THE CENTRE FOR internet & society

A comparison of legal and regulatory approaches to cyber security in India and the United Kingdom

By **DIVIJ JOSHI**

Designed by **Saumyaa Naidu**

This report is the first part of a three part series of reports that compares the Indian cybersecurity framework with that of the U.K, U.S and Singapore.

This report compares laws and regulations in the United Kingdom and India to see the similarities and disjunctions in cyber security policy between them. The first part of this comparison will outline the methodology used to compare the two jurisdictions. Next, the key points of convergence and divergence are identified and the similarities and differences are assessed, to see what they imply about cyber space and cyber security in these jurisdictions. Finally, the report will lay out recommendations and learnings from policy in both jurisdictions.

I. The Methodology

The cyber security frameworks in India and the UK have been analysed on a number of elements keeping in mind the broad nature and the different facets of a holistic cyber security framework. The methodology for assessment has been briefly outlined below:

The first metric for comparing these jurisdictions is on the historical basis of cyber security. The impact of the internet as a crucial resource has certainly not been restricted to the developed world, despite considerable differences in technological development. However, the internet developed differently in different jurisdictions owing to their unique economic, social and political environments. This metric assesses the history of the development of 'cyber security' as a matter of regulation in order to identify the impetus for and intention behind cyber security related legislation or policy in the different jurisdictions, which would shape policy outcomes. This section briefly describes how cyber security policy was developed in response to specific social, political and economic scenarios, and after a more sophisticated understanding of cyber space and the changing nature of cyber threats had been developed. The antecedents of cyber security legislation have also been analysed to see if, and how, existing laws and policies have been adapted to cover cyber security related issues, and whether similar frameworks could be usefully adapted by either jurisdiction.

The second metric for comparing these jurisdictions is on the scope of 'cyber security' in both jurisdictions. This metric addresses three concerns –

Firstly, how is cyber security prioritised within each jurisdiction? This can be assessed from the level of sophistication and focus on the development of cyber security, in terms of allocation of resource and level of commitment.

Secondly, how are areas of concern identified? Cyber security can have several, potentially competing perspectives – economic (as in protection of businesses), social (protecting individual privacy) or sovereign (national security). Cyber security means different things for different stakeholders, who prioritize certain perspectives over others. The prevailing cyber security policy usually reflects which of these perspectives dominates political discourse.[1] For example, identification of institutions as Critical Infrastructure ("**CI**") as areas of specific concern for cyber security helps understand the perspectives on 'criticality' within each jurisdiction. Critical infrastructure identification is a fundamental component of national cyber security policy, and helps identify areas of priority when making policy.[2] Assessing criticality provides some perspective on the discursive politics of cyber security. Critical Information Infrastructure ("**CII**"), which, as the nomenclature suggests, is CI in information networks, and to which cyber security is arguably most relevant, can be assessed as structurally critical i.e., important from the perspective of the interdependence of various other systems outside of cyber space to information infrastructure. Other aspects of Cyber

[1] *http://books.sipri.org/files/books/SIPRI04BaiFro/SIPRI04BaiFro17.pdf*

[2] *http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-2006-2-27-53.pdf*

Security, such as the protection of national or religious symbols from cyber attacks, can be seen as symbolically important. Such classifications can provide important insight into the focus areas of cyber security.

Thirdly, this metric studies the typology of cyber threats identified by these countries. Identifying the source of threats and the consequences of these threats, as well as the intentions behind threats is an important factor of cyber security preparedness and can help evaluate how countries respond differently to different facets of cyber threat – for example, in making distinctions between cyber-enabled threats (those which use cyber space or computer resources for committing 'real-world' or conventional offences) and cyber-dependant threats (which specifically target the security of computer systems) and in adopting different approaches towards different kinds of actors.[3]

The third metric for comparing these jurisdictions is on cyber security governance structures. During the initial development of the Internet, the responsibility for cyber security, much like the management of cyber space, was primarily undertaken by private actors serving the interests only of their own users or networks. Gradually, it became apparent that cyber security required collaboration at multiple levels between these actors, and this gave the impetus for other non-governmental actors, such as industry bodies, to begin coordinating broader efforts towards collaborative cyber security. The formal intervention of governments in this sphere began both as a result of increased reliance of public (in the sense of government-controlled) infrastructure on cyber space, as well as the realisation that the government architecture may be best placed to maximise collaboration and coordination on cyber security.[4] These three actors – businesses, independent non-governmental bodies and government institutions, have been assessed within this metric to outline the extent to which they contribute to the overall structure of cyber security mechanisms in these jurisdictions.

As the focus of this report is primarily on government institutions and policy, this metric, in particular, analyses how and to what extent existing governmental institutions have been leveraged as well as how new mechanisms have been created in the development of cyber security mechanisms. Within the government, various agencies are responsible for different structures, yet, they must find ways of coordinating efforts at cyber security. These agencies may be classified in terms of the roles they fulfil. Policy making, co-ordination, operational agencies and private sector regulators can all play different but complimentary roles in any cyber security framework.[5] This analysis is useful to see how different cyber security concerns are addressed by the institutional framework, such as those addressed at the civilian internet and those addressed at the security infrastructure.

Given the complexity of cyber threats today, responses to these require a large degree of cohesiveness and cooperation between various actors – Harknett and Stever have described this as cooperation between the 'cyber security triad' consisting of governments, the private sector, and the engaged citizen.[6] The priorities and goals of these three actors are often not aligned, although the ultimate aim is to counter cyber threats. The private sector has historically been a major actor in cyber security, which has led to parallel institutions and mechanisms existing outside of government infrastructure. However, these solutions are usually market-oriented and often miss out critical aspects of cyber security, and therefore may play an overlapping or a complementary role with the government. The third actor, namely individuals, as end-users and end-points of the network, are also essential to

[3] *https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf*

[4] *http://web.mit.edu/smadnick/www/wp/2016-10.pdf*

[5] *https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf*

[6] Richard J. Harknett, James A. Stever, The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen, 6(1) Journal of Homeland Security and Emergency Management, 79 (2009).

maintaining cyber security, as most individuals are to some degree participants in attacks on cyber space. Therefore, policy is often framed with a view to coordinate the efforts and goals of these discrete actors towards comprehensively protecting cyber space. Measures to regulate these actors are broad, and include cyber threat reporting requirements, legal sanctions against lax security practices, standard setting by the government and information campaigns aimed at specific actors. This metric analyses how policy in these jurisdictions has regulated and engaged the private sector such as businesses and civil society and the citizenry in cyber security.

The fourth metric on which cyber security policy in these jurisdictions as been compared is on foreign policy and international commitments. Legal jurisdiction being one of the most challenging issues in the global cyber space, international cooperation in this sphere is indispensable – countries cannot solely rely on their own domestic institutions and frameworks to comprehensively tackle cyber threats. Further, domestic regulation on cyber security can also have implications in other jurisdictions. For example, data sharing requirements placed on companies that handle cross-border information in one jurisdiction could threaten data privacy and sovereignty requirements in another jurisdiction. It is therefore important to analyse how these different countries approach the task of international cooperation on cyber security. Foreign policy on cyber security reflects in membership to international organizations, stances on negotiations and membership to bilateral and multilateral treaties as well as through bilateral ties and participation in international programmes. This section analyses cyber security foreign policy in both countries.

The fifth metric is how these jurisdictions place cyber security within the charter of individual rights and freedoms on the Internet. Cyber security regulation can have far reaching implications on civil liberties, in particular on the right to privacy and the freedom of speech and expression and the freedom of organization.[7] Countries have different approaches on how these values are safeguarded in regulation dealing with cyber security, and what level of legislative or judicial oversight cyber security bodies have. This metric assesses how policy in both jurisdictions addresses these concerns and the extent to which policies are cognizant of the need to balance the requirements of cyber security with online freedoms.

