Moving forward the EU-India Security Dialogue

Traditional and emerging issues

India-EU cooperation on cyber security and data protection

Research Paper No. 11 | December 2016

DAI

EU Public Diplomacy and Outreach in India and in the SAARC

Project funded by the European Union

EU-India Think Tank Twinning Initiative

IAI Istituto Affari Internazionali

GATEWAY HOUSE
INDIAN COUNCIL ON GLOBAL RELATIONS
भारतीय वैश्विक सम्बंध परिषद्

EU Public Diplomacy and Outreach in India and in the SAARC

Project funded by the European Union

EU-India Think Tank Twinning Initiative

Moving forward the EU-India Security Dialogue:

Traditional and emerging issues

Gateway House: Indian Council on Global Relations, Mumbai,
in partnership with
Istituto Affari Internazionali, Rome

India-EU cooperation on cyber security and data protection

Prepared by Gateway House: Indian Council on Global Relations, Mumbai

Gateway House Research Team

- Sameer Patil (Project Director and Fellow, National Security, Ethnic Conflict and Terrorism)
- Purvaja Modak (Project Manager and Researcher)
- Kunal Kulkarni (Senior Researcher)
- Aditya Phatak (Senior Researcher)
- Sharmila Joshi (Editor)
- Shefali Virkar, Aprameya Rao (Interns)
- Manjeet Kripalani (Executive Director)

India- EU cooperation on cyber security and data protection

Table of Contents

List of abbreviations 2

1. Introduction 3

2. Multiple cyber security challenges 3

3. Opportunities for India-EU cyber security cooperation 7

4. Impact of EU's dual-use regime on cyber security cooperation 9

5. Data protection issues impinging on India-EU ties 10

6. Policy recommendations for India-EU cyber security cooperation 11

7. Conclusion 14

List of tables

Table 1: Major cyber incidents affecting Indian and European computer systems 4

Table 2: Policy recommendations for deepening India-EU cooperation on cyber security and data protection 12

Appendix

Appendix 1: Factsheet on India-EU cyber cooperation 16

Appendix 2: Steps taken by India and EU to address cyber security threats 17

Appendix 3: India's position on the European Convention on Cybercrime, 2001 20

Appendix 4: Summary of the DSCI White paper on the EU Adequacy Assessment of India's Data Protection 21

References 23

Bibliography 27

List of abbreviations

- APT- Advanced Persistent Threat
- BTIA- Bilateral Trade and Investment Agreement
- C-DAC - Centre for Development of Advanced Computing
- CERT- Computer Emergency Response Team
- CeBIT 2016 - Centrum für Büroautomation, Informationstechnologie und Telekommunikation
- CII - Critical Information Infrastructure
- CISO - Chief Information Security Officer
- CSDP - Common Security and Defence Policy
- CSIRT - Computer Security Incident Response Team
- DDoS- Distributed Denial of Service
- DNS- Domain Name System
- DSCI- Data Security Council of India
- EC3 - European Cyber Crime Centre
- ENISA - European Union Agency for Network and Information Security
- FTA- Free Trade Agreement
- ICS- Industrial Control System
- ICT- Information and Communications Technology
- ISO - International Organization for Standardization
- IEC - International Electrotechnical Commission
- IT- Information Technology
- IT&E - Information Technologies and Electronics
- JWG- Joint Working Group
- LEAs- Law Enforcement Agencies
- MEA- Ministry of External Affairs
- MEITY - Ministry of Electronics and Information Technology
- MHA – Ministry of Home Affairs
- NCIIPC - National Critical Information Infrastructure Protection Centre
- NCSP – National Cyber Security Policy
- NIS - Network and Information Security
- NTRO - National Technical Research Organisation
- PPP- Public Private Partnership
- SCADA- Supervisory Acquisition and Data Control
- UIDAI – Unique Identification Authority of India

Methodology

Desk research and interviews with officials of the Government of India and of the Delegation of the European Union to India, lawyers specialising in data protection issues, cyber security analysts, and representatives of Indian and European IT companies operating in India.

India- EU cooperation on cyber security and data protection

1. Introduction

Advances in information technology (IT), accompanied by the decreasing costs of computing, have created opportunities for using technology for the benefit of humanity. But, the same advances have also engendered security challenges for many countries. This includes the problem of formal attribution or pinning a cyber attack on a specific entity or location, since such attacks are routed through multiple global servers. Taking advantage of this, some states have tried to use the cyber domain to pursue their geopolitical ambitions. Cyber war, or what some states conceptualise as an 'information war', has now become the most significant form of non-kinetic warfare.

The problem of attribution, along with the growing number of cyber incidents, is complicated by the absence of a global cyber security regime or norms for state behaviour in cyber space. It is further compounded by the ambiguity of the capabilities of major cyber powers— such as the U.S., Russia and China—to launch offensive and defensive cyber operations. Moreover, given the low technological entry barriers—anyone with a basic background in computers can acquire the skills to hack networks—even non-state actors such as terrorist groups, hackers, organised criminal gangs, hacktivists are exploiting cyber space for their own purposes.

In the past few years, cyber threats have become sophisticated and nuanced. A majority of cyber attacks have targeted personal and commercial computer networks, but their consequences are no longer restricted to these levels. In 2009-10, the Stuxnet malware, allegedly designed by the U.S. and Israel, attacked Iran's Natanz nuclear facility, affecting its reactors.[1]Before reaching its designated target, it also infected the computer systems of a host of manufacturing sites worldwide.[2] As a result, cyber space and the threats emanating from it have become a focus area for many countries, including India and the European Union's member states.

2. Multiple cyber security challenges

For India, cyber threats have multiplied after a few of computer systems in the public and private sector in India were infected by the Stuxnet malware in 2010. Exploiting the same vulnerabilities in those computers (which operated on the Siemens systems) as it did in Iran, the malware infected computers across India at facilities like power plants and national oil pipelines in Gujarat and Haryana; but other than this, no major disruption was reported.[3] Yet, these disruptions made India the third largest victim of the Stuxnet virus, after Iran and Indonesia.[4]

Table 1: Major cyber incidents affecting Indian and European computer systems

Year	Incident	Implications
2007 (the year such large-scale and massively disruptive attacks were carried out for the first time anywhere in the world)	Estonian websites targeted by a Distributed Denial of Service (DDoS) attack	The attack, suspected to have been carried out by Russia, disabled the websites of the government, political parties, news organisations, and banks.
2010	Stuxnet malware infects Indian computer systems	The malware infected many computer systems in India including the Supervisory Control and Data Acquisition (SCADA) systems at power plants and oil pipelines. No other adverse impact was reported.
2011	Duqu virus hits European computer networks	The Duqu virus, similar to Stuxnet, targeted a specific number of organisations in Europe; it was used to steal information that could be utilised to attack the Industrial Control Systems (ICS).
2013	DDos attack on Spamhaus' Domain Name system (DNS) servers(located across Europe)	The attacks, the result of a business dispute (between Spanhaus, a company that filters spam, and Cyberbunker, a web-hosting company), disrupted internet services in Western Europe.
2016	Computer systems at the state secretariat of Maharashtra, India, infected by a ransomware	The attack targeted the revenue and public works departments of the Maharashtra state government, but no substantial damage to the systems was reported.

Source: Gateway House research, based on data collected from media reports

India's predominant cyber security concern is the protection of Critical Information Infrastructure (CII)[5] —telecommunication networks, air traffic, signal management, nuclear reactors, power plants, oil pipelines—which are required to be functional at all times. The weakest links in the protection of this critical infrastructure are Supervisory Acquisition and Data Control (SCADA) systems, which are used to manage the operations of these facilities. A majority of SCADA systems used in India were installed 20-30 years ago, in the pre-internet era. They were therefore not built to deal with the network-based threats or cyber attacks of today.

This vulnerability spans CII in the public as well as private sectors. It is complicated by the lack of trust between the state and the private sector. The lack of trust is the product

of multiple factors, but mainly because the private sector thinks that the government does not have the technical capability to counter cyber threats, and the government sees the private sector as not being sensitive to national cyber security concerns. Besides, private sector entities are reluctant to share the vulnerabilities of their computer systems, fearing that other private sector competitors may find a way to exploit their weakness.[6]As a result, both sides are unable to do enough in terms of joining hands to counter cyber threats.

