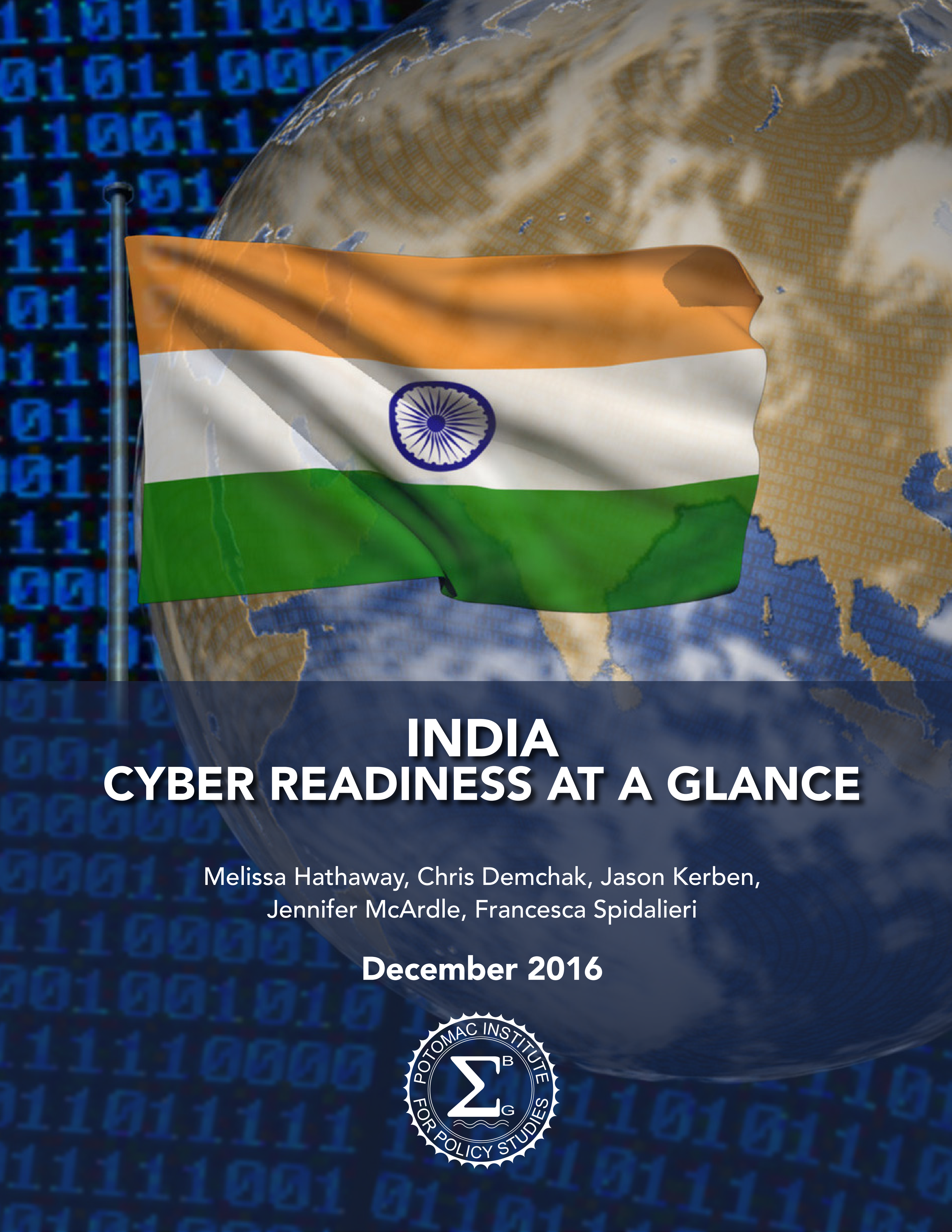


INDIA
CYBER READINESS AT A GLANCE

Melissa Hathaway, Chris Demchak, Jason Kerben,
Jennifer McArdle, Francesca Spidalieri

December 2016

POTOMAC INSTITUTE FOR POLICY STUDIES

Published by Potomac Institute for Policy Studies

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA 22203
www.potomacinstitute.org
Telephone: 703.525.0770; Fax: 703.525.0299

Email: *CyberReadinessIndex2.0@potomacinstitute.org*

Follow us on Twitter:
@CyberReadyIndex

Cover Art by Alex Taliesen.

Acknowledgements

The Potomac Institute for Policy Studies and the authors would like to thank the following individuals for their contributions: Dr. A. Nagarathna, Chief Investigator of the Advanced Centre on Cyber Law & Forensics, Co-ordinator, PG Diploma in Cyber Law & Cyber Forensics, and Senior Assistant Professor of Law at the National Law School of India University, Bengaluru; Mr. Tobby Simon, Founder and President of Synergia Foundation; Advocate Puneet Bhasin, Cyber Law Expert Managing Partner at Cyberjure Legal Consulting; Mr. Pukhraj Singh, Co-founder and CTO of Bhujang; Mr. J. Prasanna, Founder of Cyber Security and Privacy Foundation; Mr. Ashutosh Bahuguna, Scientist for the Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & IT, Government of India; and Mr. Bedavyasa Mohanty, Junior Fellow at the Observer Research Foundation's Cyber Initiative. The authors would also like to thank Alex Taliesen for cover art and Sherry Loveless for editorial and design work.