II. Comparison of Cyber Security Policy in India and the UK

A. History

India

1. Social and Political Background

India's domestic social and political environment as a rapidly developing post-colonial nation has deeply shaped its approach towards cyber space and cyber security. India's capacity for cyber security was initially limited due to a lack of awareness coupled with a lack of technology to evolve adequate structures for cyber security, the latter being cemented by international technology control regimes such as the Wassenaar Arrangement.[8] Further,

[7] Gregory T. Nojeim, Cybersecurity and Freedom on the Internet, 4 Journal Of National Security Law & Policy, 119, (2010).

[8] Saikat Datta, Internet Democracy Project, Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents, (January 2016) available at *https://internetdemocracy.in/reports/cybersecurity-ig-ifp-saikat-datta/*.

cyber security policy in India has historically been aligned with sovereignty considerations, in particular, with state-sponsored terrorism as well as internal security. Aligning policy objectives with sovereignty and security concerns, cyber security has therefore mostly been approached from a state-centric perspective with the discourse being one of national security as against a broader multi-stakeholder perspective concerning social or economic aspects of cyber security.[9]

2. Legislative History

The rapid proliferation of computer technology and the internet in India only took place in the last decade, although its roots lie in the liberalisation of the Indian economy in the early 1990s. As a result, the development of regulation for cyberspace was belated. Due to the lack of widespread use of computers and the internet until the late 1990s, there was little pressure for development of laws to regulate computers and cyber space. India's overarching law for regulating information technology, the Information Technology Act, was enacted in the year 2000, and even then, did not adequately address issues of cyber security, only introducing and penalising the incidence of hacking. Thereafter, in 2004, the Indian Computer Emergency Response Team (CERT-in) was established, and has since played the dominant role in cyber security in India. The Cert-in annual reports, which provide yearly statistics of cyber attacks, provide a picture of the exponential growth in cyber threats over the last decade.[10]

Data released by the government provides some context to the increasing relevance of cyber security policy making. As per the cyber crime data for the years 2010-2013, maintained by National Crime Records Bureau (NCRB), a total of 1791, 2876 and 4356 Cyber Crime cases were registered under Information Technology Act respectively. Further, a total of 422, 601 and 1337 cases were registered under Cyber Crime related Sections of Indian Penal Code (IPC) during the same years.[11] In addition, the number of incidents reported to the CERT-In increased exponentially, from 22060 in 2010 to 96383 in 2013. These included security incidents including phishing, scanning, spam, malicious code, website intrusions etc. As per the CERT-in Annual Report for 2016, 8,311 security breach incidents were reported in the country in January 2015 alone, an increase from 5,967 recorded the previous year.

An increase in cyber-terrorism incidents, both internationally and domestically towards the end of the last decade gave an increased impetus to establish cyber security mechanisms.[12] Subsequently, the IT Act was amended in 2008 to define the role of CERT-In, and introduced penal actions against cyber-threats, including cyber-terrorism, identity theft and data protection. The 2008 amendment also introduced a system of recognizing 'Critical Infrastructure' and mechanisms for their protection. However, the development of effective cyber security infrastructure under the IT Act has been belated. The National Cyber Security Policy, which sets out policy objectives for the government was introduced only in 2013, years after cyber security was putatively recognized as an area of concern, and has not been updated since. The central agency responsible for CII protection, the NCIIPC, similarly, was only notified in 2014, after a six-year gap from its conceptualisation under the IT Act.[13]

There is some tension between cyber security and state surveillance in India. In dealing with encryption and encrypted communications, essential aspects of secure communication, the government has preferred to forgo strong encryption for easier surveillance. An example

[9] Id.

[10] *https://www.cert.org/historical/annual_rpts/*

[11] *http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Compendium-15.11.16.pdf*

[12] Saikat Datta, Internet Democracy Project, Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents, (January 2016) available at *https://internetdemocracy.in/reports/cybersecurity-ig-ifp-saikat-datta/*.

[13] *http://nciipc.gov.in/*

of this approach to encryption is the draft National Encryption Policy, precipitated by the widespread adoption of encryption by widespread instant communication technologies such as WhatsApp.[14] The draft policy regulated algorithms and key sizes that could be used for encrypted communications, and required communication services operating in India to deposit encryption keys with the Government. The effect of this policy and its outcome is analysed later.

3. Legal Antecedents

The closest antecedent to the IT Act, the Indian Telegraphs Act of 1885, has been used as a legal basis to take control of communications infrastructure (including the internet) by the Government, including for shutting down networks and intercepting communication. This law is regularly used to deny internet access to politically volatile areas,[15] although its application to issues of cyber security is not known. Prior to the introduction of the Indian Information Technology Act, India did not have existing criminal law addressing issues of cyber security, such as targeted attacks against computer infrastructure. However, existing criminal law has been used to prosecute instances of 'data theft', which includes unauthorized access to computers.[16] There are no incidents of courts interpreting common law duties of care which are owed under tort law (for example for maintaining confidence), for the protection of data or computer resources, although there may be some support for such a duty within the interpretation of the tort of breach of confidence in India.[17]

UK

1. Social and Political Background and Legislative History

The United Kingdom had widely adopted computers and made available communication infrastructure, similar to the modern internet, by the late 1980's.[18] Consequently, it was one of the first countries to adopt an act to deal with cyber security, enacting the Computer Misuse Act of 1990. The pressure for development of computer law was in direct response to the growing computer-enabled communications infrastructure and the lack of adequate legal mechanisms to prosecute domestic cyber offences such as breaches of government or private systems. In *Regina v Gold And Schifreen*,[19] the Court of Appeal and the House of Lords, both stated the inapplicability of existing penal provisions on fraud, to deal with an issue of unauthorized access to a computer. The Computer Misuse Act introduced three new criminal offences - unauthorized access to computer material, access with intent to facilitate an offence; and unauthorized modification of computer material. However, prosecutions under the Act have been surprisingly low – this may be attributed to the high penalties and the lack of civil measures available for recovering damages by private parties, making

[14] *http://www.thehindu.com/opinion/op-ed/arun-mohan-sukumar-on-indias-draft-encryption-policy/article7685128.ece*

[15] *http://indianexpress.com/article/technology/tech-news-technology/jammu-and-kashmir-social-media-ban-use-of-132-year-old-act-cant-stand-judicial-scrutiny-say-experts-4631775/*

[16] *http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Compendium-15.11.16.pdf*

[17] *https://indiankanoon.org/doc/149860325/*

[18] Leslie Haddon, The home computer: the making of a consumer electronic, 2 Science as Culture, 7 (1988), available at *http://eprints.lse.ac.uk/64559/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Haddon%2C%20L_Home%20computer_Haddon_Home%20computer_2015.pdf*

[19] [1988] 2 WLR 984, available at *http://swarb.co.uk/regina-v-gold-and-schifreen-cacd-17-jul-1987/*.

individuals reluctant to pursue such claims.[20] In 2006, the Act was amended by the Police and Justice Act, which increased punishments for the three offences, and added a fourth offence of supplying or obtaining articles for use in computer misuse offences.[21] Further, the rise of terrorism globally, coincident with the rise in computer related offences, prompted the UK to enact the Terrorism Act of 2000, which proscribes acts '*designed seriously to interfere with or seriously to disrupt an electronic system*.'[22] Under similar pressures for the development of secure infrastructure against terrorism, the polarising Investigatory Powers Act was passed in 2016, which, among other things, required communication service providers (communication applications such as WhatsApp or Viber) to ensure that messages transmitted through their services could be decrypted by security agencies. This law also gave expansive investigatory powers to UK security agencies, highlighting the tension between cyber security, surveillance and civil liberties.

