53

ORF SPECIAL REPORT

DECEMBER 2017

Cyber (In)security: Looking Back at 2017

Samir Saran

The promise of cyberspace is immense; can India's security architecture keep up? / Photo: Kickstarter

INTRODUCTION

Cyber (in)security, 2017 has proven, is a great leveler. From the individual tweeting on her cellphone, to the corner storekeeper who relies on digital payments, to the multibillion-dollar corporation and the most technologically advanced nations – no stakeholder has been found immune from harm. The woes of the world may be the same, but India's government, businesses and civil society cannot escape the reality that the country's digital spaces are uniquely vulnerable.

Observer Research Foundation (ORF) is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research, and stimulating discussions.

To know more about ORF scan this code

ISBN 978-93-87407-41-1

India is at once a bustling digital democracy and a budding digital economy. The national imperative to keep its networks open while coming down on malicious actors is easier proclaimed than addressed. But if this unique, finely balanced model can be created and sustained, it will be a shining example for democracies and emerging markets alike. For what it is worth, 2017 illustrated the difficulties ahead for policy planners.

The potential of cyber space is a factor of the trust that it commands from users, businesses and governments. Unfortunately, malicious agents – both state and non-state – have shown themselves increasingly capable of disrupting core infrastructure and services, and undermining that trust. By some estimates, cyber crimes are expected to cost upwards of $2 trillion by 2019. The risks, however, cannot simply be measured financially. The loss of personal information, corporate reputation and national security are immeasurably more valuable.

2017 has been a tumultuous year for both technological advances as well as the means to disrupt them. Nations around the world are now waking up to the fact that 'protection' of their information systems is a national priority, both for their economies as well as their democratic institutions. For democracies attuned to the free flow of information – taking both the good and bad in their stride – this is a particularly vexing problem. Is information to be controlled and vetted?

Vulnerability within consumer devices, malicious bots, artificial intelligence and information warfare were some of the most important issues confronting cyber space in 2017. However, the cyber risk landscape is dynamic and responds rapidly to new technologies and new security measures. Considering that millions of new users are coming online every year, it is useful to take stock of this changing threat landscape and examine some developing trends which can benefit conversations on cyber security.

One of the most promising developments in cyber space is the growing interconnectivity of digital networks, and with it, communities. The internet of things (IoT) – a network of physical devices and objects designed to collect and exchange data – is perhaps the fastest growing field of technology in the 21st century. Be it moisture sensors to help farmers water their crops, or blood pressure monitoring devices placed in pacemakers, IoT has the potential to revolutionise our daily lives. Their impending ubiquity, however, makes it difficult to measure the inherent risks. As we race towards 50 billion IoT devices by 2020, each of these devices will collect vast amounts of

data on our daily habits, activities, and lives. With every new IoT device, our digital footprint is set to exponentially increase – creating an ever-expanding number of entry points for hackers and cyber criminals.

In July 2017, hackers attempted to steal sensitive data from a North American casino by hacking into its internet connected fish tank. The compromised tank was then used as a gateway into other systems in the casino. The device was an unsuspecting vulnerability in the casino's system, and is representative of the larger risks the IoT ecosystem faces.

A 2015 report by the United States Federal Trade Commission found that fewer than 10,000 households using home-automation services were generating 150 million discrete data points every day, i.e. around one data point every six seconds. Worryingly, the data collected from these devices – from 'smart' wristbands to TVs – are not always secured. Most IoT manufacturers place little emphasis on device security, and very few industry standards have been developed so far to tackle this problem.

A team of researchers from Microsoft and the University of Michigan discovered multiple vulnerabilities in Samsung's 'smart home' platform. The most noteworthy of which involved them taking control of smart locks and smoke detectors connected to the network. The significance of this cannot be overstated – if hijacked by malicious hackers or criminals, these technologies can catalyse man-made disasters and bring entire cities to their knees.

These unsecured devices can also be used in an aggregated manner to attack critical internet, or public, infrastructure. In October 2016, Dyn – a domain name management product suite – suffered a massive denial of service attack. Interestingly, criminals used over 100,000 seemingly innocuous devices, such as printers, cameras and baby monitors to rapidly scale the attack. They were coordinated through the 'Mirai' Botnet, a freely distributed malware, used to infect the IoT devices.

By some estimates, the market size for IoT products and services in India is expected to reach around $9 billion by 2020. Apart from consumer markets, much of this growth will be spurred on by government initiatives that intend to integrate IoT devices with the smart cities mission and other infrastructure initiatives. This puts New Delhi in a vulnerable position; without an adequate cyber security framework, cities become prime targets for malicious actors, considering the damage inflicted can be rapidly scaled in terms of intensity and scope.