INDIA
CYBER READINESS AT A GLANCE

TABLE OF CONTENTS

INDIA

CYBER READINESS AT A GLANCE

Country Population	1.311 billion
Population Growth	1.2%
GDP at market prices (current $US)	$2.095 trillion
GDP Growth	7.6%
Year Internet Introduced	1986 (ERNET), 1995 (public access)
National Cyber Security Strategy	2013
Internet Domain	.in
Internet users per 100 people	26
Fixed broadband subscriptions per 100 users	1.3
Mobile broadband subscriptions per 100 users	5.5
Mobile phone subscriptions per 100 users	79

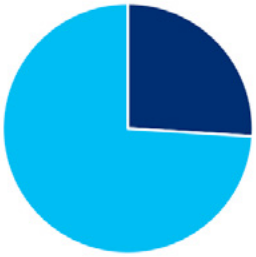
Information and Communications Technology (ICT) Development and Connectivity Standing

International Telecommunications Union (ITU) ICT Development Index (IDI)	**131**	World Economic Forum's Network Readiness Index (NRI)	**89**

Sources: World Bank (2015), ITU (2015), NRI (2015), and Internet Society.

INTRODUCTION

In the 1970s, the Indian Department of Electronics (DoE) started working with the United Nations Development Programme (UNDP) to formulate a strategy to bring computing to India – an action seen as crucial to the informatization of Indian society and to the boosting of local economies. In 1985, the National Center for Science and Technology was created and became responsible for the establishment of India's first Internet Service Provider (ISP), the Education Research Network (ERNET) – an Internet platform aimed primarily at academic and research institutions. ERNET introduced the extension ".in" for domain names in the country and provided Indian academic institutions with their first international connections.[1] This was one of three main initiatives that surfaced concurrently to connect society, academia, and government in India. The Indian Computer Maintenance Corporation (CMC) – originally a government-owned entity later converted to a public limited company in 1977 – initiated India's first public network, the INDONET network, which became operational in 1986. INDONET's goal was to create a networked infrastructure and culture within the country and it was the first to provide electronic mail, file transfer services, applications, and data networks to public and private sector entities.[2] Finally, the National Informatics Centre Network (NICNET) – a satellite-based network – connected the central government with the state governments and district administrators to enable bi-directional information sharing on censuses, medical services, election results, national policies, and other government services.[3]



India Internet Penetration: 26%

In 1995, the Internet became widely available to the Indian public, and the central government has since continued to support Internet uptake as a catalyst for economic growth, job creation, more efficient government operations, and increased access to public services. The Internet penetration rate today, however, is still among the lowest in the Asia-Pacific region and far behind other large, developing countries like China and Brazil, with only 26 percent of the population connected to the Internet.[4] With nearly a billion people still not connected to the Internet, India is home to the world's largest offline population.[5] However, unofficial 2016 statistics suggest that India's Internet penetration rates are on the rise.[6]

The government continues to push digitization to make government services available to all Indians electronically, however, these goals remain difficult to achieve because of the size of the off-line population. For example, in 2006, the Indian government launched the National e-Governance Plan (NeGP) and initiated 31 Mission Mode Projects (MMPs) to offer citizen-centric services, including pension payment, income tax collection, banking and insurance services, and other projects. Although many of these projects were implemented across the country, NeGP did not ultimately reach its desired goals.[7] Yet, India's initiatives in these areas have continued to evolve over the last decade, and lessons learned from previous setbacks have played an important role in shaping future initiatives. One of the more successful e-governance projects is the Aadhaar biometric identification scheme – the world's largest national identification number program, led by the Unique Identification Authority of India (UIDAI).[8] This biometric tool – a 12-digit unique identification document which captures details such as demographic and other biometric data – allows for timely and efficient delivery of welfare services to Indian residents and is now utilized by over 80 percent of the population.[9] While this program may allow more citizens to access e-government services, critics have expressed concern that this large repository of information could be misused for state surveillance or breached by criminals to exploit the information.

Transforming India into a "digitally empowered society and knowledge economy" is one of the main goals of the current government. Prime Minister Nerendra Modi laid out his vision in his 2015 digital strategy, called "Digital India" – a broad economic plan to prioritize job creation through innovation enabled by a robust telecommunications-connected infrastructure.[10] Realizing that connectivity underpins economic growth, the plan outlines initiatives to improve telecommunication services, including accelerating broadband deployment by at least 50 percent (currently about 7 percent) and provisioning universal access to mobile connectivity – increasing in rural India by 30 percent (currently about 45 percent). If successful, this plan could have a two-fold effect: (1) attracting foreign direct investment, and (2) increasing high-tech exports, which in turn could result in an additional GDP growth of 9 percent (~$180 billion).[11] Additionally, "Digital India" encourages industry innovation in ICT solutions for the healthcare sector, knowledge management, and financial services. This plan is one of many other related programs, such as "Make in India," "Skill India," "Start-up India," and "Stand up India," launched to further encourage younger generations and the IT industry to innovate, develop creative solutions, and promote domestic production of electronic devices – India's second largest import.[12] This is India's "digital revolution" to fully realize the economic benefits of ICT. The implementation of "Digital India" is being coordinated by the Ministry of Electronics and Information Technology (MeitY) – former Department of Electronics and Information Technology (DeITY), and each of its initiatives – including the establishment, expansion, and modernization of core ICT infrastructure infrastructure – identifies specific milestones and objectives to be completed by mid-2018.

These plans continue to position India as an ICT leader in the global marketplace. In 2016, the Indian ICT sector contributed $143 billion in revenue, $108 billion in exports, and employed about 3.7 million people.[13] E-commerce – India's fastest growing market – has grown by over 20 percent since 2015 (about $17 billion), as companies have adopted hyper-local e-commerce, innovative mobile platforms, and online payment solutions.[14] As a result, some Indian IT services companies, such as Wipro and Infosys are emerging as global competitors in the world's marketplace, while others such as Flipkart (online shopping), Quikr (online marketplace), and Nauki.com (jobs site) are becoming major players in the fast growing domestic e-commerce space.[15]