Confidential data from India's Computer Emergency Response Team (CERT) reveals that hundreds of attacks on India's SCADA systems occur annually; anecdotal evidence suggests that their scale and frequency has been increasing over the years.[7]

Europe too is grappling with this vulnerability. A malware named Duqu, similar to Stuxnet, targeted European companies in 2011. It stole data that could be utilised to attack the Industrial Control Systems. Another instance had occurred in 2007 with a series of cyber attacks on websites of the Estonian government, the country's political parties, news organisations, and banks,[8] allegedly to achieve Russia's larger political objectives.

Except for the infections caused by Stuxnet, India has not witnessed an attack at the same level as that on Estonian websites in 2007. ButIndia remains a major target of hostile countries (such as Pakistan and China) and rogue elements (including cyber extortionists and organised crime syndicates). The country's government servers and commercial entities are clearly at the receiving end of data[9] breaches[10] and espionage attacks for stealing confidential official and commercial data. According to FireEye, a private American cyber security firm, India was the target of a decade-long espionage operation through the Advanced Persistent Threat (APT)-30 vector, carried out by a China-based group, which was most likely state-sponsored.[11] Several media reports have also pointed that India was the fifth-most spied-on country by the PRISM surveillance programme of the United States' National Security Agency.[12]

With the growing sophistication of snooping technology and the wider recurrence of and malicious social media engineering attacks, cyber-enabled espionage has acquired more worrying proportions. Europe faces the same challenge; it too has been a sustained target of espionage operations—primarily attributed to Russia and China—for stealing commercially valuable and intellectual property data. Extensive assessments from private American cyber security firms FireEye and Mandiant have noted that Europe has witnessed data breaches since 2004 attributed to the APT-1 and APT-28 vectors (suspected to be from China and Russia).[1314]

Cyber threats from non-state actors

India and Europe face another potent cyber threat from the 'deep web' or the hidden internet, which hosts thriving digital black markets that sell stolen personal data,

malware, sensitive trade secrets, stolen bank and credit card information, firearms, and controlled substances and narcotics—which cannot be bought in an open market.[15] These are powered by crypto currencies such as Bitcoin, which complicates the challenge of the deep web for a country's security establishment. The anonymity offered by the deep web has, in turn, contributed to the growth of cyber crimes, which increased by 40% annually during 2012-2014 in India.[16] American internet security firms McAfee and Symantec estimate that the annual cost of cyber crimes to the global economy is between US $375 billion (€333.57 billion)[*]and US $575 billion (€511.47 billion), with 594 million people affected globally.[17][18] Annually, cybercrimes cost India around US $4 billion (€3.56 billion) and Europe around US $13 billion (€11.56 billion).[19] For Europe, this threat emanates primarily from Eastern Europe.

One of the major black market platforms on the deep web was 'Silk Road'. It was shut down in 2013 by the U.S. government, but not before generating revenues worth US $1.2 billion (€1.07 billion) between 2011 and 2013.[20] Silk Road's activities were dominated by buyers and sellers from North America and Europe, but the site also had users from India.[21] For terrorist groups that always look for new technologies, the deep web's black market is an ideal platform to purchase arms and smuggle drugs, and to raise funds.[22] No hard evidence of such activity is available at present, but it is speculated that the weapons used during the Paris attacks of November 2015 were sourced from the deep web.[23]

For India and Europe, the use of social media and cyber space by terrorist groups for spreading their propaganda has emerged as a serious challenge. This is exemplified in their security establishments' efforts to counter the terrorist group Daesh, located in Iraq and Syria. For India, the Daesh is a different challenge from those it has encountered earlier, like the Lashkar-e-Taiba and the Indian Mujahideen. Both these groups used the internet for recruitment and propaganda, but their focus was on domestic issues such as riots and Kashmir.[24] However, Daesh's brutal violence in Iraq and Syria, its reliance on 'lone wolves' for executing attacks outside West Asia, and its social media blitzkrieg focusing on propaganda and recruitment, has opened up new avenues of online indoctrination of vulnerable youth. Given Daesh's vast social media effort worldwide, with approximately 38 unique multimedia propaganda events per day,[25] a coordinated counter response is required from the countries that are impacted, and which spans across all sectors (public, private, and civil society).

For India, inadequate awareness among the government and people of cyber security issues, and a lack of preparedness to respond to cyber incidents, deepens the challenges of cyber space. For instance, law enforcement agencies (LEAs) in India lack the cyber forensic skills that are required to gather digital evidence, which is a basic requirement in combating cyber crime.

[*] U.S. Federal Reserve rate- as on 1 October 2016, USD 1: € 0.89

The absence of boundaries in cyber space means that the computer systems of India and Europe are negatively impacted by cyber incidents occurring outside their territories. This was evident in the case of Stuxnet, and in 2013 when suspected Eastern European hackers stole bank and credit card information, mostly that of European consumers, from the servers of Nasdaq and U.S. companies including, J.C. Penney and 7-Eleven.[26]

3. Opportunities for India-EU cyber security cooperation

Despite these common threats, cyber security cooperation between India and the EU remains inadequate at present. Both sides began cooperating on cyber security issues after the 2010 Brussels Summit, where they agreed to closer cooperation and mutual assistance in this field.[27] Initial steps were limited to a bilateral consultation on cyber security and cybercrime. Subsequently, in May 2015, consultations were upgraded to a Cyber Dialogue, within the framework of the bilateral Security Dialogue.

The bilateral cyber engagement takes place at four levels:

a. The Cyber Dialogue, which lacks a security focus because it covers a wide gamut of areas including issues related to internet governance. Discussed therein are training programmes for India in the field of IT and security, assessments of cyber crime, enhancing cooperation between CERTs, and cooperation on the R&D front.
b. There are discussions within the Counter-terrorism Dialogue on the use of cyber space by terrorists. At the operational level, CERT-India has a working relationship and collaboration with CERTs in Europe and with CERT-EU.
c. India and the EU have a Joint Information and Communications Technology (ICT) Working Group, set up in 2000,which has held nine rounds of meetings so far.[28] It includes representation from the government as well as industry. Themes discussed by this group include internet governance, and ICT research and innovation.
d. India also has bilateral security dialogues with countries such as France, UK and Germany, which encompass discussions on cyber security issues.

Recently, the bilateral engagement in this sphere received a boost after the India-EU Summit in Brussels in March 2016. The summit's joint statement highlighted the links between the 'Digital India' initiative and the EU's 'Digital Single Market' strategy, through increased cooperation in cyber security, ICT standardisation, and internet governance, research and innovation.[29] The EU-India Agenda for Action 2020 has, among other goals, mentioned strengthening cooperation and working towards tangible outcomes on various areas including cyber security.[30]

It is in these areas listed above that India and the EU have significant opportunities for cooperation in cyber security.

Domestically, India is stepping up its cyber focus through many initiatives:

a. In 2013, India announced a broad policy framework in the form of the National Cyber Security Policy (NCSP). Then, the National Critical Information Infrastructure Protection Centre (NCIIPC)[31]was set up in 2014, as a response to the challenge of CII protection. The Centre works with the public and private sectors for plugging gaps in their computer systems. In 2015, the government created the post of a National Cyber Security Coordinator to synchronise efforts on cyber security issues at the national level.[32]
b. The Indian government is also engaged in capacity building of law enforcement agencies through awareness raising, training programmes, and enhancing cyber forensics skills. To counter indoctrination and the use of cyber space by terrorists, the LEAs are setting up social media labs (such as one in Mumbai) as an experiment in public private partnerships to monitor social media.[33]
c. In 2015, the Indian government launched a flagship programme called 'Digital India', aimed at improving governance and citizen-centric services by harnessing IT.[34] Another flagship project, 'Smart Cities Mission', intends to utilise technology to improve the infrastructure of the country's cities.[35] Big data management will be at the heart of these projects. IT and the Business Process Management sector is also one of the focus areas of the 'Make in India' programme.[36]

At the same time, New Delhi has put cyber security concerns on India's diplomatic agenda. For example, in the last two years, India has initiated cyber security cooperation with many countries, including Mongolia, Australia, Vietnam, Canada, Malaysia, Singapore, the UK, and Japan. It has also intensified cyber security cooperation with countries such as the U.S. (through an 'Agreed Framework for Cyber Security Cooperation') and Russia (by signing an information security agreement).