Source: McKinsey Global Institute

If the risks inherent in the proliferation of an IoT ecosystem offer any lessons, it is that the ubiquity of networked systems brings with it multiple vulnerabilities. The future of cyber crime is likely to be characterised both by large data breaches or sophisticated network attacks, as well as digital 'pick-pocketing' – millions of small value transactions that can cause disproportionately serious damage without raising suspicion. A series of aggregated, relatively low-value and distributed cyber crimes may in fact present a substantially more difficult challenge to regulators and law enforcement agencies than a single, sophisticated cyber attack.

Advance fee fraud, which contributes to billions of dollars stolen every year, is the classic example of low-level activity that goes undetected and remains undeterred. Coupled with the fact that the average time to detect a breach or fraudulent activity can take several weeks, the financial costs of such crimes can be staggering. In 2016, a criminal gang called the 'Lazarus Group'

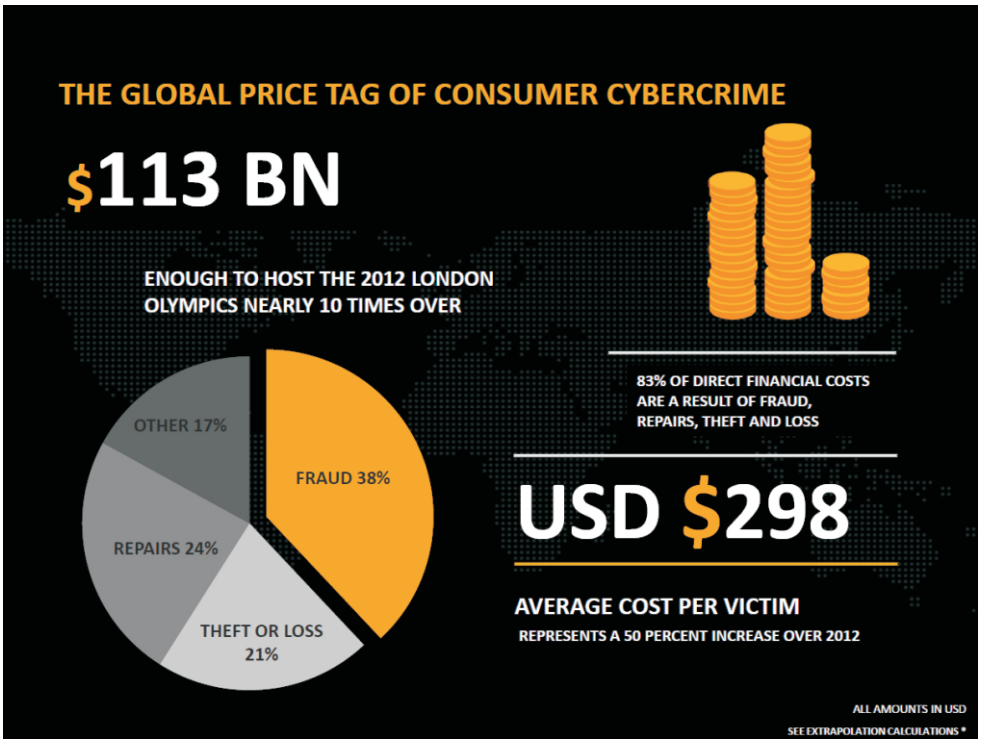
developed a software to manipulate the SWIFT system – which is commonly used for international financial transfers. By targeting banks with lower security, the group successfully initiated fraudulent transfer requests across multiple jurisdictions. Reports indicate that US$ 81 million went unrecovered from the Bangladesh National Bank, $10 million was lost from a Ukrainian bank, and a bank in Ecuador suffered losses up to $12 million, among several other such incidents around the world.

Just in 2016, Tesco Bank in the United Kingdom reported that cyber criminals stole up to £ 2.5 million from over 9,000 customers. In 2016, Indian banks suffered a financial breach that affected 3.2 million debit cards. These digital pickpockets are not only harder to identify but the damage caused is nearly impossible to restitute. A pattern of attacks is not readily apparent in these circumstances, wasting crucial response time necessary for responding to these breaches. Further, many countries still lack the resources to devote time to smaller crimes.