Government figures indicate that cyber attackers have become a major source of criminal activity. The UK reported 2.46 million cyber incidents and 2.11 million victims of cyber crime in 2015.[23] The UK's cyber security infrastructure has also gradually become more sophisticated. At an organizational level, information security was historically a function of a wing of the Government Communications Headquarters (GCHQ), which was responsible for protecting government information systems. In parallel, organizations like the CERT-UK were established as part of the government strategy on Cyber Security, and existing bodies like the Centre for the Protection of National Infrastructure were given additional responsibilities on cyber security. In 2016, these disparate organizations were consolidated under the National Cyber Security Centre, which is the primary authority on cyber security in the UK.

2. Legal Antecedents

There are a few antecedents of data protection in the development of the tort of confidence. Under common law, applicable in the UK, a duty of care is owed to another party where there is "*a sufficient relationship of proximity*" that an act of carelessness had harmed the victim. Hypothetically, this could provide a basis for tortuous liability of a resource owner in maintaining a standard of cyber security.[24] The UK has high level protections for individual privacy, which is recognized as a human right, and also has comprehensive data protection laws in line with EU regulations for privacy. The UK's membership in the European Union has played a large role in its domestic legislation concerning cyber security. The Data Protection Act of 1998, enacted in order to comply with the EU Data Protection Directive, included provisions on the safety of personal data held by data controllers, and also penalised unauthorized access to such data.[25] With the UK set to leave the EU after the June 2016 referendum, the impact of this on its cyber security laws is still an open question. This is discussed in more detail in the section on international considerations below.

Key Findings on History

The historical context to cyber security in India and the UK has affected policy development in this area significantly. In particular:

- Cyber security has been a regulatory priority in the UK for much longer than in India, and consequently, the UK has a much better defined policy and framework for cyber security.

[20] *http://etheses.whiterose.ac.uk/2273/1/Fafinski_S_Law__PhD_2008.pdf*

[21] Police and Justice Act 2006 (Commencement No. 9), Order 2008 SI 2008/2503.

[22] *http://www.legislation.gov.uk/ukpga/2000/11/contents*

[23] *http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file*

[24] *http://www.wigleylaw.com/assets/Uploads/Legal-aspects-of-cybersecurity.pdf*

[25] *http://etheses.whiterose.ac.uk/2273/1/Fafinski_S_Law__PhD_2008.pdf*

Interestingly, however, India shared the 5th rank on the ITU's Global Cyber Security Index for 2014, which measures and ranks countries based on internal commitment to cyber security.[26]

- Both countries have struggled to adapt existing law to rapid technological developments, opting instead to develop new legislation or new institutions to focus specifically on cyber security.
- A major focus of cyber security in both countries has been on national security in light of the growing threat of organized actors, including foreign actors and terrorist organizations. Both nations have therefore attempted to expand the influence of cyber security through security legislation.
- The UK's international sphere of influence has also been exercised through its expanded cyber security capabilities, being part of the 'five eyes' surveillance alliance,[27] in stark contrast to India, which is only inching towards being a major player in cyber diplomacy.

B. Scope of Cyber Security

India

1. Prioritisation of Cyber Security and Policy Objectives

Cyber security has gradually emerged as an area of priority for Indian lawmakers following repeated security lapses within existing information structures coupled with a policy agenda of rapidly increasing digitization and increasing access to the internet.[28] However, while the focus on developing cyber security institutions has increased and spending has increased exponentially,[29] there is no long-term budgetary allocation for cyber security,[30] and most stakeholders suggest that current budgetary allocation is inadequate.[31]

Section 2(1)(nb) of the IT Act in India defines 'cyber security' as "*protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction*." This definition has also been adopted in other legislations, including the CERT-In Guidelines under the IT Act.[32] As far as legislative intent behind enacting 'cyber security' measures is concerned, this broad definition tells us very little about what 'cyber security' entails, encompassing the 'protection' of all communication and all from any form of 'unauthorized' access or use, which would also include in its scope cyber-enabled crimes which are deemed illegal, such as restrictions on speech.

The National Cyber Security Policy, 2013 (**2013 Policy**) is more illuminating as to India's policy objectives in securing cyber space, although it lacks in terms of defining tangible ways to achieve those goals. The policy notes that cyber space is a common resource used by different actors, among whom it is difficult to draw boundaries, and that cyber security has to take this perspective into account. The policy is cognizant of the broad methods involved in ensuring cyber security – identification of threats, information sharing between parties,

[26] *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx*

[27] *https://www.privacyinternational.org/node/51*

[28] *https://thewire.in/84925/aadhaar-privacy-security-legal-framework/*

[29] *http://pib.nic.in/newsite/PrintRelease.aspx?relid=113218*

[30] *https://factordaily.com/budget-2017-will-digital-india-get-cyber-security-allocation/*

[31] *http://economictimes.indiatimes.com/news/industry/tech/internet/indias-cyber-security-budget-woefully-inadequate-experts/articleshow/46036354.cms; http://www.thehindubusinessline.com/info-tech/centre-likely-to-quadruple-allocation-for-digital-india/article8241178.ece.*

[32] *https://www.dsci.in/sites/default/files/CERT-In%20Notification.pdf*

investigation and coordinated responses. The objectives of the 2013 Policy highlight the social and economic significance of protection of personal data and protecting against cyber crime, as well as the importance of protecting critical infrastructure, which could hamper the functioning of the national economy. While the policy is helpful inasmuch as it recognizes the various facets of cyber security, the policy in unhelpful in demarcating different approaches to national cyber security and spelling out how the government aims to approach these different facets, for example, how responses to cyber terrorism or attacks against critical infrastructure would be different from cyber crimes like data theft. It also fails to provide concrete goals or measures of achieving cyber security. Similar to the National Cyber Security Policy, but just as vague, is the XII Five Year Plan report on Cyber Security, for 2017 – 2022, which focuses on possible ways to achieve cyber security in a systemic manner over the plan period. The Plan Report also identifies some clear steps which can be taken as target deliverables for cyber security, however, few of these are yet operational.[33]

Cyber crime is identified as a priority in both the Five Year Plan as well as the Cyber Security Policy. Further, hacking, theft of data, computer related crimes and cyber terrorism are crimes which are prosecuted under various sections of the IT Act or the IPC and operationalized through law enforcement agencies. There is little distinction between cyber-enabled and cyber-dependant crimes, and no specific policy approach for the latter.

There is no law on data protection applicable to governmental authorities. In fact, there is little emphasis in laws on securing individual personal data held by private parties as an aspect of cyber security. Incidences of individual and consumer data protection vis-à-vis online services, are mostly left to the realm of private law, including contractual remedies. The primary umbrella tool for data protection remains a sole provision for reasonable security practices required by ‘body corporates’ under Section 43A of the IT Act, read with the Reasonable Security Practices Guidelines, which require compliance with reasonable security standards prescribed under the guidelines, such as ISO 27001 Information Security Management Standard or any other standard with government approval.

Cyber security is clearly a growing priority for India – both for government policy as well as for a private sector and a society increasingly reliant on a secure internet. While India’s cyber security framework indicates a clear need to secure socially and economically important sectors like banking and finance, energy, cyber security is identified as being particularly critical to India’s foreign policy and defence objectives.[34] Similarly, while cyber security policy acknowledges the variety of factors which could pose threats to cyber security - including foreign states, criminals, accidents or natural disasters – policy is largely focussed on tackling organized cyber threats such as terrorist groups or foreign states, which could pose a threat to national security, and as such, cyber security is not seen as an objective to achieve through a multi-lateral approach, with a heavy preference for fulfilling statist and nationalist objectives through policy. Moreover, policy in India is focussed upon improving its cyber defensive strategies rather than its cyber offensive capabilities.