Meanwhile, in the military domain, the three wings of the Indian armed forces are at advanced stages of integrating network-centric warfare capabilities, and are increasing the awareness of cyber threats and cyber-enabled espionage among their personnel.

Europe too has taken initiatives in the cyber domain:

a. The continent as a whole took the first step in 2001 to evolve a common strategy for cyber crimes in the form of the Council of Europe's Budapest Convention on Cybercrime.[37] (India opposes this Convention. The detailed position of India is outlined in Appendix 3).
b. In 2013, the EU published its 'Cybersecurity Strategy', its first comprehensive policy document on the issue.[38]
c. In June 2016, the European External Action Service released the 'Global Strategy for the EU's Foreign and Security Policy' document which outlined the EU's

efforts in protecting against cyber threats, while striving for an open and safe cyber space.[39]

d. Organisationally, the EU has been at work since 2004when it established the European Union Agency for Network and Information Security (ENISA) to work with member states and the private sector in the field of information and network security. To counter cyber crimes, in 2013 Europol specifically set up the European Cyber Crime Centre (EC3),[40] which is the one-point source for all data regarding cyber crimes and threats.

In the military domain, the European Defence Agency has put forward cyber defence as a priority area. The 2016 Strategy has also emphasised enhancing cyber security cooperation with core partners such as the U.S. and the North Atlantic Treaty Organization (NATO).[41]

4. Impact of EU's dual-use regime on cyber security cooperation

A potential dampener for enhanced India-EU cyber security cooperation is the Wassenaar Arrangement and EU's dual-use regime.

Since the 2008 attacks on Mumbai, India has initiated important internal security measures designed to respond better to terrorist activities. One such measure has been the installation of mass surveillance systems such as the Central Monitoring System for counter-terrorism purposes. India is utilising its IT base to develop domestic solutions for setting up these systems, but many of these technologies also need to be imported off-the-shelf. This presents an opportunity for India-EU cooperation.

But India will certainly not receive the full benefit of any agreement with EU on the sharing of cyber security know-how because of the EU-wide application of the restrictions placed by the Wassenaar Arrangement, the multilateral export control regime governing the worldwide export of arms, and dual-use goods and technologies, which all EU countries adhere to.[42]

In December 2013, the Wassenaar Arrangement was amended to include controls on the export of 'intrusion software', a key element of surveillance systems.[43] [44] These amendments to the Arrangement's dual-use and munitions lists were spearheaded by the major EU members—UK[45] and France.[46] The EU has included the control lists of the Wassenaar Arrangement in its legislation and practices—the Wassenaar's 'Dual-Use Goods and Technologies List' is included in the 'Common EU list of dual-use items'[47] (including the 'intrusion software'), while its 'Munitions List' is mirrored in the 'Common Military List of the EU'.[48] The EU and its member states are thus committed twice over to applying stringent standards of export control for dual-use technologies.

Sure, the amendment to the Wassenaar Arrangement may have been intended to prevent the export of surveillance mechanisms to authoritarian governments and regimes worldwide, but the amendment has disadvantaged India specifically, which is not a member of the Arrangement. India therefore finds itself in a weakened position when dealing with the EU and its member states as a consumer of dual-use technologies. The amendment can also potentially work against India in the case of any bilateral cyber security disagreement.

5. Data protection issues impinging on India-EU ties

The EU has stringent and elaborate data protection and privacy laws, which have been linked to human rights. The European Court of Human Rights has observed that the protection of personal data falls under the ambit of Article 8 of the European Convention on Human Rights, which guarantees the right to respect for private and family life, home, and correspondence.[49]

The principal EU legal instrument on data protection is Directive 95/46/EC of 1995, which states the rules for processing and transfer of personal data, including international transfers.[50] [51] The provisions of this Directive, relating to the international transfer of personal data, affect India directly, specifically Article 25, which specifies the criteria for a country to be declared as having adequate protection.[52] In May 2010, Graham Greenleaf, an Australian professor who studied India's data protection regime as part of a EU-commissioned study, presented his findings to EU. He concluded that India's provisions for data protection cannot be regarded as adequate as per the EU's standards.[53] The EU's concern is the security and confidentiality of personal data, including preventing any unauthorised access to such data,[54] which can be potentially used by cyber criminals.

The Data Security Council of India (DSCI), the main industry body on data protection in India, contested Greenleaf's report. The DSCI responded to this EU-commissioned paper with a White Paper in January 2012.[55] It strongly argued that the regulatory changes brought in by the amendment to India's IT Act, 2000, have significantly closed the perceived gap in the regulatory and enforcement mechanisms for privacy protection. It said that these changes have made the country eligible to qualify as providing 'adequate protection' from the EU Directive's standpoint (a table summarising the DSCI White Paper on the EU commissioned paper is in Appendix 4). However, some legal experts in India are of the opinion that the amendments to the IT Act, 2000, are weak and do not provide effective protection.[56]

The DSCI's position is echoed by the Indian government, which also insists that India has adequate data protection laws under the IT Act, 2000, along with its amendments and rules. Together, the government asserts, these provide a comprehensive legal framework for privacy and data protection.[57]

The differences over India's data adequacy status have also featured in the India-EU Bilateral Trade and Investment Agreement (BTIA) negotiations, which began in 2007. So far, 16 rounds of negotiations have been held, the last one in 2013.[58] Since then, the talks have been suspended due to differences over market access and procurement related issues[59] and India's demand for 'data secure' status from EU.[60] India has linked this demand to trade, arguing that without such a status it will be difficult for both sides to engage in cross-border trade in services.However, the European Commission insists that the issue of data protection adequacy should be separated from the BTIA talks.[61] India and EU have discussed setting up a Joint Working Group (JWG) to bridge differences on India's data adequacy;[62] its status remains unknown. Incidentally, in 2013, the EU had done another study which had acknowledged the progress made by India in data protection regulations. However, the report, for unknown reasons, concluded that India did not have adequate data protection laws.[63]

While the BTIA talks remain stuck, other related complications have arisen. Some countries like Switzerland, Israel, and Japan are harmonising their data protection regimes with the EU's standards of data protection in order to increase engagement with the EU.[64] This is putting further pressure on India and Indian companies to raise their standards.

Legal experts in India are of the opinion that the evolution of a global privacy and data protection regime is being driven, to a large extent, by EU regulations. These are bureaucratic, with cumbersome and sometimes incomprehensible regulations, and are therefore creating difficulties for countries such as India. While there can be a broad agreement on privacy principles, the implementation of those principles should be left to each country, which can adapt regulations as per local socio-cultural attitudes to privacy.[65] The experts recognise that India does have enforcement problems but that the country is taking steps to address these concerns.

In particular, in 2016, India passed the Aadhaar Act (Targeted Delivery of Financial and Other Subsidies, Benefits and Services),[66] which provides for a unique identification number to those residing in India for targeted delivery of subsidies, benefits, and services. The Aadhaar Act contains a separate chapter titled 'Protection of Information' by which the Unique Identification Authority of India, established under the Act, is obligated to ensure the security of information about individuals. It restricts the sharing of this information and penalises any unauthorised access of such information.[67]

6. Policy recommendations for India-EU cyber security cooperation

For deepening India-EU cyber security cooperation, it is necessary to look at EU's cyber cooperation with other countries and understand the range of issues covered:

- EU-U.S.: The EU and the U.S. work in close coordination on cyber-related issues, both bilaterally and in multilateral fora. An annual vibrant U.S.-EU Cyber Dialogue discusses cyber security, data protection and internet governance issues, as well as confidence building measures and capacity building in third countries.[68] They also have a Working Group on Cyber security and Cybercrime, which focuses on cyber incident management, public private partnerships on security of critical infrastructure, raising awareness, and cyber crime.[69]
- EU-China: The EU has a similarly active cooperation with China. Both sides have deliberated and discussed cyber crimes, innovation and cooperation on 'Smart Cities Mission', 5G technology, broadband, etc. Many of these issues are also of salience for India.

While the path to creating trust and evolving deeper India-EU cooperation is indeed long and winding, as India's cyber security cooperation with the U.S. has shown, if India and the EU demonstrate their intent to advance cooperation with patience and perseverance, the true potential of the relationship will be realised.