For developing countries like India that are coming online on a wave of cheap and unsecured mobile devices, the implications are grave. This assumes added significance in light of the Aadhaar platform that seeks to improve government services, foster financial inclusion and build a digital economy. While the data in transit might be secure, the infrastructure and application layer of the ecosystem – which includes mobile handsets and services such as Paytm, continue to remain vulnerable. This is compounded by the fact that India's supply chains reside abroad, which makes it difficult to ensure system-wide compliance with security requirements.

Already, news reports have highlighted instances of personal data leaks and attempted unauthorised authentication. While the biometric database might continue to remain secure, a new wave of sophisticated digital pickpockets are likely to find vulnerabilities to use against individual, low-value targets that are more attractive compared to heavily secured 'fat cats'. The most vulnerable are likely to be the poorest, whose relative lack of digital skills and access to law enforcement capacity make them susceptible to such attacks.

A commonality between the insecurity represented by IoT and digital pocketing is that the vulnerability resides not just in the technology, but also in the human beings operating them. From forgetting to change default passwords on their thermostats to leaving access codes on a post-it note, the stage at which humans interact with machines represents a lucrative point of intrusion.



Source: 2013 Norton Report

Cyber crimes for financial gain, however, comprise only one side of the coin. Increasingly, more and more of our lives are lived online; our thoughts and actions affected by developments in the digital realm. The man-machine integration is near the cusp of completion, where every single action leaves a digital footprint. As Chief Justice Roberts of the US Supreme Court said, "modern cell phones... are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."

Technology is fast evolving from a mere tool to an extension of our own selves – when we communicate online and store our thoughts on the cloud, we are not mere chefs wielding knives, we are authors, scripting our own private biographies. Over the past decade, scientists have been exploring the possibility of linking the human brain to computers – converting neurological impulses into code. It is only now that technological businesses like Tesla are foraying into this space, attempting a convergence of 'biological intelligence with technological intelligence', hinting at the commercial value in the hitherto untapped human data.

Currently, the law sees individuals and the technologies they use as two distinct entities. However, if we erode protections for our technological tools, we also encroach upon the private spaces of individuals. As this becomes viable in the next decade, how will our legal institutions seek to build distinctions between what we think and what we

store online? If legal warrants can compel the divulgence of the contents of our hard drives, can the same warrants be used to divulge our thoughts? When centuries worth of legal scholarship around privacy has been navigating us towards increased control over our information, the challenge of tomorrow will be to remain private and yet connected.

These same technologies will also pose constitutional challenges in India. For example, the Indian Constitution prohibits self-incrimination during criminal trial. Time and again the Supreme Court has interpreted this to protect the privacy of mental processes. Once these processes are 'on the cloud', will they be treated as private thoughts or merely records of thoughts to be used as documentary evidence?

Traditionally, Indian policy has been slow to evolve in the face of rapidly changing technology. The ill-fated National Encryption Policy of 2015, for example, unduly prioritised law enforcement imperatives against civil liberties and higher security standards. Once the line between the biological and technological blur, India will require new frameworks to ensure the integrity of such sensitive systems and protect the privacy and other fundamental rights of the individual.

Additionally, the direct threat from new technology is a fact that cannot be ignored. As artificial intelligence capabilities continue to grow in the near future, the likelihood of automated and autonomous attacks is on the rise. Data theft and network penetration represent only the least damaging scenarios. Former United States President Barack Obama has even gone on to say that a sophisticated machine learning algorithm could potentially steal nuclear codes.

The 2016 Dyn attack was orchestrated by real humans, who used bots to execute attacks when they saw fit. Many believe that we are inching closer to an AI powered botnet attack, which is likely to be even more devastating. The US' Defence Advanced Research Projects Agency recently conducted a 'Cyber Grand Challenge', which pitted algorithms against each other to search for network vulnerabilities and patch them. Many have already warned that these techniques will be used to exploit vulnerabilities instead of fixing them.

According to Darktrace, a company which specialises in AI cyber security, countries like India are fertile testing ground for such attacks considering the lack of effective security architecture. In fact, the company reports that, already, a low-level attack took place in November 2017, which used malware that could learn as it was spreading, and altered its methods to stay in the system for as long as possible. Already, India struggles with conventional cyber

attacks. The scale and intensity of new AI powered attacks could potentially cripple critical infrastructure and services.

It is unsurprising that Microsoft has called for a 'Digital Geneva convention' in order to establish the rules of the game when it comes to cyber space. Unfortunately, it is unclear if nation states have the necessary political will to undertake such actions. Previous attempts such as the United Nations Group of Governmental Experts on cyber norms for peaceful use of ICTs ended in a deadlock, with countries disagreeing on whether norms of non-interference would compromise their state sovereignty.