2. Assessment of Criticality

The IT Act provides the basis for recognizing areas of focus for cyber security, by establishing a system for the protection of critical information infrastructure. Critical Information Infrastructure is defined under Section 70 of the IT Act as “*the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety*.” The IT Act also contemplates the National Critical Information Infrastructure Protection Centre, which was established by a Gazette of India notification on January 16, 2014. The NCIIPC Rules under the IT Act lay down the manner in

[33] *http://meity.gov.in/writereaddata/files/downloads/Plan_Report_on_Cyber_Security.pdf*

[34] *https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%2C%20IG%20%26%20IndianForeignPolicy_SDatta2016.pdf*

which the NCIIPC should perform its functions. As per the NCIIPC charter, its function is to "*take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders*." However, there is a conspicuous absence of reference to multi-stakeholder perspective, with the limited reference being towards engaging the private sector for the purposes of Human Resource development.

The scope of 'criticality' in Indian cyber security can be understood with reference to the NCIIPC Guidelines (**Guidelines**),[35] which provide a methodology to assess and rank the criticality of sectors. The Guidelines recognise national security, economy, public health and safety, as the key considerations in assessing whether the object of protection is critical. The Guidelines use the following factors to determine criticality –

1. *Functionality: This is a 'set of functions, procedure and or capabilities associated with a system or with its constituent parts. It may be viewed at two levels- Functional Uniqueness and Functional Dependency'.*
2. *Criticality Scale: This is the 'availability access, delivery and consummation of essential services'.*
3. *Degree of Complementarities: Which recognizes that the 'Failure of one system has potential to shut down other Critical Information Infrastructure relatively quickly in a cascading manner'.*
4. *Political, Economic, Social and Strategic Values: which includes 'what is held important for political stability, economic prosperity, fraternity, unity and integrity of the nation'.*
5. *Time Duration: which has 'significance in the identification and categorization of CII. The same system may or may not be critical for all the time. Systems or their constituent needs to be identified in their alignment with period'.*

This framework, while primarily focussing on the structural importance of CII, also allows for 'political, economic and social and strategic values' as considerations for criticality. Currently, the following sectors have been identified as CII - banking and financial sector; ICT and telecommunication; transportation; power; energy; the Ministries of Home Affairs, External Affairs and Heavy Industries; and Niti Ayog.[36] Apart from CII, the Act allows the 'appropriate government' to declare any computer which directly or indirectly affects the facility of critical information infrastructure to be a 'protected system'.[37] Once notified as a protected system, a CII is protected from unauthorized access or disruption by stricter laws, and comes under the ambit of 'cyber terrorism'. A number of CII have been identified as 'protected systems', including the TETRA Secured Communications Network, the UIDAI database and the Long Range Identification and Tracking System. Finance and banking systems too have been a focus of regulatory concern.

However, the broad definition of 'protected system' leads to a dilution of the objective of identifying specific focus areas for protection. For example, state governments, such as the Chhattisgarh Government,[38] have liberally interpreted these systems to include any manner of computer systems and networks.

3. Categories of Threats

The NCIIPC Guidelines provide some clarity to the approach towards the various aspects

[35] *http://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf.*

[36] *https://internetdemocracy.in/wp-content/uploads/2016/03/Saikat-Datta-Internet-Democracy-Project-Defending-Indias-CII.pdf*

[37] *http://www.orfonline.org/expert-speaks/nciipc-its-evolving-framework/*

[38] *http://www.chips.gov.in/sites/default/files/critical%20information%20eng.pdf*

of cyberspace which must be protected, and identifies physical and environmental threats to cyber security, as well as security risks caused by inadvertent software. Further, the Guidelines identify a 'Vulnerability/Threat/Risk' assessment methodology to map potential weak points in infrastructure security.

Similar to the NCIIPC, the IT Act establishes the Indian Computer Emergency Response Team (CERT-in), whose primary responsibility is to respond to 'cyber security incidents', particularly in non-critical sectors. The CERT-In rules provide a more comprehensive threat assessment. A cyber incident, as per the CERT-in Rules,[39] is defined as "*any real or suspected adverse event that is likely to cause or causes and offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity or availability of electronic information, systems, services or networks resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource, changes to data or information without authorization; or threatens public safety, undermines public confidence, have a negative effect on the national economy or diminishes the security posture of the nation.*" The Rules provide clear categories of threats and expressly prioritises them as follows:

1. Threats to physical safety of human beings;
2. Incidents of a 'severe natures' (including DDOS, spread of cyber contaminants, etc.) on the public information infrastructure.
3. Frequent incidents, such as identity theft or defacement of websites.
4. Compromise of individual accounts on multiple systems

There also exist state and sectoral CERTs, including for the army, air force, and navy; one for banking, known as FinCERT; and one for railways, known as RailCERT. However, no rigid conceptual distinction is sought to be made for different aspects of cyber security, including classifications of different actors who pose risks to cyberspace and classifications of different methods and intentions behind cyber threats. Similarly, while sectoral classifications and focus areas exist within the cyber security framework, there is little emphasis on developing a typology different cyber threats and actors and developing measures to tackle them appropriately. The CERT-In Rules, however, disown any responsibility (thus accountability) for the CERT-In to maintain cyber security or adequately respond to the same.

UK

1. Prioritisation of Cyber Security and Policy Objectives

Cyber security is identified as a major (Tier 1) threat to national security, and one of six areas of priority in the national security context, since at least 2010,[40] where it finds mention in its Strategic Defence and Security Review, an annual document outlining the key strategies for the protection of national security to be pursued by the Government.[41] There is a specific cabinet post for cyber security, under the Cyber Security and Information Assurance Office and the Cabinet Office, which supports the Prime Minister, also focuses on Cyber Security, and releases the five-year National Cyber Security Strategy (**Strategy**), which was first introduced in 2011.[42]

[39] *https://www.dsci.in/sites/default/files/CERT-In%20Notification.pdf*

[40] *https://www.export.gov/article?id=United-Kingdom-Cyber-Security*

[41] *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/575378/national_security_strategy_strategic_defence_security_review_annual_report_2016.pdf*

[42] *https://www.ncsc.gov.uk/content/files/protected_files/document_files/National%20Cyber%20Security%20Strategy%20v20.pdf*

The Strategy is the primary policy document setting out the UK government's five-year plan to counter cyber threats. Among other things, the Strategy identifies areas of core concern, develops new institutions focussed on cyber security, and specifies a long term budgetary allocation for cyber security. The UK's cyber security strategy for the years 2016-2021 defines cyber security as the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.[43] Similar to the definition under the Indian IT Act, cyber security is focussed on 'information systems' which includes physical infrastructure and 'associated infrastructure', but also includes misdirection of services provided by these information systems within its scope. From a budgetary allocation of £860 Million from the previous five-year strategy, the Government now plans on investing a sum of £1.9 Billion over these five years.[44]

The Strategy clearly identifies three primary stakeholders in cyber security – individuals, businesses and organizations, and the Government itself. It stresses the importance of a secure internet and cyber space to the economy and recognizes that regulation for cyber security is complementary to the development of cyber security in the private sector, and to address market failures when it comes to cyber threats.

While terrorism and foreign actors, similar to in India, have been the basis for the development of stronger cyber security mechanisms with a focus on national security, the Strategy attempts a balance between national cyber security concerns and economic and individual concerns. While it identifies cyber security as important to the UK's defensive capabilities and identifies that it can pose a threat to national security, the approach balances these considerations with the concerns posed by private sector insecurity and individual data protection. The sovereign-focus of the Strategy reflects in its aim to develop indigenous cryptographic capabilities.[45] Further, offensive cyber capabilities are an area of focus in UK's defence policy, which is charted in the National Offensive Cyber Programme, to help attain the UK's goals of deterrence through developing offensive cyber capacities.[46]

At the same time, UK policy relies heavily on industry and industry cooperation, both in the delivery of cyber defence (for example, through communication intermediaries), the creation of better standards and intelligence sharing. However, the Strategy is mostly reliant on market forces for the same, and does not contemplate private sector regulation such as standard setting or reporting requirements, for improving cyber security.