Measures to further cooperation on issues of cyber security and data protection are suggested in Table 2.

Table 2: Policy recommendations for deepening India-EU cooperation on cyber security and data protection

Policy recommendation	**Guiding principles**
Cyber security	
JWG on cyber security	The Cyber Dialogue must be carried forward with regular meetings. It should also include discussions on the use of social media by terrorists, given the pervasiveness of the threat.
Public-private partnership (PPP) for mitigating cyber threats	The PPP should leverage the expertise and experience of private sector ICT companies. India has a strong IT base, with Indian IT and business process management companies exporting more than US $100 billion (€ 88.95 billion) annually.[70] Moreover, major European ICT companies are already active in India. Therefore, it is imperative for these companies to be an important element in addressing cyber threats. The expertise of these companies can be used to raise strong encryption standards, promote cyber security research, and create cyber security professionals. Their engagement should also focus on creating a network or platform where they can report the cyber attacks they face. This will certainly contribute to the resilience of computer systems in India and Europe.
Cyber crime and the deep web	
Fostering cooperation between the LEAs	An important part of cyber crime investigations is the collection of evidence. Therefore, despite their differences on the European Cybercrime Convention, India and the EU must foster practical cooperation between their respective law enforcement agencies and also with Europol for evidence collecting methodologies. This can be done by designating nodal agencies/officials to access digital evidencein timely manner. This cooperation should also include real-time

	sharing of information between both sides. As part of this engagement, India and the EU can create standards on sharing information and uniform methods of reporting cyber incidents.
Sharing lessons on their respective investigations of deep web-related cases	The challenge of cyber crime and the deep web cannot be tackled alone. A multi-jurisdictional approach is a basic requirement. Besides, solutions to the problem of the deep web are not necessarily restricted to the technology domain, and traditional investigation methods remain valid. In this context, law enforcement agencies in India and Europe can share lessons on their respective investigations of cases related to the deep web.
Interaction between the Europol's E3C and India's proposed National Cyber Coordination Centre	The Europol's E3C and India's proposed National Cyber Coordination Centre should have a formal working relationship in order to tackle cyber crime. Since the E3C also works on critical infrastructure protection, this interaction can also plug gaps in that domain, and both sides can share their best practices and work on minimum standards for security of the CII.
Informal technical cooperation among the LEAs	As against the flourishing ecosystem of the deep web, governments are still limited by silos in their responses to counter the online black markets. Technical cooperation among the Indian and the European LEAs can also be forged informally to collect the IP addresses of computers in the deep web as a first step, just like Project Honey Pot.[71]
Data protection and privacy	
Understanding Indian sensitivities on privacy issues	The EU needs to understand that every country has different socio-cultural attitudes to privacy. Hence, rather than pushing to make EU regulations a global benchmark, Brussels can work out an agreement on privacy principles with New Delhi that leaves the implementation of those principles to India's policy establishment.
Bridge differences on India's data adequacy issue	Data protection laws in India are yet to be declared as adequate by the EU—this, when done, will allow the transfer of personal data. With other countries increasingly moving towards harmonising their laws with EU regulations, the pressure will mount on India—not only from the EU but also from other countries too—to increase its standards.. Moreover, the new EU Regulations on data protection will come into effect in 2018. Therefore, despite the stalled BTIA negotiations, both sides must continue to work on data adequacy issues and resolve their differences.
'Digital India' and 'Smart Cities Mission'	
Dialogue on smart cities	The EU co-funded European Business and Technology Centre (EBTC) has recently become a partner in Pune and Navi Mumbai's 'Smart Cities' plans.[72][73] Instead of individual cities in India signing memorandum of understanding (MoU) with the EBTC, India and EU can set up a separate dialogue for 'Smart Cities'. The EU has a similar dialogue with China.[74] ENISA's work on cyber threats to smart cities should be a part of these discussions.[75]
Collaboration between Ministry of Electronics and Information Technology (MEITY) and ENISA on Internet of Things (IoT) Infrastructure in India	The IoT is still in its infancy in India, but the MEITY has recently come up with a draft policy on the IoT. Considering the criticality of the IoT and its link with 'Digital India', this paper proposes a collaboration between MEITY and ENISA on IoT as ENISA has recognised various cyber security challenges arising due to the IoT[76]. The ENISA as an advisory and training outfit can also help build human resources for handling IoT infrastructure and services in India.
Capacity building	

Increasing awareness on cyber security issues	While cyber threats keep evolving, the basic response to mitigate these threats remains simple. Cyber hygiene is the key to awareness. India and the EU can host a 'Cyber security awareness month' similar to the 'EU-U.S. cyber security awareness raising month[77]' of October 2015.
Cyber security research	The EU is expected to spend €500 million for research on cyber security and hopes that the private sector will spend three times that amount on the same.[78] Some of that research can focus on studying the cyber threats in emerging economies such as India. In particular, the existing technical capability of India on crypto currencies is inadequate. Therefore, research on these currencies and their financial and security implications must be undertaken. For this, the private sector in India and Europe should also involve the academic and scientific community. For instance, the Bombay Stock Exchange has joined hands with the Indian Institute of Technology-Kanpur for setting up a Cyber Security Centre of Excellence.[79]
Cyber forensics	The Verizon 2016 Data Breach Investigations Report states that India has witnessed a number of data breaches.[80]Surprisingly, Indian law enforcement agencies have not been able to detect even a single attack or breach. This is a worrying factor since the time taken to detect a breach is increasing while the time taken to respond and prevent the loss of control of a system is decreasing. This is primarily due to a lack of adequate cyber forensics capacity—skill sets and infrastructure—of the Indian LEAs. The EU can play an important part in building this capacity for India.
Cyber threat intelligence sharing	European countries must be forthcoming in sharing their experiences with non-European powers such as India on lessons learnt from past incidents. This can be a part of the capacity building of law enforcement agencies.
Joint simulation labs	The EU can help India set up simulation laboratories and testing facilities for carrying out controlled experiments.[81] Also, since the private sector is at the forefront of technologies, including the 'deep web', rather than government bodies, these facilities should have representation from the European private sector too.
Global cyber security cooperation	
Pushing for a global agreement on the protection of critical infrastructure from cyber attacks	Since both India and the EU have seen the consequences of cyber attacks on the CII, they must take the lead in facilitating a global agreement for protecting critical infrastructure from cyber attacks by engaging with like-minded parties(such as the U.S, Australia, Israel, and others).
Regulating the behaviour of non-state actors in cyber space	A big challenge for state actors in cyber space is to regulate the cyber capabilities of non-state actors. India and the EU can take the lead in developing an international consensus on dealing with non-state actors and thereby contribute to global cyber security cooperation.
Creating a Cyber Action Task Force	Given the criticality of a cyber threat and the lack of a dedicated global cyber security organisation, India and the EU can facilitate the creation of a Cyber Action Task Force, an organisation similar to the Financial Action Task Force (Paris), which works on combating money laundering and terrorist financing. The Cyber Action Task Force can consist of senior policy makers, and private sector and technical experts, who work to establish a set of norms and best practices. This proposed agency can be aligned with the CERTs in each country for coordination and information sharing.

7. Conclusion

The ability and capacity of the cyber saboteurs to think and act across multiple jurisdictions remains the biggest challenge in countering cyber threats; more so because the governments responding to these cyber threats are hampered by their respective

national jurisdictions. So, even if a country is prepared to mitigate cyber security challenges, the challenge of unforeseen risks still exists, which necessitates cooperation.

India and the EU must adopt a pragmatic approach to cyber security cooperation by assessing areas of common concern and expeditiously sorting out their differences, mostly on data protection. Data transfer and sharing is the key to tackling the issues that are encountered within the cyber domain. The efforts in this context cannot be limited to government and regulators. Businesses must also contribute and cooperate in mitigating cyber threats.

Enhanced cyber security cooperation between the two sides will potentially have a beneficial effect in other domains of India-EU defence and security cooperation.