In the future, these questions can be rendered redundant with the advances in machine learning. A sophisticated automated system capable of propagating without human intervention raises a troubling question – who is in control? Already states are debating rules for 'Lethal Autonomous Weapons Systems' – AI systems that will be able to make life or death decisions in war.

This has raised complex questions around laws of war and human ethics. India, as chair of the Group of Governmental Experts Meeting on Autonomous Weapons, has already deliberated on many of these questions in November 2017. Where does the liability lie for machines that function outside human control? Which principles of international law provide protection against these attacks? These important questions beg resolution today; whether a consensus on the use and development of these weapons is possible, remains to be seen.

While many of these developments pose security challenges to individuals and businesses, the past year witnessed an event many thought was never attainable through technology – the subversion of democratic processes. Even today, the precise scope of Russia's 'influence operations' on elections in the United States and Western Europe is unclear. What is certain, however, is that Russia deftly manipulated the electoral process and social media in some cases to achieve its desired outcomes.

Hacking into the US Democratic National Committee's e-mail system was only the tip of the iceberg. The wave of leaks which followed damaged Hillary Clinton's presidential prospects by throwing the Democratic Party into disarray and fueling the popular anti-establishment mood against her. Equally significant was Russia's disruptive use of social media. The medium itself represents liberal values on and of the internet – an open and inclusive platform capable of bringing communities together. By inserting fake news and generating manipulated trends, Russia successfully undermined these values by polarising the American electorate.

For decades, Russia and other authoritarian regimes were haunted by the spectre of 'colour revolutions' at their doorstep. America's creative use of information technology and civil society resistance towards the end of the 20th century represented 'asymmetric operations' against communist regimes. To Russia, an enfeebled economy, cyber operations represented the perfect counter force – difficult to anticipate and difficult to trace but easy to execute across oceans. The digital disruptions of tomorrow seem eerily similar to the colour revolutions of the past.

Although the interference with American presidential elections has gained the most attention, to Russia, this is not new. Over the past five years, it has perfected these techniques in Eastern Europe – in states like Ukraine, Georgia and even Germany. Most countries in the EU states are bracing for similar operations during their own elections – with France having successfully taken somewhat controversial countermeasures such as banning TV and creating phony email accounts and fake documents to misdirect Russian hackers.

Speaking at CyFy 2017 – the Observer Research Foundation's annual conference on technology, security and society – several panellists highlighted that Russian motivations are likely multifaceted. For one thing, they seek to undermine democratic processes in order to legitimise their own political systems. On the other hand, they also seek to disrupt the current forms of cyber governance, testing the limits to which conflict in cyber space is permissible.

India's primary geopolitical rival, China, has already developed the tools necessary to carry out such operations. After years of perfecting cyber espionage and other such techniques, even against powerful countries such as the United States, the likelihood that China will attempt to influence India's democratic institutions must not be dismissed. As a democracy, India will have to toe a fine line between preserving the free flow of information and preventing malicious actors from manipulating that information.

China, however, is not the only threat. Considering Pakistan's weaker conventional military prowess, what is to stop it from using asymmetric methods of cyber warfare? The implications of these events are dire. For one thing, revisionist regimes now have a reliable template to emulate in other parts of the world. That such actions require limited financial and technical resources dramatically reduce the costs of destabilising perceived rivals. Our traditional political and military structures no longer seem capable of keeping up with the deluge of attacks that rely on misinformation and propaganda.

These methods are no longer constrained by traditional paradigms of power. In the 20th century, military capability was determined by the size of a state's army, navy or air force. That Russia, a one-and-a-half

trillion-dollar faltering economy, subverted institutions in America, an eighteen trillion-dollar superpower, only goes to show how effective 'influence operations' can be.

A democracy thrives on trust in government institutions and even in media. By undermining the integrity of this relationship, Russia successfully fueled polarisation and disaffection amongst the American public, thereby subverting the very basis of democratic norms and values. By all accounts, this was its ultimate objective. That other liberal democracies in Europe are bracing for similar events only serves to highlight the efficacy of these malicious methods.

These developments have thrown up critical questions around managing this upheaval. What structures and institutions must we build and empower to tackle these threats? The idea that causing disruptions through ICT activities is not a resource intensive exercise is only half true. It is steeped in western presumptions of power – that the one with the money and the muscle wins the war. The truth though is that both cyber defence and cyber offence need significant allocation of resources – not just in the institutions that emerged as a result of the teetering post-Cold War stability.