The protection of government data is a priority,[47] with specific bodies constituted for and policies directed towards this aspect of information protection, and a clear classification scheme for the protection of confidential government data,[48] which is markedly different from the Indian approach, where government data protection lacks a clear policy. However, while there is a comprehensive data protection legislation as well as laws which recognize privacy as a human right, there is little mention of individual privacy and data protection as a priority in national cyber security policy.

[43] *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf*

[44] *https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy*

[45] *https://www.cfr.org/blog-post/four-takeaways-new-uk-cybersecurity-strategy*

[46] *http://researchbriefings.files.parliament.uk/documents/POST-PN-0554/POST-PN-0554.pdf*

[47] *http://webarchive.nationalarchives.gov.uk/20100304041448/http:/www.cabinetoffice.gov.uk/media/328380/protecting-information.pdf*

[48] *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf*

2. Assessment of Criticality

This balance is also reflected in the UK's identification of CI and the protection measures for the same. The strategy identifies that, apart from government infrastructure, the systems of media organizations, major businesses, data holders and similarly places private organizations can also have a major impact on the bearing on the lives of UK citizens, the stability and strength of the UK economy, or the UK's international standing and reputation.

There is no statutory definition of CII in the UK. However, Government policy documents have defined CII as any IT systems which support key assets and services within the national infrastructure.[49] The Centre for the Protection of National Infrastructure (**CPNI**) was the primary agency responsible for the critical infrastructure, until the recent creation of the National Cyber Security Centre, a body tasked with being an interface between industry and the government, for 'advise, guidance and support' on cyber security. In the interests of national security, the UK does not make its Critical Infrastructure publicly known, however, the CPNI identifies 13 sectors within UK, including chemicals, civil nuclear communications, defence, emergency services, energy, finance, food, government, health, space, transport and water as being critical sectors.[50]

3. Categories of Threats

There is no clear typology of threats within the UK cyber security strategy. The strategy's basis of threat assessment is not entirely clear, however, it does identify specific areas of concern and frames these threats and actors within a specific typology, unlike its Indian counterpart. In particular, the strategy identifies cyber-criminals, terrorists, hacktivists, state-sponsored hackers and 'script kiddies' as threats. Further, the strategy identifies areas of concern from a vulnerability perspective, including lack of training, an expansion of insecure devices and the ready availability of hacking capabilities. The UK's approach towards CII recognizes the need to protect the integrity of CII from both physical threats as well as electronic attacks.

The national strategy recognizes cyber crime as a major aspect of cyber security and recognizes two distinct aspects of cyber crime, as being either cyber-dependant or cyber-enabled crimes. The National Cyber Crime Assessment recognizes that the majority of cyber crime incidents emanate from organized cyber crime groups, a majority of which are located outside the jurisdiction of the UK. The Computer Misuse Act penalises the unauthorized access to computers in various situations, while criminal law also recognizes the use of computers in the commission of traditional offences.

Key Findings on Scope of Cyber Security

- India and the UK both identify cyber security as a national priority. Both countries have a forward-looking road map to address cyber security holistically, through their national cyber security policies. However, there are significant gaps in actualising cyber security measures. In India, for instance, cyber security initiatives are hobbled by the lack of a fixed and recurring budgetary allocation.
- Both jurisdictions primarily assess cyber security from a national security perspective, although the UK has a larger emphasis on multi-stakeholderism and is more collaborative in its approach.
- Threats to cyber security are more clearly identified in UK policy, which identifies various actors/circumstances which could pose a threat. The development of a threat typology is not as apparent in India.
- The UK prioritises government data protection in its policies, while this emphasis is missing specific mention in India.

[49] *https://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf*

[50] *https://www.cpni.gov.uk/critical-national-infrastructure-0*

- In terms of military policy, the UK places a strong emphasis on cyber offensive capabilities, while India concentrates solely on its defensive capabilities.

C. Cyber Security Structures

India

As assessed in the previous section, cyber security policy in India is largely a unilateral process centred around the role of the state. This has resulted in a structural framework which largely emphasises the Government's role in cyber security, towards achieving the specific cyber security objectives of national security, defence and other critical areas identified by the Government. The lack of a multi-lateral approach or support for engaging the private sector or the citizenry has similarly resulted in few organizational mechanisms which interface primarily with the private sector or individuals.

1. Cyber Security Industry and Public-Private Cooperation

In the absence of a strong cyber security framework, the onus of private information security is often left to the user. Given the legal restrictions imposed on importing crucial cyber security technology, and India's technological gulf with developed countries, the Indian cyber security industry is integral to the cyber security landscape. The cyber security industry in India is fast maturing due to the rapid pace with which digitization is being adopted, both as a matter of policy and otherwise. The industry was estimated to be worth around USD 1.12 billion in 2016 and is expected to grow strongly, according to a report by research firm Gartner.[51] A large sphere of influence on policy comes from industry bodies such as the Data Security Council of India (DSCI) and the National Association of Software and Services Companies (NASSCOM), which collaborated to jointly set up a cyber security taskforce, with the aim of developing cyber security solutions for the private sector.[52] There are other industry bodies with their specific focus, all of which have some influence on private sector cyber security, including the Confederation of Indian Industry (CII), Federation of Indian Chambers of Commerce and Industry (FICCI), Association of Unified Telecom Service Providers of India (AUSPI) and Cellular Operators Association of India (COAI). These actors largely operate independently, and their functions include setting industry standards and self-regulation. Industry frameworks often run in parallel with governmental policy and suggest best practices beyond regulatory compliances.

There is no formal framework for consulting industries and associations like the ones described above, nor any mechanism for certification of industry standards (the IT Act currently endorses the ISO 27001 InfoSec standard).[53] Political lobbying in India is not regulated and consultative initiatives are largely on an ad-hoc basis. The Joint Working Group (JWG) on Cyber Security,[54] is one such initiative, which aimed to set up an institutional framework for cyber security collaboration between the private and public sphere. However, most recommendations of the JWG report[55] have not been operationalized. Similarly, the JWG as well as the collaboration between Indian and US industry associations mooted Information Sharing and Analysis Centres (ISAC), which are crucial for sharing information and jointly collaborating against cyber threats, which have not have any formal recognition.[56] Apart from

[51] https://www.gartner.com/newsroom/id/3430717

[52] https://www.dsci.in/taxonomypage/1182

[53] https://www.iso.org/isoiec-27001-information-security.html

[54] http://pib.nic.in/newsite/mbErel.aspx?relid=89361

[55] http://pib.nic.in/newsite/printrelease.aspx?relid=88442

[56] http://www.mea.gov.in/bilateral-documents.htm?dtl/6014/indiaus+cyber

a single ISAC for the finance sector, set up at the Institute for Development and Research in Banking Technology, there are no ISAC's set up by the Government of India.[57] The fact that these plans towards collaborative efforts have received little regard in the Indian cyber security institutional framework are testament to the fact that cyber security is largely state-centric and unilateral. One area where the private and public sector do meet is on supply of cyber-security technology and services capabilities. The Government has empanelled 57 organizations to conduct security auditing of its cyber security practices.[58]

2. Institutional Framework

Within the Government, there are a number of institutions which are responsible for sometimes intersecting aspects of cyber security.[59] There is no clear primary body responsible for developing cyber security policy. This responsibility is divided among the newly created Ministry of Electronics and Information Technology (which developed the National Cyber Security Policy), the Home Ministry (in charge of internal security, including intelligence agencies), and the National Information Board and National Security Council, responsible to the Prime Minister's Office (under the office of the National Security Advisor). The lack of a formal inter-governmental information sharing mechanism also damages collaboration on these issues between government bodies. The task of operationalizing cyber security initiatives falls on a mix of law enforcement agencies and newly created cyber security organizations, like the CERT-In and NCIIPC. Similarly, there is no single co-ordinating agency responsible for co-ordinating efforts towards cyber security in India. The National Information Bureau is, however, in the process of setting up such an agency in the form of the National Cyber Coordination Centre, which is due to become operational in June, 2017, and is expected to fulfil the role of a central coordinating agency for law enforcement and security purposes in cyber space also incorporating the functions of the CERT-In within its mandate.[60] Similarly, a National Cyber Crime Coordination Centre has also been mooted, but not implemented.[61]

The CERT-In, besides being the primary incident response agency for non-critical threats, is also the central agency responsible for information collection on cyber security incidents and also to monitor non-compliance with cyber security directions under the IT Act, and its mandate is broad enough for it to investigate and respond to potentially any manner of cyber security concerns, while the NCIIPC's function is limited to the identification and protection of CII. The CERT-In is obligated to convey cyber security incidents relating to critical sectors, to the NCIIPC.