Appendix 1

Factsheet on India-EU cyber cooperation

Cooperation with the EU: Platforms for cyber cooperation between India and the EU

- Joint ICT Working Group, set up in 2000, comprising G2G and B2B level dialogues focusing on internet governance, ICT research and innovation
- Cyber Dialogue at the G2G level covering security and internet governance issues
- Cooperation between CERT India and the CERT-EU

Table 1.1: Cooperation with the individual EU member states:

Country	Engagement
Estonia	• 2014: MoU signed by India and Estonia for capacity building in the sphere of e-government for five years
France	• 2000: MoU on mutual cooperation in ICT signed by India and France • 2003: MoU signed by India and France for establishing a 'Indo-French Cyber University' for information exchanges in the fields of education, training, transfer of technology, and research • 2013: India-France agreed to collaborate on ICT cluster, open data and cloud computing • 2013: First round of the India-France cyber dialogue held in Paris
Finland	• 2010: Agreement signed for cooperation in the field of information security
Germany	• 2013: India and Germany held consultations on cyber issues • 2015: India and Germany signed an MoU for security cooperation for countering terrorism, including online terrorist propaganda • 2016: India participated in the technology exhibition CeBIT 2016 at Hannover to promote the 'Make in India' campaign in the electronics and IT sectors
Poland	• 2015: India and Poland agreed to cooperate in the areas of capacity building, skill development, R&D and innovation in emerging technologies
Sweden	• 2016: India and Sweden endorsed the creation of a new JWG on Digital Technologies and Economy
United Kingdom	• 2015: India-UK Cyber Dialogue in October 2015 • 2016: India and the UK signed anMoU for cooperation on countering the cyber attacks both countries face; the agreement includes exchange of knowledge and experience in detection, resolution, and prevention of security-related incidents

Source: Gateway House research, based on the data obtained from the Government of India's Ministry of External Affairs and Ministry of Electronics and Information Technology.

Appendix 2
Steps taken by India and EU to address cyber security threats

Table 2.1: Policies implemented by India on cyber security and data protection

Act/Policy	Year	Details
Cyber security		
National Cyber security Policy	2013	It aims at protecting the information infrastructure in cyberspace, reducing vulnerabilities, building capabilities to prevent and respond to cyber threats and minimising damage from cyber incidents. The objective is to create a secure cyberspace ecosystem, strengthen the regulatory framework, and launch a comprehensive national awareness programme on the security of cyberspace.
Data Protection		
Information Technology Act (with a 2008 amendment)	2000	It elaborates on offenses, penalties, and breaches and outlines the justice dispensation systems for cyber-crimes and provides for the constitution of a Cyber Regulations Advisory Committee.
Right to Privacy bill	2014	The bill extends the right to privacy to all residents of India. It defines nine specific privacy principles: i) notice ii) choice and consent iii) collection iv) limitation v) purposes limitation vi) access and correction vii) disclosure of information viii) security ix) openness and accountability. It requires authorisation by the relevant state authority for the collection and processing of sensitive personal data. An earlier version of this bill was under consideration in 2011, but it lapsed.
Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act	2016	It provides for, as a part of good governance, efficient, transparent, and targeted delivery of subsidies, benefits, and services to individuals residing in India by assigning of unique identity numbers to such individuals.

Source: Gateway House research, based on data obtained from the Government of India's Ministry of Electronics and Information Technology and The Centre for Internet & Society, a Bengaluru-based NGO.

Table 2.2: Policies implemented by Europe on cyber security and data protection

Convention/ Policy/ Directive	Year	Details
Cyber security		
Budapest Convention on Cyber crime (with an Additional Protocol in 2003)*	2001	It is the first international treaty seeking to address internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations. It also sets out procedural law issues related to cyber crime. In addition, the Convention contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Signatory Parties.

Cyber Security Strategy of the European Union	2013	It sets out the EU's approach to preventing and responding to cyber disruptions and attacks. It details a series of actions to enhance the cyber resilience of IT systems, reduce cyber crime, and strengthen the EU's international cyber security policy and cyber defence.
Directive on security of network and information systems	2016	This directive provides legal measures to boost the overall level of cyber security in the EU by ensuring member states' preparedness, cooperation among all the members by setting up a cooperation group, and a culture of security across sectors—all of which are vital for the economy and society. Businesses in the sectors identified by member states as operators of essential services will have to take appropriate security measures and notify serious incidents to the relevant national authority.
Data Protection		
Directive 95/46/EC of the European Parliament and the European Council	1995	It was formulated for the "Protection of individuals with regard to the processing of personal data and on the free movement of such data." It applies not only to the processing of personal data but also to transfer of such data, including international transfers. It lays down the criteria for a country to be declared as having adequate protection.
Data protection directive, Regulation (EU) 2016/679	2016	This regulation will replace Directive 95/46/EC (General Data Protection Regulation). It seeks to harmonise the protection of the fundamental rights and freedoms of human beings in terms of processing activities and to ensure the free flow of personal data between member states. It will come into force from 2018.

Source: Gateway House research, based on data obtained from the official websites of the EU, European Union External Action, European Commission, and the Council of Europe
**- The Budapest Convention is from the Council of Europe*

Table 2.3: Agencies of the Government of India working on cyber security and data protection issues

Agency	**Year of establishment**	**Details**
IT security		
Centre for Development of Advanced Computing	1988	The premier R&D organisation in the IT and electronics, working on strengthening national technological capabilities. It works in close junction with the MEITY.
CERT India	19 January 2004	Works under the MEITY and is a nodal agency dealing with cyber security threats. It aims to strengthen the security-related defence of the Indian internet domain. CERT India has a working relationship with the CERTs of other countries.
Ministry of Electronics and Information Technology	2012 (earlier the Department of IT)	Promotes e-governance for empowering citizens, promoting the growth of the electronics, IT and information technology-enabled services (ITeS) industries, and enhancing India's role in internet governance. It also focuses on developing human resources in this field, and promoting R&D.
National Critical Information Infrastructure Protection Centre (NCIIPC)	2014	The nodal agency for taking all measures, including associated R&D, for the protection of CII in India. The NCIIPC has identified 12 macro sectors as critical infrastructure sectors, zeroing in on the most vulnerable infrastructure facilities in the public and private sectors; it coordinates with other relevant agencies.
Cyber Crime		
Indian Cyber Crime Coordination Centre/ National Cyber Coordination Centre	Proposed	The creation of the centre has been recommended to fight against cyber crimes. It has been accepted, in-principle, by the Ministry of Home Affairs (MHA). The centre will work on online cybercrime reporting, cybercrime monitoring, setting up of forensic units, capacity building of the police, prosecutors and judicial officials, promotion of R&D, etc.

Source: Gateway House research based on data obtained from the Government of India's Ministry of Electronics and Information

Technology, Computer Emergency Response Team, and the Centre for Development of Advanced Computing.

Table 2.4: Government agencies in the EU working on cyber security and data protection issues

Agency	Year of establishment	Details
IT security		
European Union Agency for Network and Information Security (ENISA)	2004	Works closely with EU member states as well as private firms to strengthen network and information security as an advisory agency. It looks into matters of information privacy, security issues related to software and hardware products, security solutions for firms and governmental agencies on managing the risks arising out of online information. It is not a law enforcement agency and does not regulate the operating of rules and regulations regarding network security.
CERT-EU	Pilot project – 2011; formalised - September 2012	An IT solution agency which helps EU organisations run their cyber operations, helping them fight cyber threats. It serves as the internal IT security team of the EU, comprising IT experts from the main institutions of the EU. It cooperates with CERTs in member states, as well as with private IT firms.
Cyber crime		
European Cyber Crime Centre, EUROPOL	January 2013	Acts as a law enforcement agency and deals with cyber crimes in EU member states. It focuses on areas like cybercrimes committed by organised criminal groups. It acts as the one-point source for all data regarding cyber crimes and threats that can emanate from across Europe and the world. Also acts as an investigating agency assisting investigations by member states by helping them on technical and forensic issues regarding cyber security.

Source: Collated and analysed by Gateway House, based on data obtained from the official websites of the European Union Agency for Network and Information Security, Computer Emergency Response Team, and EUROPOL.