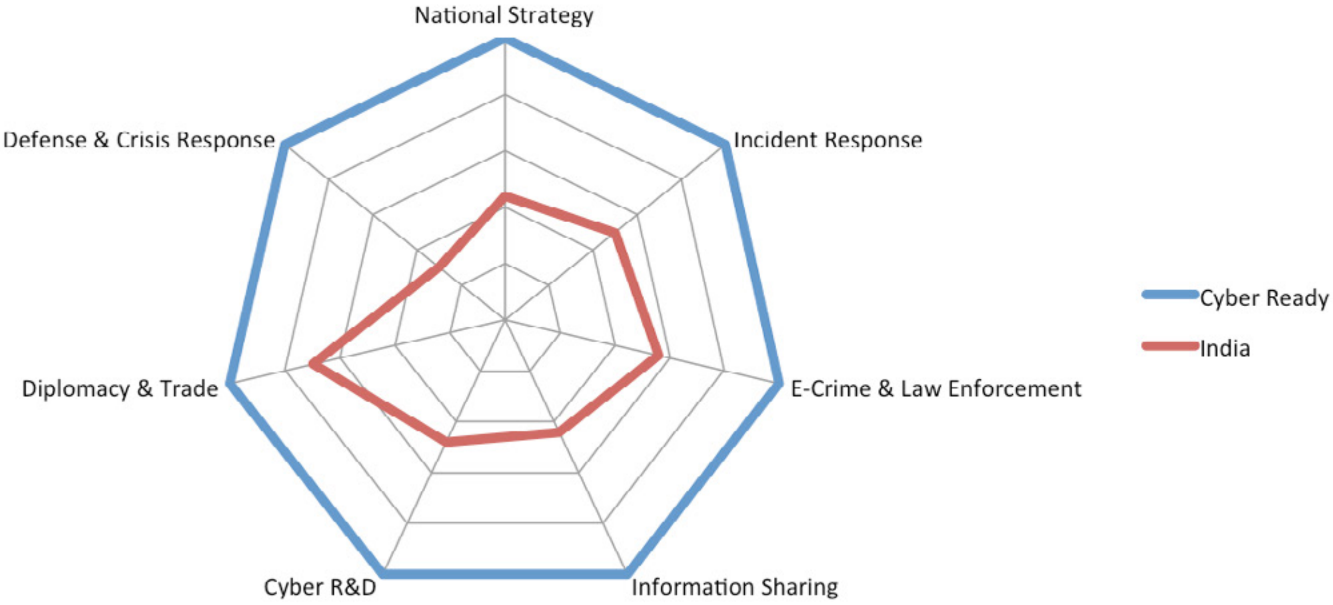
Although India's digital strategy has the potential to generate greater digital dividends and has already been quite successful in attracting foreign direct investments in the ICT sector, the government has yet to make cyber security an equal priority – aligned with the economic initiatives. Cyber security is not a new issue for India, but the government now recognizes that it can also transform cyber challenges into opportunities to drive India's ICT security and resilience agendas. In launching "Digital India," PM Modi equated cyber risks to a "global threat of bloodless war," and asserted that "India has a big role to play [in dealing with global cyber threats]" and that his country "can provide innovative and credible solutions […] to ensure that the entire world lives in peace."[16]

While national statistics are not readily available, India continues to rank high on both the list of countries identified as major points of origin for cyber attacks – third behind the US and China – and as a leading target for cyber crime and ransomware. Countries like India are an attractive target for hackers because they have experienced a rapid increase in ICT uptake, e-commerce activities, online banking and financial transactions, but this increased connectivity has not been accompanied by higher security awareness.[17] The High Court of India commissioned a study that showed that cyber crimes such as ransomware, identity theft, and phishing attacks cost the country over $4 billion in 2013.[18] In 2015, India's National Security Advisor, Ajit Kumar Doval, included cyber security as one of the major internal security challenges faced by the country.[19]

Despite the several cyber security-related initiatives that India has put forward, including the initial 2008 Information Technology (IT) Act, the recent establishment of a dedicated National Cyber Security Coordination Centre (NCCC), and the commitment of "Digital India" to strive for a safe and secure cyberspace,[20] India's infrastructure security and resilience, legal and regulatory measures, and broader economic reforms have not kept pace with the digital revolution envisioned by PM Modi. This is magnified by India's lack of a professional cyber security workforce and the persistent digital, educational, income, and gender divide between on- and off-line populations. In addition, India's 2013 "National Cyber Security Policy" lacked an implementation plan and most of the government's current policies are best described as "piecemeal."[21] Critics have also pointed to a number of recent cyber espionage attacks as indicative of India's lack of a resilient cyber and coordinated security response apparatus.[22] Finally, senior national security officials have drawn attention to the lack of an integrated approach between the various agencies mandated to protect India's critical information infrastructure.[23] In summary, there is still a substantial gap in terms of national-level preparedness for cyber risks.

India faces many challenges that make it difficult to determine how cyber security will be prioritized moving forward. The primary objective for India is, in fact, the preservation of law, order, and security. Past and continuing challenges, including existing and perceived threats associated with separatism, sectarianism, terrorism, and militancy, have dominated the national security agenda. [24] Improving the country's cyber security posture will require committing sufficient resources and up-leveling the importance of it to the future of India's national and economic security.

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate India's current preparedness levels for cyber risks. This analysis provides an actionable blueprint for India to better understand its Internet-infrastructure dependencies and vulnerabilities and assess its commitment and maturity to closing the gap between its current cyber security posture and the national cyber capabilities needed to support its digital future. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0 (national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response) follows.



India Cyber Readiness Assessment (2016)

1. NATIONAL STRATEGY

In 2010, the Indian government fell victim to a series of high-profile computer intrusions at the National Security Council, the National Security Advisory Board (NSAB), and other high profile offices. The government responded to these incidents by creating an Inter-ministerial Task Force on Cyber Defence & Preparedness, chaired by the National Technical Research Organisation (NTRO) – India's technical intelligence agency.[25,26] This was also one of the earliest multi-stakeholder initiatives on cyber defence.

In 2013, the Indian government released the first "National Cyber Security Policy," which acknowledges that unsecured cyberspace can undermine confidence in the state and its supporting infrastructure.