For a country like India, which still does not possess a coherent national cyber security architecture, responding to new asymmetric threats such as influence operations will be a difficult challenge. Such operations rely on political, ethnic and religious faultiness – which are abundant in India – to polarise individuals. Already, 'fake news' spread through WhatsApp forwards and social media has led to real instances of violence along these very lines. This year alone, for example, fake rumours about violence against Hindu's in Myanmar helped fuel anger against a wave of Rohingya Muslim refugees.

Sprawling cyber commands and advanced weaponry will not address the asymmetric capability of hundreds of internet trolls glued to computer screens with the single-minded aim of falsifying news, spreading propaganda and subverting democratic institutions. It can be contained by building capacity at the grassroots – by scripting and consolidating narratives to counter untruths and empowering communities to detect and disregard falsehoods.

Taken together, these risks exemplify the double-edged nature of cyber space. While the internet has emerged as a vehicle for transformation, its development has come with significant costs. Today, a wide array of malicious actors – be it states or rogue individuals – threaten to disrupt and dismantle the internet's core infrastructure and values. Unfortunately, these threats are non-traditional, dynamic and dispersed, and large cyber defence institutions are limited in their ability to tackle them. Instead, the individual is

likely to be front and centre in facing these challenges. We need to reimagine the role of the individual, who is at once a target and a trustee on the internet.

Accordingly, to tackle these threats, New Delhi will have to recalibrate its policy response. For one thing, building cyber capacity at the local law enforcement level is a must – a decentralised threat requires a decentralised response. Apart from building a new cadre of cyber security specialists, the Indian police force must build the capability to detect petty cyber crimes, and to analyse how these threats aggregate and cause systemic damage. Additionally, new institutional mechanisms must be put into place to build trust between individuals, businesses and the state. Victims of cyber crimes, especially low-value crimes, are currently reluctant to share information with the government. They must be able to have faith that the state will address their loss, and provide timely access to justice.

Second, new regulatory frameworks in India must incorporate 'security by design' amongst commercial products and services. A 2016 report by the Ministry of Finance on digital payments suggested a hierarchical approach to cyber security based on the systemic risk posed by different infrastructure layers and applications. This is a model that deserves replicating across networks – vulnerability must be addressed at its root. For example, some legislators in the United States have introduced a bill that will require devices to conform to specified industry standards and prohibits vendors from supplying devices that have default passwords or that possess known security vulnerabilities. India must be proactive in setting its own standards and norms for digital products, even as new platforms and networks continue developing in the market.

Third, India must invest in diplomacy. First, in areas like the UN GGE, as chair of the group on autonomous weapons, India is in a position to direct the conversation on norms, technologies and regimes to favour its interests. Simultaneously, India must also cultivate relationships with cyber powers like the United States, Israel and the EU, that can help in developing cyber security products and law enforcement training. And lastly, to reform international information sharing policies between countries and tech companies, considering that most Indian data is stored abroad.

Fourth, developing new technologies in India must be treated as a national security imperative. The government must fund research into emerging technologies, their impact on society and their implications for geopolitics. The new AI arms race between America and China is taking place in universities and think tanks, with generous aid from the government. Accordingly, these same powers will have the authority to shape how such innovations will reorganise society. To avoid being relegated in global politics, the effort to develop new technologies and to shape the norms which govern their use, must be catalysed by the Indian state.

Fifth, as a democracy, India must create institutions which are capable of bringing together local communities in order to create awareness about fake news and malicious propaganda. For example, the EU now has a 'specialized strategic communications unit', which brings to light influence operations by foreign actors. Additionally, the United States has recently listed election institutions as critical information infrastructure; a move which India should also consider in order to better prevent politically motivated hacking into party accounts and other such malicious efforts.

For a country that aspires to be a truly digital economy, India must internalise that the security of its ICT infrastructure is not a post facto consideration but a precondition for growth. At the same time, the over-securitisation of cyber governance can often lead to undermining rights which, in turn, negates the country's values as a free and democratic nation. The right answer ultimately rests on a fine balance between an ambitious aspiration of what Digital India will be tomorrow and a realistic assessment of what India's capabilities are today.ORF

(This piece has been submitted to Seminar Magazine *for publication in their 2017 Annual Edition.)*

ABOUT THE AUTHOR

Samir Saran is Vice President, Observer Research Foundation.

OBSERVER RESEARCH FOUNDATION
Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-43520020, 30220020. Fax : +91-11-43520003, 23210773
E-mail: contactus@orfonline.org
Website: www.orfonline.org