Appendix 3

India's position on the European Convention on Cybercrime, 2001

India, in principle, agrees with the necessity to fight and counter cyber crime. Therefore, it does not does not fundamentally contest the Convention and rather uses it as a guideline for reforming the county's national legislation. India has incorporated most of the substantive provisions of the Convention in its IT Act through the amendment in 2008.[82]But the Convention remains unacceptable for India because of the following reasons:

- Drafting process: India has generally opposed treaties that have been drafted without its consultation. Therefore, India, along with China and Brazil, has argued that the Convention remains a treaty drafted by Europe, reflecting its priorities.[83]
- Implications of Clause 32 (b) of the Convention for India's sovereignty: India is particularly opposed to this clause, which talks about "trans-border access to stored computer data with consent or where publicly available" and specifically states that a party may, without the authorisation of another party, "access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."[84] This clause has grave implications for any country's sovereignty and therefore India has deemed it to be discriminatory.
- The China factor: India also believes that the Convention in its present form is insufficient in tackling the cyber crimes that it faces, predominantly originating from China. Signing the Convention will therefore not solve India's problems, and China too has not signed the Convention.

Appendix 4

Table 4.1: Summary of the DSCI White Paper on the EU Adequacy Assessment of India's Data Protection

Points raised by the EU-commissioned paper	DSCI's position
Content Principle: Purpose Limitation—use and disclosure	
There is no specific limitation on the ability of companies or the government to collect personal information, except in relation to credit information. Furthermore, the IT Act2000 does not impose limitations on the internal use of personal information by the organisation collecting such information.	It may be noted that the report by the EU assessing India's adequacy was released in 2010, prior to the enactment of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('Privacy Rules')[85]. These Rules were enacted by the central government of India vide powers under section 43A of the IT Act 2000. The Privacy Rules, specifically Rule 4 (1)(iii), 5 (1), 5(2) (a), 5 (3), 5 (5) now bring specific content with respect to the privacy principle of 'purpose limitation'. The Privacy Rules require collection of information for a lawful purpose connected with a function or activity of the collector of information, and require the information collected to be used only for the purpose for which it has been collected.
With regards to the IT Act 2000 and its 2008 amendment, the EU observes that they cover only a small part of what is usually covered by privacy and data protection laws. According to the EU, the IT Act 2000 does not deal specifically with data protection, and core concepts such as 'personal data/information', 'processing', 'disclosure', and 'consent' are not defined.	The Privacy Rules define "personal information" and "sensitive personal data or information". Rule 5 requires entities to take written consent "regarding purpose of usage" before collecting information. It also binds the companies not to collect information unless it is necessary for the stated purpose. Rule 6 requires companies to acquire prior consent before 'disclosure of information' to third parties, and disallows the third party from further disclosure.
Content Principles: Data quality and proportionality principles—collection limitations, deletion / preservation of data	
Indian law cannot be considered to provide adequate protection in relation to the collection of personal information.	Rule 5 (1) and (2) of the Privacy Rules address the requirements of this privacy principle, obligating companies to take consent for the purpose of usage before collection of information. It also stipulates that the information collected should be for the lawful purpose, and collected only if the information is necessary for the purpose.
The EU raises concerns regarding the deletion of personal data when it is no longer necessary to retain the same for the legitimate purpose for which it was collected.	Rule 5(4) of the Privacy Rules clearly stipulates that sensitive personal data or information shall not be retained for any length of time longer than is required for its lawful purposes.
Content Principles: Transparency	
The IT Act 2000 does not impose obligations on private sector organisations to disclose details of their practices.	The Privacy Rules obligate a body corporate[86] that collects, receives, stores, processes, deals in, or handles information to provide for a privacy policy regarding such information, including personal sensitive data. Rule 4 requires entities to maintain "clear and easily accessible statements of its practices and policies" in the public domain so as to make them easily available to the providers of information; this includes publishing the privacy policy on the website of the company.
Content Principles: Security	
The 2010 report examined Indian laws to	This was addressed by Rule 8 of the Privacy Rules, which requires

assess whether they meet the security principle of adequacy. The principle requires technical and organisational security measures by the data controller that are appropriate to the risks presented by the processing. The report says that no such security standard exists.	companies to have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational, and physical security control measures. The rule states that the international standard IS/ISO/IEC 27001 on 'Information Technology – Security Techniques - Information Security Management System—Requirements' is one such accepted standard. If the members of any industry association are following any standard other than the IS/ISO/IEC codes of best practices for data protection, then the same needs to be approved and notified by the central government for effective implementation.
Another aspect affecting India's adequacy, according to the EU, is the lack of an encryption policy from the central government as required by section 84A of the IT Act 2000.	The DSCI stated that the Department of Information Technology is in the process of notifying an encryption policy designed to significantly address the information security concerns of businesses as well as consumers. *(Update: In 2015, the Indian government had published a draft encryption policy, but it was later withdrawn due to heavy criticism from the civil society and public at large about the stringent provisions related to retaining and storing data such as retaining the instant messenger messages for at least 90 days.)*
Content Principles: Onward transfer	
The EU report raised concerns on the lack of laws restricting the transfer of personal data out of India (onward transfers).	This concern has been addressed by Rule 7 of the Privacy Rules, which allows transfer of sensitive data to any company or person within or outside India only if the same level of data protection is maintained by such company or person. Further, the transfer is allowed only for the performance of the lawful contract and when the provider of information has consented to data transfer.
Content Principles: Rights of Data Subjects (access, rectification and opposition)	
The EU principles of adequacy also require the data subjects be given certain rights such as: • Informing of data subjects at the time of collection • Right to obtain a copy of all data relating to him/her that are processed • Right to rectification of those data where they are shown to be inaccurate • Right to object to the processing of the data relating to him/her	The Privacy Rules stipulate intimating (providing notice), publishing policies, and making practices transparent to the data subjects. Rule 5(6) requires companies to permit the data subjects to review the information provided to ensure that information is correct, and if found to be inaccurate or deficient, is corrected. Rule 5(7) allows the data subject to withdraw their consent at any time by writing to the body corporate.
Adequacy Assessment: Procedural and Enforcement Mechanism	
The EU assessed the procedural and enforcement mechanisms in India with regards to data protection, primarily from five perspectives (i) Independence and functions of supervisory authorities (ii) Role of courts (iii) Provision of appropriate redress to the injured parties (iv) Delivery of a good level of compliance (v) Provision of support and help to individual data subjects.	The EU observes some positives with India's procedural and enforcement mechanism but maintains that it has gaps and overall is not adequate. The Indian position, as stated by DSCI, is that the Indian courts along with quasi-judicial authorities such as the Adjudicating officer (under the IT Act 2000), do meet these requirements. Appropriate redress and support is provided to aggrieved parties and data subjects by the IT Act and the Privacy Rules, along with Article 32 of the Constitution(which rovides,extensive powers to the Supreme Court of India to enforce Constitutional rights).

Source: Data collected from the Data Security Council of India

References

[1] Nakashima, Ellen and Joby Warrick, 'Stuxnet was work of U.S. and Israeli experts, officials say', *The Washington Post*, 2 June 2012, <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html>
[2] Byres, E., A. Ginter, J. Langill, 'Tofino Security White Paper- How Stuxnet spreads – A study of infection paths in best practice systems', 21 March 2011, <http://www.tofinosecurity.com/how-stuxnet-spreads>
[3] Fitter, Pierre, 'Stuxnet attack wakes India up to threat to critical infrastructure', *India Today*, 5 September 2012, <http://indiatoday.intoday.in/story/stuxnet-cyber-war-critical-infrastructure-of-india-ntro/1/216107.html>
[4] Shearer, J., 'W32.stuxnet', 26 February 2013, <http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>
[5] Critical information infrastructure means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.
[6]Patil, Sameer, "India's vulnerable SCADA Systems", Gateway House, 17 June 2014, <http://www.gatewayhouse.in/indias-vulnerable-scada-systems/>
[7]Patil, Sameer, Interview with Indian government officials, New Delhi, December 2013
[8]Traynor, Ian, 'Russia accused of unleashing cyberwar to disable Estonia', *The Guardian*, 17 May 2007, <http://www.theguardian.com/world/2007/may/17/topstories3.russia>
[9] For the purpose of this paper, data will mean the following:

a. Government-related information and databases in electronic form including their confidential emails and contact details of officials, and national security-related information;
b. Commercial information and databases in electronic form including confidential emails, business and product development plans; and financial information such as passwords, bank account or any payment instrument details; and
c. Personal sensitive information such as physical, physiological and mental health conditions; sexual orientation; medical records and history; passwords and biometric details.

