/en/crime-india-2018-0
NFHS 5 Survey (2021) National family health survey, India (2019–20), Assam. http://rchiips.org/nfhs/NFHS-5Reports/Assam.pdf

Parent M (2020) Cyberattacks are on the rise amid work from home—how to protect your business. The Conversation, 08 Dec. https://theconversation.com/cyberattacks-are-on-the-rise-amid-work-from-home-how-to-protect-your-business-151268

Presidential Actions (2021) Executive order on improving the nation's cybersecurity. The White House, 12 May. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

PTI (2020) Assam launches cyber safety awareness campaign. Outlook, 02 Oct. https://www.outlookindia.com/website/story/india-news-assam-launched-cyber-safety-awareness-campaign/361332

PTI (2021) Joint committee on data protection bill gets another extension to submit report. The Economic Times, 25 Mar. https://economictimes.indiatimes.com/news/india/joint-committee-on-data-protection-bill-gets-another-extension-to-submit-report/articleshow/81686245.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

Radhakrishna T (2019) City surveillance, intelligent TMS, cyberdome projects are coming up in Guwahati, says Assam state police chief. ETGovernment, 18 Nov. https://government.economictimes.indiatimes.com/news/governance/city-surveillance-intelligent-tms-cyberdome-projects-are-coming-up-in-guwahati-says-assam-state-police-chief/72096231

Rahul K (2018) Two men beaten to death in Assam. The Hindu, 09 June. https://www.thehindu.com/news/national/other-states/two-men-lynched-on-suspicion-of-being-child-lifters-in-assam/article24122413.ece

Sapkale Y (2019) Aadhaar data breach largest in the world, says WEF's global risk report and Avast. Moneylife, 19 Feb

Sarma PK, Bhattacharyya R (2021) Assembly elections of India, 2021: revisiting Assam. Space Cult India 9(1):6–28. http://doi.org/10.20896/saci.v8i4.1189

Sentinel Digital Desk (2021) UPI & payment frauds soar high in north-eastern states: report. The Sentinel, 07 May. https://www.sentinelassam.com/national-news/upi-payment-frauds-soar-high-in-north-eastern-states-report-537286

SolarWinds Security Advisory (2021) Solarwinds, 6 Apr. https://www.solarwinds.com/sa-overview/securityadvisory

Temple-Raston D (2021) A 'worst nightmare' cyberattack: the untold story of the solarwinds hack. NPR, 16 Apr. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

The 17 Goals (n.d) Department of Economic and Social Affairs, Sustainable Development. United Nations. https://sdgs.un.org/goals

The Hindu BusinessLine (2021) Data of 3.5 m MobiKwik users allegedly hacked, 31 Mar. https://www.thehindubusinessline.com/info-tech/data-of-35-m-mobikwik-users-allegedly-hacked/article34192591.ece

The Print Team (2021) How Chinese cyber-attacks, Mumbai blackout depict a new era of low-cost high-tech warfare, 03 Mar. https://theprint.in/opinion/how-chinese-cyber-attacks-mumbai-blackout-depict-a-new-era-of-low-cost-high-tech-warfare/614892/

The Shillong Times (2021) Only 12 pc of cybercrime victims sought police help, reveals survey, 16 Mar. https://theshillongtimes.com/2021/03/16/only-12-pc-of-cybercrime-victims-sought-police-help-reveals-survey/

Tidy J (2021) Hacker tries to poison water supply of Florida city. BBC, 08 Feb. https://www.bbc.com/news/world-us-canada-55989843

Union Budget (2021) Ministry of Finance, Government of India. https://www.indiabudget.gov.in/