The Task Force on Cyber Defence & Preparedness helped inform India's cyber policy and future organizations. In 2013, the Department of Electronics and Information Technology (DeITY) – which was elevated and given the status of Ministry of Electronics and Information Technology (MeitY) in 2016 – released the first "National Cyber Security Policy." The cyber security strategy noted that increased ICT penetration had been a catalyst for Indian economic growth and social development, increasing employment opportunities, and raising the standards of living. Moreover, the document highlighted the role of the Indian government in driving ICT adoption in public services (e.g., government-to-citizen services, citizen identification, and public distribution systems), health care (e.g., telemedicine, remote consultation, and mobile services), education (e.g., e-learning and virtual classrooms), and financial services (e.g., mobile banking and payment gateways). While the document summarized the benefits India has realized based upon increased ICT penetration, it also warned about the inherent risks associated with an unsecured cyberspace, which in turn has the capacity to "reduce state resources" and "undermine confidence" in the state and its supporting infrastructure.[27]

The document articulated a clear vision for India, stating that its goal was "to build a secure and resilient cyberspace for citizens, businesses, and government."[28] Additional objectives to ensure resiliency and trust in cyberspace included: strengthening the regulatory framework for ensuring a secure cyber security ecosystem; enhancing and creating national and sectoral level 24x7 mechanisms for obtaining cyber threat information; operating a 24x7 National Critical Information Infrastructure Protection Center (NCIIPC); and creating a cyber security workforce of 500,000 individuals by 2018. The document provided 15 additional objectives and related action areas, such as creating a secure cyber security ecosystem; developing an assurance framework; encouraging open standards; promoting the protection and resilience of critical information infrastructure; and creating cyber security awareness. In many ways, the document was highly aspirational, because while it outlined clear objectives and action items, it did not offer an implementation plan or specific guidelines to achieve those goals.

The strategy called for the creation of a central national body charged with coordinating all matters related to cyber security in India. However, while a National Security Council Secretariat (NSCS) was established as the central coordinating body for cyber security and Internet governance, the Ministry of Communications and Information Technology within the Department of Telecommunications was the body tasked with the implementation of national-level cyber security policy.[29]

In 2015, the position of the National Cyber Security Coordinator was created and staffed – taking advantage of institutional knowledge – by the former head of India's CERT at MeitY. The Coordinator is positioned within the Prime Minister's Office and is also the head of the newly established National Cyber Coordination Center (NCCC), located under MeitY. The NCCC's mission is to engage public and private sector entities, including intelligence agencies, law enforcement, ISPs, and industry to mitigate the effects of online threats, facilitate cyber threat intelligence sharing, and evaluate malicious information that may flow into the networks. The Finance Ministry has allocated US$130 million for NCCC operations, but the NCCC is still building capacity and staffing the organization and it is unclear how it will carry out its intended operational activities and mission from a technical perspective.[30]

Although the Indian government has yet to publish an updated national cyber security strategy that aligns the country's economic vision with its national security imperatives, it has outlined nine core principles for cyber security: (1) the promotion of peace and stability; (2) a multi-stakeholder approach; (3) the support of funding for the United Nations Group of Government Experts (UN GGE); (4) capacity building and research and development (R&D); (5) technical cooperation among Computer Emergency Response Teams (CERTs) and standard setting; (6) the promotion of economic growth; (7) cooperation between law enforcement officials; (8) the support of freedom online; and (9) the protection of data and privacy.[31]

Moreover, the Indian government has recognized the benefits and threats derived from the use of ICTs, and both the 2013 "National Cyber Security Policy" and the 2015 "Digital India" initiative acknowledged the importance of Internet connectivity and ICT development as key drivers of Indian economic growth. Yet, while "Digital India" seeks to increase ICT penetration and ICT applications in citizen-facing services, the national cyber security strategy squarely focuses on securing India's information infrastructure and building cyber security awareness. Thus, until the digital and cyber security strategies are aligned, India may not realize the economic promises and national security guarantees needed to support its digital future.

2. INCIDENT RESPONSE

The amended 2008 IT Act (section 70A) proposed the designation of a government organization as the "national nodal agency" for the protection of critical information infrastructures, and section 70B assigned that role to the Indian Computer Emergency Response Team (CERT-In), charging it with "securing Indian cyberspace."[32]

However, it was not until 2014 when malicious software was discovered throughout India's industrial control systems,[33] that DeITY (now the Ministry of Electronics and Information

The National Critical Information Infrastructure Protection Centre (NCIIPC) is the central authority for the protection of critical information infrastructure in India.

Technology, MeitY) officially announced the creation of the National Critical Information Infrastructure Protection Centre (NCIIPC) under the National Technical Research Organisation (NTRO) as the dedicated agency for critical sectors. The government defines critical information infrastructure as "those facilities, systems, or functions, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation."[34] This includes 12 sectors that fall under NCIIPC's mandate, including: energy, transportation, banking and finance, telecommunications, manufacturing, defense, law-enforcement, e-governance, and water, among others.[35] A mandate for this type of governmental organization that includes a combination of both the public sector and private sector is notable and offers some opportunities to further information sharing activities and collaboration. NCIIPC's key responsibilities include: identifying critical sub-sectors; issuing daily and monthly cyber alters and advisories; conducing malware analysis and cyber forensics; tracking malware and botnets; promoting cyber security awareness and training; operating a 24x7 help desk.[36] In order to facilitate better incident response among critical information infrastructure providers, the NCIIPC has each organization or ministry within a designated critical sector identify a "nodal officer" or computer information security officer (CISO) to be the key point-of-contact with NCIIPC.