3. Regulatory Framework for Individuals and Corporations

In lieu of collaborative efforts towards improving cyber security, the private sector is sought to be regulated through the imposition of certain security standards and reporting requirements. Rule 3(9) of the Intermediary Guidelines Rules contains a reporting requirement for all intermediaries. The RBI Guidelines on Cyber Security, also mandate banks

[57] *http://pib.nic.in/newsite/PrintRelease.aspx?relid=112078*

[58] *http://loksabha.nic.in/Members/QResult16.aspx?qref=44417*

[59] For a snapshot of the various governmental actors involved in cyber security in India, see *https://internetdemocracy.in/watchtower/*.

[60] *http://indianexpress.com/article/business/business-others/cyber-security-coordination-centre-to-be-set-up-ravi-shankar-prasad-3008887/*

[61] *http://www.orfonline.org/expert-speaks/policing-cyber-crimes-need-for-national-cyber-crime-coordination-centre/*

to report ‘unusual cyber security incidents’,[62] and require banks to meet certain baseline standards for their cyber security mechanisms.[63] Similarly reporting requirements for specific cyber security incidents (as set out in the CERT-in Rules) are within the mandate of the CERT-In to enforce, which are applicable to every service providers, intermediaries, data centres or body corporates, which encounter specific kinds of cyber security incidents.[64] Besides this, telecom (UASP)[65] and ISP licenses impose network security requirements upon private operators, however, these are too vague to effectively regulate, for example, the requirement to ‘not use any hardware/software which are identified as unlawful and/or render network security vulnerable.’[66] Recently, guidelines have also been released for frameworks for cyber security resilience for insurance companies.[67] As discussed previously, the only general mandate for private information security practices which is applicable to all incorporated bodies, is as per Section 43A of the IT Act and the Rules made under it.

There are also some initiatives focussed on improving cyber security awareness and providing tools to businesses and to individuals to proactively deal with cyber threats. The cyber swachhta kendra set up by CERT-in, a botnet analysis centre set up for the benefit of end-users, is one such example.[68] One major policy goal on which the private sector has been engaged is the development of indigenous cyber security technical capabilities as well as the spread of information security awareness, for which purpose projects like the Information Security Education and Awareness project have been floated. However, cyber security awareness among individuals and the private sector appears to be lacking, compared to the pace of growth of cyber threats,[69] and a similar lack of cyber security expertise and human resource capabilities exists in the private sector.[70]

UK

1. Cyber Security Industry and Public-Private Cooperation

The UK has a diverse cyber security community, with active participation from individuals, industry, government and civil society. The UK has a maturing cyber security industry, with a well established market in the UK.[71] A number industry bodies exist with a core focus on cyber security, such as TechUK, an industry body representing around 900 companies in the high technology industry.[72] Apart from this, there are various multi-stakeholder initiatives which aid in policy development. The Information Assurance Advisory Council is one such organization which works closely with the UK government in developing and implementing

[62] *https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0*

[63] *https://rbidocs.rbi.org.in/rdocs/content/pdfs/CSFB020616_AN1.pdf*

[64] As per Rule

[65] *http://www.dot.gov.in/sites/default/files/as-iii_2.pdf?download=1*

[66] Clause 34.25 *http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf*

[67] *https://www.irdai.gov.in/ADMINCMS/cms/frmGuidelines_List.aspx?mid=3.2.2*

[68] *http://www.cyberswachhtakendra.gov.in/*

[69] *http://indianexpress.com/article/technology/tech-news-technology/india-lags-in-cyber-security-preparedness-and-awareness-experts-4482589/*

[70] *http://www.thehindubusinessline.com/info-tech/india-lagging-in-cyber-security-awareness/article9046626.ece*

[71] *https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf*

[72] *http://www.techuk.org/*

cyber security policy.[73] The UK government also works on developing and funding research in cyber security with businesses, through schemes like the CyberInvest cooperative investment scheme.[74]

There is an emphasis on the development of the indigenous cyber security industry in the UK policy. Initiatives like the Cyber Essentials Scheme are soft pushes towards standardisation of cyber security procedures and compliances. Through the Cyber Essentials Scheme, for example, the UK government aims to encourage cyber resilient frameworks through self-certification, which is also one of the conditions for businesses being empanelled for certain government contracts.[75] Another examples is the CBEST Vulnerability Testing Framework, which helps certain institutions at the core of the UK's financial sector, to identify areas where the financial sector would be vulnerable to sophisticated cyber-attack.[76] There also exists an institutional framework for information sharing with the private sector through the Cyber Information Sharing Partnership.[77] There is a clear distinction of roles and responsibilities of various actors, while the need for information sharing and coordination across various arms of the government is also recognized.

2. Institutional Framework

There is no umbrella legislation which governs information technology or cyber security in the UK, and its various agencies operate under distinct legislative mandates, such as the Civil Contingencies Act of 2004, or the Security Services Act of 1989.[78] Therefore, executive agencies tasked with maintaining cyber security have a great degree of flexibility in developing different approaches towards cyber security. This is in some contrast to India, where organizations which have been created specifically to counter cyber threats have been created through legislation. The Office of Cyber Security was formed in 2009 and became the Office of Cyber Security and Information Assurance (**OCSIA**) in 2010. The OCSIA is both responsible for developing and coordinating cyber security policy across various wings of the UK government, and also works in tandem with the private sector for information exchange and standard setting. The OCSIA, among other responsibilities, identifies areas of strategic importance and is responsible for budget allocation across various initiatives undertaken by the UK.

The National Cyber Security Centre (NCSC) is the authoritative agency for implementing cyber security policy. It is responsible for advising on and coordinating cyber security response across the government and industry. The NCSC, set up in 2016, incorporates the roles and functions of the Communications-Electronics Security Group, which was the intelligence wing of the UK National Security agency, the GCHQ, and is also in charge of the functioning of the CERT-UK, as well as the Centre for Cyber Assessment and the cyber-related functions of critical infrastructure protection which were undertaken by the Centre for the Protection of National Infrastructure. The fact that the NCSC is one of two wings of the GCHQ, an agency whose primary responsibility is towards national security, is indicative of the national security emphasis in UK policy.[79] Cyber crime investigation and prosecution is operationalized through the National Cyber Crime Unit of the National Crime Agency, which coordinates

[73] *http://www.iaac.org.uk/about/*

[74] *https://www.gchq.gov.uk/press-release/%C2%A365-million-cyberinvest-scheme-boost-world-class-uk-cyber-security-research*

[75] *https://www.gov.uk/government/publications/cyber-essentials-scheme-overview*