[10]Verizon, '2016 Data Breach Investigations Report', <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>, p. 10.
[11]FireEye, 'APT30 and the Mechanics of a Long-Running Cyber Espionage Operation', April 2015 <https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf>
[12] Greenwald, Glenn and Shobhan Saxena, 'India among top targets of spying by NSA', 23 September 2013, <http://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece>
[13]Mandiant, 'APT 1: Exposing One of China's Cyber Espionage Units', <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>
[14]FireEye, APT28: A window into Russia's cyber espionage operations?', 27 October 2014, <https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html>
[15]Patil, Sameer, "The 'deep web': new threat to business', Gateway House, 6 January 2015, <http://www.gatewayhouse.in/the-deep-web-new-threat-to-business/>
[16] Ministry of Home Affairs, Government of India, 'Setting up of Expert Study Group for tackling Cyber Crimes', 24 December 2014, <http://pib.nic.in/newsite/PrintRelease.aspx?relid=114013>
[17] Center for Strategic and International Studies and McAfee, 'Net Losses: Estimating the Global Cost of Cybercrime', June 2014, <http://www.mcafee.com/in/resources/reports/rp-economic-impact-cybercrime2.pdf> p. 2.
[18] 'Norton Cybersecurity Insights Report', <https://us.norton.com/norton-cybersecurity-insights-report-global>, p. 4
[19] Symantec, *'2013 Norton Report'*, <http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.pptx>
[20] Federal Bureau of Investigation, United States Department of Justice, 'Criminal Complaint against Ross William Ulbricht', 27 September 2013, <https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf>
[21]Patil, Sameer, interview with cyber security professionals, Mumbai, December 2014
[22]Weimann, Gabriel, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: US Institute of Peace Press, 2006), pp. 137-138.

[23]Candea, Stefan, Jürgen Dahlkamp, Jörg Schmitt, Andreas Ulrich and Wolf Wiedmann-Schmidt, 'How EU Failures Helped Paris Terrorists Obtain Weapons', *Spiegel Online*, 24 March 2016, <http://www.spiegel.de/international/europe/following-the-path-of-the-paris-terror-weapons-a-1083461.html>
[24]Patil, Sameer, interview with Indian government officials, New Delhi, July 2016
[25] Winter, Charlie, 'Documenting the Virtual 'Caliphate'', Quilliam Foundation, 2015, <https://www.quilliamfoundation.org/wp/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf>, p. 5
[26] Peterson, Andrea, 'Why stolen European credit card numbers cost 5 times as much as U.S. ones', *The Washington Post*, 29 July 2013, <https://www.washingtonpost.com/news/the-switch/wp/2013/07/29/why-stolen-european-credit-card-numbers-cost-5-times-as-much-as-u-s-ones/>
[27] European Union External Action, 'EU-India Joint Declaration on International Terrorism', 10 December 2010, <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/118405.pdf>
[28] European Union External Action, 'Fact Sheet: EU-India Relations', 29 March 2016, <http://eeas.europa.eu/factsheets/docs/eu-india_factsheet_en.pdf>
[29] European Union External Action, 'Joint Statement: 13th EU-India Summit, Brussels, 30 March 2016, < http://www.consilium.europa.eu/en/meetings/international-summit/2016/03/20160330-joint-statement-eu-india_pdf/>
[30] Ministry of External Affairs, Government of India, 'EU-India Summit: EU-India Agenda for Action 2020', 30 March 2016, <http://www.mea.gov.in/Images/attach/EU_India_Agenda_for_Action_post_VC.pdf>
[31]Ministry of Electronics and Information Technology, Government of India, 'Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013', 16 January 2014, <http://meity.gov.in/sites/upload_files/dit/files/GSR_19(E).pdf>
[32]Aggarwal, Varun, 'Gulshan Rai becomes first chief of cyber security; post created to tackle growing e-threats', *The Economic Times*, 4 March 2015, <http://economictimes.indiatimes.com/news/politics-and-nation/gulshan-rai-becomes-first-chief-of-cyber-security-post-created-to-tackle-growing-e-threats/articleshow/46449780.cms>
[33] Staff Reporter, 'Mumbai gets country's first 'Social Media Lab'', *The Hindu*, 17 March 2013, <http://www.thehindu.com/news/national/mumbai-gets-countrys-first-social-media-lab/article4516705.ece>
[34] Ministry of Electronics & Information Technology, Government Of India, 'About the programme', <http://www.digitalindia.gov.in/content/about-programme>
[35] Ministry of Urban Development, Government of India, 'Strategy', <http://smartcities.gov.in/writereaddata/Strategy.pdf>
[36] Department of Industrial Policy and Promotion, Ministry of Commerce, Government of India, 'IT and BPM', <http://www.makeinindia.com/sector/it-and-bpm>
[37] Council of Europe, 'Convention on Cybercrime', 23 November 2001, <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf>
[38]Csernatoni, Raluca, 'Time to Catch Up: The EU's Cyber Security Strategy', European Public Affairs, 4 March 2016, <http://www.europeanpublicaffairs.eu/time-to-catch-up-the-eus-cyber-security-strategy/>
[39] European Union, 'Shared Vision, Common Action: A Stronger Europe- A Global Strategy for the European Union's Foreign and Security Policy', June 2016, <https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_review_web.pdf>, p. 21.
[40] Europol, 'Combating Cybercrime in a digital age', <https://www.europol.europa.eu/ec3>
[41] European Union, "Shared Vision, Common Action: A Stronger Europe- A Global Strategy for the European Union's Foreign And Security Policy", June 2016, <https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_review_web.pdf>, p. 21.
[42] The Wassenaar Arrangement, 'Abut Us', <http://www.wassenaar.org/about-us/>
[43] The Wassenaar Arrangement, 'List of Dual-use Goods and Technologies and Munitions List', <http://www.wassenaar.org/wp-content/uploads/2015/06/WA-LIST-13-1.pdf>, p. 73
[44] Government of the United States, 'Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items', 20 May 2015, <https://www.federalregister.gov/documents/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items>

[45] Government of the United Kingdom, 'United Kingdom Strategic Export Controls Annual Report 2013', 17 July 2014, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/331865/9781474108232_ACCESSIBLE_v0.2.pdf>
[46] Maurer, Tim, 'Internet Freedom and Export Controls', Carnegie Endowment for International Peace, 3 March 2016, <http://carnegieendowment.org/2016/03/03/internet-freedom-and-export-controls-pub-62961>
[47] European Commission, 'Regulation (EU) 2015/2420 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items', 12 October 2015, <http://trade.ec.europa.eu/doclib/docs/2016/january/tradoc_154129.2015-2420.pdf>, p. L 340/15
[48] European Council, 'Common Military List of the European Union', 9 February 2015, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2015:129:FULL&from=EN>
[49] European Union Agency for Fundamental Rights, 'Handbook on European data protection law', 2014 <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>
[50] European Parliament and the Council, 'Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data', 24 October 1995 <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046>
[51] In April 2016, the European Council adopted a new single law on data protection i.e. Regulation (EU) 2016/679, repealing the existing Data Protection Directive 95/46/EC. This Regulation will apply from 25 May 2018 to the EU member states. The Regulation also contains adequacy requirements but this has not been examined for the purposes of this paper.
[52] It states that 'adequacy' should be assessed on a case by case basis 'in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations' particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
[53] An abridged version of this report can be found at: <http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_b4_india.pdf>
[54] European Union, 'Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)', 27 April 2016, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC>
[55] Data Security Council of India, 'Whitepaper: EU Adequacy Assessment of India', 7 January 2012, <https://www.dsci.in/sites/default/files/WhitePaper%20EU_Adequacy%20Assessment%20of%20India.pdf>
[56]Nappinai, N.S., *Technology Laws*, (Lexis Nexis: Forthcoming)
[57]Lok Sabha, 'Unstarred Question No. 3202: Legislation for Data Protection', 16 March 2016, <http://164.100.47.192/Loksabha/Questions/QResult15.aspx?qref=31968&lsno=16>
[58]Rajya Sabha, 'Unstarred Question No. 1934: Delayed talks on India EU FTA', 11 May 2016, <http://164.100.47.5/qsearch/QResult.aspx>
[59] European Trade Commission, 'Countries and regions: India' <http://ec.europa.eu/trade/policy/countries-and-regions/countries/india/>
[60] Ministry of Commerce and Industry, Government of India, 'Anand Sharma Asks EU to Declare India Data Secure', 17 October 2012, <http://pib.nic.in/newsite/PrintRelease.aspx?relid=88472>
[61]NASSCOM, 'EU-India FTA Discussions Gather Steam', <http://www.nasscom.in/euindia-fta-discussions-gather-steam?fg=235321>
[62] Ministry of Commerce and Industry, Government of India, 'Sharma and Gucht Review India-EU BTIA Negotiations', 30 May 2013, <http://pib.nic.in/newsite/erelcontent.aspx?relid=96316>
[63] This report is not in the public domain. Gateway House was informed about this report during the interview with the DSCI representatives, who have seen a copy of this report.
[64]Kulkarni, Kunal, interview with DSCI representatives, Mumbai, September 2016
[65]Kulkarni, Kunal and Purvaja Modak, interview with lawyers and DSCI representatives, Mumbai, September 2016