CERT-In was established in 2004 and today acts as the national central body for cyber incident response, incident cross-sectoral coordination, and the implementation of proactive measures to reduce cyber risks across federal and state governments, industry, and academia. CERT-In serves also as an advisory body for both the public sector and critical information infrastructure, and works to develop cyber security standards for all enterprises.[37]

India established its first Computer Emergency Response Team (CERT-In) in 2004, tasked with coordinating cyber incident response activities and implementing proactive measures to reduce cyber risks.

The amended 2008 Act and the 2014 IT Rules assigned CERT-In a broader set of objectives, including: collecting, analyzing and disseminating information on cyber incidents; forecasting and publishing alerts of cyber security incidents; providing emergency measures for handling cyber security incidents; coordinating cyber incident response activities; issuing guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response, and reporting of incidents; and other cyber security-related functions as prescribed.[38]

Subsequently, CERT-In released a framework document allowing it to track its progress towards meeting the objective areas outlined in the 2008 amended IT Act. Each objective area was assigned associated actions and measures of success. Since the release of the framework document, CERT-In has updated its Cyber Crisis Management Plan (CCMP) to counter cyber attacks and cyber terrorism, as well as other cyber-related incidents that impact critical national assets and endanger public safety or national security. In addition, CERT-In is conducting security audits of critical infrastructure organizations; cyber security exercises at the sectoral, national, and international levels; and entering into formal agreements to collaborate with other national CERTs and sectorial CERTs. CERT-In is also utilizing media advertising to boost citizen awareness and provide additional cyber awareness training.[39]

Additionally, CERT-In established a security alert system that publishes daily "advisories" and "vulnerability notes" on potential cyber threats and vulnerabilities on their website and distributes them to interested CERT-In listserve subscribers.[40] Moreover, CERT-In publishes an annual report that provides an overview of CERT-In activities, including a summary of its botnet tracking and training workshops and statistics regarding cyber-related incidents.[41] Finally, in response to increasing incidents of cyber fraud and underlying insecurities of digital transactions, India Finance Minister Arun Jaitley recently announced the establishment of a dedicated CERT for the financial sector (CERT-Fin) to strengthen the security and resilience of the Indian financial system.[42]

The government allocated ₹85 (~$13.6 million) during the 2015-2016 financial year for three activities: CERT-In operations, the Cyber Appellate Tribunal,[43] and cyber security research and development (R&D).[44]

3. E-CRIME AND LAW ENFORCEMENT

The Indian government recognizes the severity and impact of cyber crime and in light of this, has passed and updated several statues to better respond to cyber crime and security breaches of information technology infrastructure. The IT Act of 2000 – later amended in 2008 – provides a broad legal framework for the Indian government to address a range of cyber security-related challenges. Cyber crimes that are listed under the act include: "Tampering with Computer Source Documents" (section 65); "Punishment for sending offensive messages through communication services, etc." (section 66A); "Punishment for publishing or transmitting obscene material in electronic form" (section 67); and "Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security" (section 69B), among other crimes.[45]

After the amendment of the IT Act in 2008, the constitutionality of the statute that prevents the transmission of "offensive material" was debated in the Indian Supreme Court. In 2015, the Supreme Court struck down section 66A, deeming it unconstitutional, noting that the statute had been widely misapplied by police in various states to arrest innocent persons for posting critical commentary on social and political issues and political leadership online.[46]

Moreover, under the 2000 IT Act (section 84A), the Indian government considered the adoption of a "National Encryption Policy." In 2015, the Indian government posted a draft of the policy online that was formulated by an expert group at the former DeITY. The draft language highlights some of the technical and institutional overlaps between cyber security, cyber crime, and lawful interception. The document triggered widespread criticism, based upon some interpretations that all citizens who use encryption services – for example WhatsApp – would be required to store plain text versions of encrypted communications for 90 days or face potential legal action. Moreover, the policy also suggested that e-commerce sites would be obligated to keep plain text data and encrypted text data of users for 90 days from the date of the transaction.[47] As a result of the criticism, the Indian government removed the document after one day, stating that the document was "just a draft and not the view of the government."[48] However, some of the same security concerns that motivated the creation of the draft "National Encryption Policy" are also driving India to develop a Central Monitoring System (CMS) for the "lawful interception and monitoring of communication to address…national security concerns."[49] Many law enforcement officials, however, are not fully aware of their adjudicating powers under the Information Technology Act of 2008 and the successful investigation and prosecution of cyber crimes is still impaired by the lack of standard procedures for searching, seizing, and forensically examining of digital evidence.[50]

To help increase capacity and understanding of issues at the intersection of science, technology, policy, and law, the Indian government has developed a series of training centers. For instance, the Advanced Centre for Research, Development and Training in Cyber Law and Forensics at the National Law School of India University in Bangalore works to translate the law into technical terms and vice-versa by providing training and education to judicial officers, prosecutors, investigative agencies, cyber secrity personnel, technologists, and others. Funded by DeITY (now MeitY), the Centre provides a unique hands-on training component.[51] Additionally, the government – via a public-private partnership with the Data Security Council of India (DSCI)[52] and the National Association of Software Services and Companies (NASSCOM)[53] – has developed cyber labs in Mumbai, Bangalore, Pune, and Kolkata.[54] The labs are designed to train law enforcement officials and industry partners in cyber securi-

> *Through a public-private partnership with the Data Security Council of India (DSCI) and the National Association of Software Services and Companies (NASSCOM), the Indian government has worked with industry to develop cyber training labs in Mumbai, Bangalore, Pune, and Kolkata.*

ty and forensics. Thus far, 49,000 individuals have been trained through the DSCI cyber labs pan-Indian program.[55] In addition, with initial support from MeitY, the India University's National Law School has set up a Cyber Law Centre and a Cyber Forensic Lab and conducts regularly training of law enforcement agencies in both cyber laws and cyber forensics.