[76] *http://www.bankofengland.co.uk/publications/Pages/news/2014/088.aspx*

[77] *https://www.ncsc.gov.uk/cisp*

[78] *http://www.legislation.gov.uk/ukpga/2004/36/section/35*

[79] *https://www.gchq.gov.uk/who-we-are*

cyber crime response and prevention efforts across law enforcement. While there is no cyber security command within UK national security forces, the military reserves include the cyber security reserve forces, which works within the Ministry of Defence and the Joint Forces Command and is responsible for national security in cyberspace. which is part of the Ministry of Defence, Cyber defence capabilities for the military are operationalized through the Ministry of Defence CERT. The creation of the NCSC as a central coordination agency has also been an important step towards realising the potentials of information sharing and a macroscopic perspective on cyber security issues.[80]

3. Regulatory Framework for Individuals and Corporates

The UK adopts a light-touch regulatory approach towards individuals and corporates, so far as their legal responsibilities towards cyber security are concerned. The UK government publishes advisories on best practices which can be implemented by private parties.[81] However, there is no requirement for adherence to these standards, although the industry is seen as generally compliant with best practices in cyber security, driven by market and reputational risks.[82] The light touch private sector regulation is also reflected in the absence of general mandated reporting requirements. However, for certain sectors, such as the financial sector regulated by the Financial Conduct Authority,[83] there are specific obligations for complying with cyber security measures as prescribed in law. While reporting requirements exist among specific sectors, particularly for critical infrastructure, information disclosure remains voluntary. As far as individuals are concerned, UK policy mostly focuses on data protection regulation and cyber crime targeted at individuals. There are also mechanisms in place for spreading awareness among individuals in society at large, and specific skill development programmes to increase cyber security capabilities.[84]

Key Findings on Cyber Security Structures

- There are important industry and civil society stakeholders in both India and the UK. However, in terms of organizations focussing on cyber security, the UK has a much more robust cyber security society than in India, with industry bodies and civil society being important stakeholders in developing policy as well. This consultative framework could possibly be the reason for the UK adopting a light-touch regulation towards industry standards and reporting requirements. Further, both jurisdictions have programmes and structures aimed at skill development, although the UK places a greater emphasis upon cyber security awareness.
- Two primary institutional actors emerge as far as operationalization of cyber security is concerned. Both jurisdictions specifically account for critical infrastructure protection (NCSC in the UK and the CIIPC in India) and emergency response (CERT-UK and CERT-In). The UK does not have a specific cyber security legislation under which these authorities have been set up, in contrast to the IT Act in India, which governs their functioning.
- There is an absence of a central coordinating organization in India, which is a function fulfilled by the UK National Cyber Security Centre. However, the proposed National Cyber Coordination Centre is expected to fulfil this role in India.

[80] *https://www.ncsc.gov.uk/*

[81] *https://www.ncsc.gov.uk/guidance*

[82] *https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf*

[83] *https://www.handbook.fca.org.uk/handbook/SYSC/3/2.html*

[84] *https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf*

D. International Considerations

India

Cyberspace has emerged as important foreign policy concern in India. As far as major international commitments are concerned, India has not acceded to the Budapest Convention, the most comprehensive international commitment on cyber security issues, primarily due to its absence during negotiations.[85] Further, given the strong emphasis on state sovereignty in India's foreign policy, including in its cyber security policy, there is no defence related international collaboration on cyber security issues.[86] However, cyber security has emerged as an important talking point for certain international organizations of which India is a member, for example, the ITU-IMPACT group and the Council of Security Cooperation in Asia Pacific (CSCAP). India's role in the development international cyber security has also been noted through its acceptance into the UN Group of Governmental Experts on IT, and with the helm of the Global Conference on Cyber Space (GCCS) being handed over to the Indian government.[87]

Bilateral coordination on issues of cyber security has emerged as a major international foreign policy objective. In particular, Indian cyber security policy is highly influenced by its bilateral ties with the USA.[88] Cyber security had emerged as a focus of bilateral concerns in the face of the 'war against terror' and international security concerns. Further, technology and capability sharing partnerships with US security and intelligence agencies, of which India was a major beneficiary, has led to cyber security institutions being modelled on their US counterparts, like the CERT-In.[89] Further, there is cooperation among industry bodies in the US and India to set up private institutions for improving cyber security and information sharing.[90]

Given India's tensions with its major neighbouring states, Pakistan and China, regional cooperation on security issues is a complex issue. However, cyber security has emerged an important policy agenda in multi-lateral regional associations such as the ASEAN and the Shanghai Cooperation Organisation. Further, CERT-in is a member of international agencies coordinating on information sharing and emergency response in cyber security, such as the Asia Pacific CERT.[91] However, cyber security policy is concentrated on cooperation with the US, rather than regional or multi-national cooperation. Besides this, India has bilateral ties on improving cyber security within countries including the UK, Malaysia, Singapore and Russia.[92] These bilateral efforts are aimed at improving cross-border investigation and prosecution of cyber security incidents.

With its implicit support for multi-stakeholderism in internet governance through the support of the IANA transition, India has attempted to chart a different course in its foreign policy.[93] However, even here, India's proposals in this regard have maintained a largely sovereign and state-centric basis.

[85] *http://www.orfonline.org/expert-speaks/india-and-the-budapest-convention-why-not/*

[86] *http://pib.nic.in/newsite/PrintRelease.aspx?relid=113218*

[87] *https://thewire.in/108713/cold-war-code-war-india-needs-ready/*

[88] *https://thewire.in/42021/the-long-and-winding-road-to-us-india-cyber-cooperation/*

[89] *http://www.datacenterdynamics.com/content-tracks/security-risk/india-us-sign-another-agreement-on-cyber-security-cooperation/97606.fullarticle*

[90] *https://internetdemocracy.in/reports/cybersecurity-and-india-us-bilateral-ties-a-very-brief-history/*

[91] *https://www.apcert.org/about/structure/members.html*

[92] *https://internetdemocracy.in/2015/12/with-or-without-us-bilateralism-india-cybersecurity-policies/*

[93] *https://internetdemocracy.in/2015/09/opportunism-or-glasnost/*

UK

The UK's Cyber Security Strategy recognizes that cyberspace has a necessarily international character and places special emphasis on 'international action' to prevent cyber attacks. Two distinct facets of foreign policy on cyber security are of note. Firstly, the UK emphasises international coordination with like-minded international partners. To this end, it has ratified the Budapest Convention on Cyber Crime, which mandates specific requirements for preventing cyber threats for each treaty member. Further, the UK has several bilateral agreements with countries including the United States of America,[94] China,[95] and India,[96] among others. A second major aspect of foreign policy is the development of offensive cyber capabilities and first-strike capabilities, which may be used for deterrence or 'operational purposes' as identified in the national strategy.[97]

UK foreign policy formally supports the multi-stakeholder governance model for cyber space, which is explicitly mentioned in policy, and is apparent from the UK's lead in organizing the Global Conference on CyberSpace, which is an annual multi-stakeholder conference on cyberspace issues held since 2011.[98] However, cyber security issues remain a national security priority and consequently, are largely state-centric.

The UK's membership in the European Union also determines its domestic strategy in relation to cyber security, to some extent. The EU directive on data protection is applicable to the UK and informs UK law, which is soon to be replaced by the General Data Protection Directive. The GDPR requires, among other things, compliance with comprehensive data security mechanisms and general breach reporting obligations, which are missing under current UK law. Similarly, the Directive on security of network and information systems (NIS Directive) is also required to be implemented by member states by 2018, and is the first pan-European directive specifically addressing cyber security. The directive mandates, among other things, emergency response requirements and information sharing and coordination among member states. However, with the UK set to leave the EU by 2019, the effect of EU directives (which it will be required to incorporate prior to 'brexit'), and the negotiation of the UK government and industry to comply with EU norms relating to cyber security is still unknown.[99]

Key Findings on International Considerations

- Both jurisdictions support a multi-stakeholder model for internet governance in international forums. However, India's advocacy for such a model is a more recent development, and is not made out from its general emphasis on sovereign concerns. The UK, on the other hand, has been quite pro-active in engaging with the multi-stakeholder model, even where cyber security is concerned.
- India and the UK both regard bilateralism as an important foreign policy tool for cyber security concerns. India relies primarily on bilateral soft ties and partnerships, while the UK is a member of the Budapest Convention on Cybercrime, which emphasises binding international commitments.