[66] Ministry of Law and Justice, Government of India, 'The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016', 26 March 2016, <https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf>
[67] However, concerns have been raised in respect of confidentiality and disclosure provisions in the Aadhar Act. See Hickok, Elonnai and Sinha, Amber, "Salient Points in the Aadhaar Bill and Concerns", The Centre for Internet and Society, 21 March 2016, <http://cis-india.org/internet-governance/salient-points-in-the-aadhaar-bill-and-concerns>
[68] Office of the Press Secretary, White House, 'Fact Sheet: U.S.-EU Cyber Cooperation', 26 March 2014, <https://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation>
[69] European External Action Service, 'Fact Sheet: EU-US cooperation on cyber security and cyberspace', 26 March 2014, <https://eeas.europa.eu/statements/docs/2014/140326_01_en.pdf >
[70] Department of Industrial Policy and Promotion, Ministry of Commerce, Government of India, 'IT and BPM', <http://www.makeinindia.com/sector/it-and-bpm>
[71] Project Honey Pot, 'About Project Honey Pot', <https://www.projecthoneypot.org/about_us.php>
[72] European Business and Technology Centre, 'Pune Smart City Development Corporation Limited (PSCDCL) and the European Business and Technology Centre (EBTC) sign MoU for knowledge sharing and technical cooperation', 26 September 2016, <http://ebtc.eu/index.php/information-hub/press-corner/press-releases/587-pune-smart-city-development-corporation-limited-pscdcl-and-the-european-business-and-technology-centre-ebtc-sign-mou-for-knowledge-sharing-and-technical-cooperation>
[73] European Business and Technology Centre, 'Press Release: EU - India Smart Cities Knowledge and Innovation Program', 4 December 2015, <http://ebtc.eu/index.php/information-hub/press-corner/press-releases/323-press-release-environment/577-press-release-eu-india-smart-cities-knowledge-and-innovation-program>
[74] 'EU-China Smart cities', <http://eu-chinasmartcities.eu/>
[75] European Union Agency for Network and Information Security, 'Smart Cities', <https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-cities>
[76] European Union Agency for Network and Information Security, 'Securing Europe's IoT Devices and Services', 16 October 2015, <https://www.enisa.europa.eu/events/copy_of_enisa-workshop-on-cyber-security-for-iot-in-smart-home-environments/1-enisa-securing-europes-iot-devices-and-services>
[77] U.S. Department of State, '"Joint Elements" from U.S.-EU Cyber Dialogue', 8 December 2015, <http://www.state.gov/r/pa/prs/ps/2015/12/250477.htm>
[78]Sayer, Peter, 'EU plans $2B investment in cyber security research', *Computerworld*, 5 July 2016, <http://www.computerworld.com/article/3090891/security/eu-plans-2b-investment-in-cybersecurity-research.html>
[79]Modak, Purvaja, interview with a representative of the Bombay Stock Exchange, Mumbai, September 2016
[80]Verizon, '2016 Data Breach Investigations Report', <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>, p. 10.
[81]Modak, Purvaja, interviews with representatives from the Indian private sector and Cyber Security professionals, Mumbai, September 2016
[82] Ministry of Electronics and Information Technology, Government of India, 'Information Technology Act', <http://meity.gov.in/content/information-technology-act>
[83] S., Shalini, 'Budapest Convention on Cybercrime – An Overview', Centre for Communication Governance at National Law University, Delhi, 3 March 2016, <https://ccgnludelhi.wordpress.com/2016/03/03/budapest-convention-on-cybercrime-an-overview/>
[84] Cybercrime Convention Committee, 'T-CY Guidance Note # 3, Transborder access to data (Article 32)', 5 November 2013, <https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY(2013)7REV_GN3_transborder_V11.pdf>
[85] Ministry of Communications and Information Technology, Government of India, 'Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011', 11 April 2011, <http://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf>
[86] "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities; Explanation to section 43A of the Information Technology Act 2000.

Bibliography

1. Bray, Chad and Danny Yadron, 'Nasdaq, Others, Targeted by Hackers', 26 July 2013, <http://www.wsj.com/articles/SB10001424127887324564704578627640005 24279>

2. Centre for Development of Advanced Computing, "Corporate Profile", <http://cdac.in/index.aspx?id=CorporateProfile>

3. Computer Emergency Response Team for the EU institutions, bodies and agencies, 'About Us', <https://cert.europa.eu/cert/plainedition/en/cert_about.html>

4. European Commission, 'The Directive on security of network and information systems (NIS Directive)', 28 July 2016, <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>

5. European Union Agency for Network and Information Security, 'About ENISA', <https://www.enisa.europa.eu/about-enisa>

6. Express News Service, '150 computers at Maharashtra Mantralaya attacked by Locky virus', *The Indian Express,* 26 May 2016, <http://indianexpress.com/article/mumbai/maharashtra-mantralayas-150-computers-attacked-by-locky-virus-2819393/>

7. Hickok, Elonnai, 'Leaked Privacy Bill: 2014 vs. 2011', The Centre for Internet and Society, 31 March 2014, <http://cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011>

8. High Representative of the European Union for Foreign Affairs and Security Policy, 'Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace', 7 February 2013, <https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf>

9. Hokins, Nick, ''New Stuxnet' worm targets companies in Europe', *The Guardian*, 19 October 2011, <https://www.theguardian.com/technology/2011/oct/19/stuxnet-worm-europe-duqu>

10. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India, 'Client's/Citizen's Charter', <http://www.cert-in.org.in/>

11. Kshetri, Nir, The *Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*, (Switzerland: Springer International Publishing, 2016)

12. Lee Dave, 'Global internet slows after 'biggest attack in history'', BBC, 27 March 2013, <http://www.bbc.com/news/technology-21954636>

13. Ministry of Electronics and Information Technology, Government of India, 'National Cyber security Policy 2013', 2 July 2013, <http://meity.gov.in/content/national-cyber-security-policy-2013-1>

14. Ministry of Electronics and Information Technology, Government of India, 'About MeitY', <http://meity.gov.in/content/about-dit>

15. Ministry of Electronics and Information Technology, Government of India, 'Active MoUs', <http://meity.gov.in/content/active-mous>

16. Ministry of Electronics and Information Technology, Government of India, 'Country wise status', <http://meity.gov.in/content/country-wise-status>

17. Ministry of External Affairs, Government of India, 'India-France Relations', August 2013, <https://www.mea.gov.in/Portal/ForeignRelation/India-France_Relations.pdf>

18. Ministry of External Affairs, Government of India, 'India – United Kingdom Relations', June 2015, <http://www.mea.gov.in/Portal/ForeignRelation/United_Kingdom_2015-07_27.pdf>

19. Ministry of Home Affairs, Government of India, 'Draft Bill on Right to Privacy', 29 September 2011, <http://cis-india.org/internet-governance/draft-bill-on-right-to-privacy>

20. Ministry of Law and Justice, Government of India, 'The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016', 25 March 2016, <https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf>

21. Spamhuas, 'Answers about recent DDoS attack on Spamhaus', 28 March 2013, <https://www.spamhaus.org/news/article/695/answers-about-recent-ddos-attack-on-spamhaus>