The Ministry of Home Affairs (MHA) is also advocating to increase the country's capacity to deal with cyber crime and cyber insecurity. MHA issued an advisory to state governments to build the technical capacity required to tackle cyber crime, including training professionals for detection, registration, investigation, and prosecution of cyber crime. As a result, the MHA is supporting the establishment of Cyber Crime Police Stations (CCPS) and Cyber Crime Investigations and Forensics Training Facilities (CCIFTC) in each Indian state under its police modernization scheme. Cyber forensics training and investigation labs have been established in the states of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur, Jammu, and Kashmir. The government has also established a state-of-the-art facility for cyber crime investigation at the National Police Academy (NPA) in Hyderabad to provide hands on training to police officers tasked with combating cyber crimes.[56]

The Indian Central Bureau of Investigation (CBI) – the lead body that investigates breaches of central laws – views cyber crimes from two different perspectives: one is that computers are the means to commit crimes, and the other is that computers are the target of crimes. As a result, the CBI has set up various bodies to help combat cyber crime. The CBI has a Cyber Crimes R&D Unit, a Cyber Crime Investigation Cell, and a Cyber Forensics Laboratory (which includes a digital imaging center), and a Network Monitoring Centre. The CBI also has a separate Economic Offenses Division that leads the investigation of cyber crimes related to banking and financial services.[57] The CBI's Cyber Crime Investigation Cell was established in 2001 and has a core team of individuals, who frequently interface with the US Federal Bureau of Investigation (FBI), INTERPOL, and the police forces of other countries.[58]

In 2016, the government proposed the establishment of an Indian Cyber Crime Coordination Center (IC4), a ₹400 (~$64 million) "cyber control hub" under the MHA meant to monitor "child pornography and online trolling."[59] Moreover, the Indian government launched a Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra), part of CERT-In, in December 2016. The botnet center works with the ISPs to detect botnets, alerts owners of software infections on their devices, and directs them to the CERT-In website which recommends procedures to remove malicious software and infections.[60] This initiative is a component of the "Digital India" and had initial funding of ₹100 (~$16 million).[61]

Realizing the importance of cyber security as an important precursor to digital inclusion and e-governance, various state governments have also initiated statewide projects to tackle cyber crime and data theft. For instance, the Government of Maharashtra has launched a "Cyber Maharashtra" project with a budget of ₹1000 (~$150 million),[62] and other states like Andhra Pradesh[63] and Telangana are following suit.[64]

India is not a signatory of the Council of Europe Convention on Cybercrime but will become a member of the Shanghai Cooperation Organisation's "Agreement on Cooperation in the Field on Ensuring International Information Security."

Internationally, the Indian government is partnering with other countries and international organizations to reduce cyber crime. India has signed 39 mutual legal assistance treaties (MLATs) with various countries, which often include the exchange of cyber crime information among signatory countries to facilitate swifter incident response and indictment of criminals. The MHA International Security II Division is the central body that handles requests for information regarding extra territorial crimes, including cyber crime. A seven-member body was also recently formed within the CBI to ensure compliance for all MLA requests.[65]

Nonetheless, India is not a signatory of the Council of Europe Convention on Cybercrime (commonly known as the Budapest Convention). It rejected the Budapest Convention because of Section 32B of the Convention, which allows members to access or receive stored computer data located in another member state, should the requesting member obtain lawful and voluntary consent. India views this as an infringement on the sovereignty of a country.[66] Even though India has yet to become an official member of the Shanghai Cooperation Organisation's (SCO) "Agreement on Cooperation in the Field on Ensuring International Information Security," in 2016, Indian government officials signed a "Memorandum of Obligations" with the Council of the SCO Heads of States for the purpose of gaining full-fledge membership in the SCO. Their membership is likely to be accepted at the summit of leaders of the SCO member states in Astana in June 2017. As part of its accession, India will have to accept all documents that have been adopted by SCO member states in the last 15 years, which will include the "Agreement on Cooperation in the Field on Ensuring International Information Security."[67]

4. INFORMATION SHARING

As stated in the amended IT Act of 2008 (section 70B), CERT-In is the designated national agency for emergency incident response, as well as the collection, assessment, and sharing of information on cyber incidents.[68] CERT-In is responsible for sharing relevant information 24x7 regarding cyber attacks, vulnerabilities, solutions, and cyber crisis management. Additionally, NCIIPC is responsible for sharing malware analysis and other information with critical infrastructure organizations and their critical sub-sectors.[69]

While India does not have a national information sharing policy, the 2013 "National Cyber Security Policy" does highlight the importance of information sharing and cooperation as a key strategic area. The national cyber security strategy highlights three main action areas: (1) developing bilateral and multilateral relationships with other countries in the areas of cyber security; (2) enhancing national and global cooperation among security agencies, CERTs defense agencies and militaries, law enforcement, and the judicial systems; and (3) creating a mechanism for dialogue related to the technical and operational aspects of cyber security with industry in order to facilitate recovery and resilience efforts, including with critical information infrastructures.[70]

Moreover, the 2013 strategy notes the importance of creating an information sharing national-level mechanism for the timely exchange of threat information. Two years after the release of the national cyber security strategy, the Indian government set aside ₹775 (~$124 million) over a five-year period to create the national level mechanism intended to generate situational scenarios of existing and potential cyber threats and to facilitate information sharing.[71]

While India does not have a national information sharing policy, the 2013 "National Cyber Security Policy" does highlight the importance of information sharing and cooperation as a key strategic area.