[94] *https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation*

[95] *https://www.gov.uk/government/publications/china-uk-high-level-security-dialogue-official-statement/china-uk-high-level-security-dialogue-communique*

[96] *http://www.mea.gov.in/bilateral-documents.htm?dtl/27584/indiauk+joint+statement+during+the+visit+of+prime+minister+of+the+united+kingdom+to+india+indiauk+strategic+partnership+looking+forward+to+a+renewed+engagement+vision+for+the+decade+ahead*

[97] *http://www.economist.com/news/britain/21709603-online-attacks-foreign-powers-will-be-met-kind-vows-government-britain-flexes-its*

[98] *https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement*

[99] *https://www.twobirds.com/en/news/articles/2016/uk/brexit-data-protection-and-cyber-security-law-implications*

E. Civil Liberties Considerations

India

There has always been considerable tension among security concerns and civil liberties, and cyber space has provided one more battleground for this. Cyber space has exacerbated these tensions by allowing security concerns to be deeply integrated within civilian use of the internet and cyberspace. In India, organizations which are involved in various aspects of cyber security are also involved in intelligence and national security. Consequently, the issue of privacy and surveillance has emerged as a major flashpoint in cyber security policy. Section 69B of the IT Act, for example, allows the government to order the monitoring and decryption of information on the internet in order to counter the spread of any 'cyber contaminant'. Under this Section, CERT-In has carte blanche to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.[100] The proposed National Cyber Coordination Centre is also likely to have widespread surveillance powers.[101]

Indian policy recognizes the importance of cyber security in promoting sovereign or economic concerns, but makes no explicit reference to the role cyber space plays in the promotion of civilian liberties and freedom of speech and organization. Consequently, cyber security policy is rarely framed with a view to benefit civilian privacy or data protection, as outlined above. This aspect also comes into focus when security concerns clash with civil liberties. For example, the draft national encryption policy (discussed above) did not heed privacy and civil liberties concerns, instead favouring national security and surveillance mechanisms. This disregard is a necessary outcome of the unilateral approach towards cyber security governance framework where important public stakeholders are not included in the negotiation of policy. Further, the various legislative and executive mechanisms for decryption of information, or monitoring of online content, have no direct judicial oversight or any form of public oversight,[102] and are also not amenable to the Right to Information Act.[103] In fact, some, such as the surveillance mechanisms under the ISP license, or the scope to monitor information under the Intermediaries Guidelines Rules, are also sufficiently far removed from a direct legislative mandate for mass surveillance.

UK

The National Cyber Security Strategy for the UK notes that it shall apply core values as a guiding principle in implementing policy. These core values include democracy, the rule of law, liberty, open and accountable governments and institutions human rights and freedom of expression. Apart from this, the protection of individual privacy is also a fundamental principle of the policy. The UK Foreign Secretary's 'international norms of conduct' in cyber space also include these fundamental freedoms.[104] However, regulations or policy initiatives do not directly address how they incorporate such norms.

UK policy indicates a preference towards choosing values in favour of national security concerns over civil liberties concerns. The Investigatory Powers Act, 2016, for example, requires all communications providers to ensure that there are backdoors for encrypted

[100] *http://meity.gov.in/writereaddata/files/69B%20Notification%20-April%202016.pdf*

[101] *http://www.hindustantimes.com/india/india-s-cyber-protection-body-pushes-ahead/story-4xa9tjaz6ycfDpVg95YqPL.html*

[102] *http://sflc.in/surveillance-is-there-a-need-for-judicial-oversight/rti*

[103] *http://cis-india.org/internet-governance/blog/policy-brief-oversight-mechanisms-for-surveillance*

[104] *https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf*

content, which can be accessed by law enforcement agencies in the UK.[105] However, the interception and monitoring powers of UK law enforcement do need to pass muster of a quasi-judicial body set up (as a secret court) to issue warrants for interception and monitoring of communications.[106]

Key Findings on Civil Liberties

- The UK and India both prioritize security concerns over civil liberties concerns, which is most apparent in how both countries address the issue of cyber security and surveillance.
- While UK policy makes an explicit commitment to protecting fundamental freedoms and core values, this does not find mention in Indian policy, although it may be implicit in policy addressed at individual data protection and improving ease of access to cyberspace.
- The UK has stronger judicial oversight mechanisms for monitoring and interception of communications for cyber security than under Indian law, where the oversight mechanisms are mostly within the executive branch.

III. Conclusion

A comparison of cyber security policies across India and the UK reflects several common threads in some areas and significant divergence in others. The differences in approaches can largely be attributed to differing circumstances in both countries. However, despite a significant gap in terms of historical access to technology and resources to deploy towards protecting cyber space, India has, over the last two decades, increasingly emphasised cyber security as an important policy concern. The UK has fairly developed processes and systems, and cyber security has been a policy concern for considerably longer than in India. Naturally, the UK cyber security framework is more comprehensive and cohesive than in India. However, using the indicators in the Global Cybersecurity Index, India is not significantly far off from the UK cyber security commitment and development is concerned.[107] This may also partially be a cause of both countries being unable to apply pre-existing laws to address new situations in cyberspace.

Policy in both nations is approached from a sovereignty perspective, i.e. from the frame of national security agendas. Similarly, intelligence and defence institutions remain deeply involved in cybersecurity in both jurisdictions. However, the identification of actors, threats and aims and objectives of the cyber security policy differs considerably. The UK is considerably more open to multi-stakeholder input in moulding its policies, while cyber security in India remains bifurcated between private initiatives and government initiatives, which tend to focus on national security concerns. The UK's embrace of multi-stakeholder principles should be adopted in Indian policy, which has already recognized the importance of multi-stakeholderism in the international context. The Indian government can do a lot more in terms of spreading awareness about cyber security and developing indigenous cyber security research. India could also usefully employ the soft approaches taken by the UK to incentivise businesses to comply with security best practices without necessarily mandating strict regulation, like the implementation of the cyber essentials scheme.

Fundamental aspects of cyber security infrastructure remain common across both jurisdictions, such as the establishment of emergency response agencies and critical information protection. Besides these, there are several disparate institutions handling

[105] *https://arstechnica.co.uk/tech-policy/2017/05/investigatory-powers-act-legal-analysis/*

[106] *https://www.theguardian.com/commentisfree/2015/nov/04/internet-surveillance-judiciary-theresa-may-web-browsing*

[107] *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf*

disparate mandates on cyber security. For this reason, it is critical that the proposed National Cyber Coordination Centre, on the lines of the UK's National Cyber Security Centre, as a one stop shop for cyber security-related concerns. Further, the roles of each organization must be clearly demarcated to avoid overlap and ensure accountability.

India's international approach to cyber crime seems to have been held up for diplomatic reasons. The Budapest Treaty establishing international cooperation on cyber security and cyber crime, of which the UK is also (albeit belatedly) a member, is an important aspect of international coordination on cyber security issues, which would be much tougher to negotiate on a bilateral basis. It is recommended that India revisit the possibility of entering into international commitments given the large degree of cooperation required for investigating cyber threats.

Indian cyber security is also un-rooted in fundamental principles on which such legislation should be based. The fundamental principles UK policy recognizes ensures that the main strategy for cyber security keeps in mind aspects of civil liberties and individual's concerns in the internet as a shared resource. While this may place constraints on the government's hold over cyber security, security policy must be adapted towards upholding civil liberties, and not the other way around. The UK however, in its actions, needs to balance its national security concerns with civil liberties concerns around privacy and surveillance.