There have been instances, albeit limited ones, of information sharing between the Indian government and industry. In 2010, India's CBI entered into a memorandum of understanding (MoU) with NASSCOM and DSCI to facilitate information sharing on emerging technology, security standards, and best practices between law enforcement and industry.[72] While this was an important initiative, in 2012, DSCI and the Indian government released the "Recommendations of [the] Joint Working Group on Engagement with the Private Sector on Cyber Security" and highlighted that private-public information exchange was insufficient. The document creates a roadmap for the private-public-partnership and advocates for the establishment of institutional mechanisms to promote convergence and coordination between the public and private sector. The document also outlines private sector intentions to set up Information Sharing and Analyses Centers (ISACs) in various sectors, which would cooperate with sectoral CERTs at the operational level.[73]

Subsequently, the Indian Banks-Center for Analysis of Risks and Threats (IB-CART) – a body modeled after the US financial service ISAC (FS-ISAC) – was set up in India in 2014 by the Reserve Bank of India's Institute for Development and Research in Banking Technology. The IB-CART's main objectives include: disseminating and fostering the sharing of relevant and actionable threat information among members to ensure continued public confidence in the banking sector; aiding the sector's resources to assist the entire sector with cyber situational awareness and advanced warning; and conducting research and intelligence gathering to alert members of evolving or existing threats. To date, IB-CART has attracted more than 90 institutions from at least 60 public, private, and foreign banks in India.[74] While other private, real-time cyber threat intelligence networks are used more widely in the financial services sector, IB-CART may one day become a model for future ISACs, such as in the power[75] and petroleum sectors.[76]

The Indian Banks-Center for Analysis of Risks and Threats (IB-CART) shares information and alerts with more than 90 participants from at least 60 public, private, and foreign banks in India.

5. INVESTMENT IN RESEARCH AND DEVELOPMENT

India's 2013 national cyber security strategy ("National Cyber Security Policy") outlines India's commitment to cyber security R&D to meet short, medium, and long-term economic and policy goals. The strategy provides a list of R&D action areas, including: the development of trustworthy systems (i.e., testing, deployment, and maintenance throughout the systems lifecycle); the use of R&D to promote tailor made, cost effective, indigenous solutions to cyber security challenges for future export; and the facilitation of joint R&D with academia and industry for cutting-edge technologies and security research.

MeitY has furthered acknowledged the importance of indigenous cyber security R&D as applied to India's national security. Indigenous R&D allows India to develop tailor made solutions and products in the face of export restrictions on sophisticated products and systems from advanced countries. The government science and technology roadmap advocates for indigenous R&D as a means to protect its ICT supply chain from manipulation. Moreover, India has expressed concern over imported IT products because it believes that these products may present "veiled security threat[s]."[77]

MeitY notes the important role the private sector plays in addressing short-term R&D, leading to commercially viable products. Even though India has emerged as the second largest exporter of computer and information services in the world and is making significant strides in e-commerce, the private sector still faces challenges.[78] For instance, the World Bank ranks India low in terms of ease of doing business – starting a business, dealing with construction permits, enforcing contracts, and paying taxes.[79] Moreover, unstable electricity and issues with the quality of broadband service has also been an obstacle in the past, especially in the areas of cyber security R&D. Some of these constraints continue to impact local entrepreneurs and multinational companies interested in conducting business in India, although PM Modi has promised to address these concerns.[80] For example, under "Digital India," a public-private partnership unveiled a user-friendly website, entitled "eBiz," providing users the ability to more easily start and operate a business.[81] Additionally, in 2013, NASSCOM initiated the 10,000 Start-ups Program (Start-up Warehouse). This initiative, modeled on "Start-Up Chile," seeks to create a micro-ecosystem where early stage start-up founders can work together and share their best practices with each other. Start-up Warehouse was launched in Kolkata with initial funding of approximately $35 million from the West Bengal Government (Ministry of IT) and the Small Industry Bank of India. It was conceived by NASSCOM and is now supported by more than 35 global corporations including Google, Kotak Bank, Hitachi, IBM, Intel, Microsoft, Sony, and Wipro. At least eight other state governments are following Kolkata's lead and incubating start-up centers. They realize the economic potential of this activity and the importance of providing global exposure to Indian entrepreneurs, thereby connecting them to the global marketplace.[82]

Outside of fostering a more conducive business environment, India also plans to build a more professional cyber security workforce of 500,000 skilled workers by 2018 through capacity building, skills development, and training.[83] In particular, MeitY launched a broad Information Security Education and Awareness (ISEA) project to address the human resource requirement in the country, train government personnel, promote cyber security awareness, and create a national repository of courses in information security.[84] It also set up a dedicated grant administration scheme and called for R&D proposals in various ICT areas, such as cryptography and cryptanalysis, network and systems security, security architectures, vulnerability and assurance, monitoring, surveillance, and forensics.[85]

Moreover, a variety of cyber security-related courses and degree programs are offered at a number of Indian universities. The well-known Indian Institutes of Technology (IITs) offers undergraduate, graduate, and doctoral level degree programs where students can focus on cyber security and network security-related issues. A number of universities also offer undergraduate and master's degree programs in cyber security, such as the Indian Institute of Technology Mumbai, the M. S. Ramaiah Institute of Technology (MSRIT) in Bangalore, SJES College of Management Studies in Bangalore, Jadavpur University in Kolkatta, and the K.K. Modi International Institute in New Delhi.[86] Recently, the India Institute of Technology in Kanpur became part of the world's largest student run cyber security challenge. The competition tests student knowledge of information security, from hardware and software penetration testing to protection, digital forensics, and government policy.[87] While academic programs are now available for the newer generation, the students leaving university are not necessarily prepared with the requisite skills needed by industry.[88]

As a result, industry is working to build cyber capacity. For example, NASSCOM launched a "NASSCOM Cyber Security Task Force" in 2015, aimed at making India a hub for cyber security research, training, and products, which is expected to generate a $35 billion market by 2025.[89] DSCI also intends to train at least one million professionals in cyber security and to build 1,000 successful cyber security-related companies.[90] India's aspirations to develop a digitally empowered society and knowledge economy requires a robust commitment and investment in cyber security basic and applied research and broader university programs to close the gap between talent availability and workforce demand.

6. DIPLOMACY AND TRADE

The Indian Ministry of External Affairs (MEA) treats cyber security as a tier-one foreign policy element and India has been actively engaged in diplomatic and trade and commerce negotiations related to cyber security for a few years. The Joint Secretary for Policy Planning at the MEA acts as the head of cyber issues, and is charged with negotiating agreements with third countries. The MEA has a division entirely devoted to cyber security entitled the "E-Governance and Internet Technology" (EG&IT) division staffed with four permanent representatives.[91] The MEA also has a Global Cyber Issues Cell that tracks international matters impacting national policy and that represents India's cyber security interests, abroad.[92]

The Indian Ministry of External Affairs treats cyber security as a tier-one element of foreign policy.

India has been very active in the international arena to help shape international norms in cyberspace. Indian National Security Advisor, Ajit Doval, has called cyberspace a "global common" in need for a renewed approach and new norms when it comes to diplomacy or conflict.[93] To further its cyber diplomacy agenda, India has participated in multilateral discussions in various international fora including: the United Nations Group of Government Experts (UN GGE) in the context of international security and ICT, the United Nations Commission on Science and Technology Working Group on Enhanced Cooperation, and the United Nations Office on Drugs and Crime Open Ended Inter-Government Working Group on Cybercrime.[94] The government consistently states that "cyber security is the top issue when it comes to global security" and stresses India's commitment to tackle cyber threats.

In addition, India has been involved in a number of high-level bilateral and multilateral cyber dialogues with a variety of countries, including Australia, Canada, China, Germany, France, Japan, Kenya, Russia, South Korea, US, United Kingdom, and United Arab Emirates. Although it has adopted different approaches on key cyber security and Internet governance issues that sometimes appear to advocate for one position with one set of players and another position with others. For instance, statements made after a trilateral meeting in April 2016 among the foreign ministries of In-

India has worked to shape international norms in cyberspace through multilateral discussions related to global cyber issues in various United Nations forums.

dia, Russia, and China seemed to suggest that India supports a multilateral approach to Internet governance issues.[95] On the other hand, the "US-India Cyber Relations Framework" agreement signed between India and the US in September 2016 noted that both countries are committed to a multi-stakeholder model of Internet governance. The agreement commits the two countries to conduct information exchanges on cyber threats and other issues of mutual concern; promote bilateral cooperation on law enforcement and cyber crime issues; coordinate cyber capacity-building efforts; support an open, interoperable, secure, and reliable cyberspace; and encourage responsible state behavior in cyberspace.[96]

While ICT and cyber security matters are not listed by the Indian Ministry of Commerce and Industry as a top-tier element of foreign trade policy,[97] India is advancing its digital agenda and select cyber security issues in numerous other economic fora and trade negotiations. For example, India is an active member of the BRICS Summits. At the 7th Annual BRICS Summit in 2015, the leaders of Brazil, Russia, India, China, and South Africa addressed issues of common interest and priorities to strengthen and broaden intra-BRICS cooperation. The group emphasized the central importance of the principles of international law enshrined in the UN Charter, particularly the political independence, territorial integrity, and sovereign equality of states, non-interference in internal affairs of other states, and respect for human rights and fundamental freedoms.[98] India expressed deep concern regarding the potential misuse of ICTs for purposes which threaten international peace and security. In 2016, India hosted the 8th Annual BRICS Summit in Goa, where it advocated for public and private investments in infrastructure, especially connectivity, to ensure sustained long-term growth.[99] The leaders stressed the importance of their economic partnership, advocated for approaches to bridge the financing gap in infrastructure, and tasked the New Development Bank (NDB)[100] – a multilateral development bank proposed by India at the 4th BRICS Summit in 2012 and formally established in 2015 – with advancing sustainable development projects in BRICS, emerging economies, and developing countries. A representative from India was appointed as the first President of the bank, and India will host both the next NDB Board of Governors' annual meeting and the first BRICS Trade Fair in 2017.

India also recognizes the strategic importance of the Regional Comprehensive Economic Partnership (RCEP) to its future. RCEP, currently in its last rounds of negotiations, is an Asia-Pacific free trade agreement among the 10 economies of the ASEAN region (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam) and six of its free trade partners (Australia, China, India, Japan, New Zealand, and South Korea). The 16 participating RCEP countries account for nearly 30 percent of global GDP and over one quarter of the world's exports. At the November 2016 ministers meeting, India convinced all other countries to bundle the different parts of the negotiations for goods, services, and investments together into one package.[101] If India is successful, the RCEP will become the largest regional trading bloc in the world.[102] The goal of the RCEP is to lower trade barriers, promote economic and technical cooperation, protect intellectual property, encourage competition, facilitate dispute settlement, and improve market access for exporters of goods and services. The RCEP gives India a platform to influence its strategic and economic status in the Asia-Pacific region and bring to fruition its "Act East Policy." While the negotiation is not finalized, elements of the trade measures include data protection measures, intellectual property rights, restrictive rules on exceptions to copyright, and data sovereignty claims for national security purposes.

Although the Indian government considers cyber security a top-tier element of its foreign policy, the MEA continues to be understaffed, making it difficult to address the wide range of cyber issues in foreign affairs and trade. Given the importance of cyber security policy, this could prove increasingly problematic for India.

7. DEFENSE AND CRISIS RESPONSE

Organizations within four Indian government agencies have cyber security mandates incorporating national cyber defense: the Prime Minister's Office, the MHA, MeitY, and the Ministry of Defense.

The National Technical Research Organisation (NTRO) – modeled after the National Security Agency in the US – is a specialized technical research and intelligence gathering unit under the administrative control of the Prime Minister's Office. Established in 2004, the NTRO does strategic monitoring of satellite and terrestrial Internet communications. The NTRO is the lead repository of India's technical assets, including intelligence satellites, unmanned aerial systems, and intelligence aircraft. It provides technical intelligence to other government agencies on internal and external security issues.[103] Additionally, reporting to the NTRO, is the National Institute of Cryptology Research and Development (NICRD). Founded in 2007, the NICRD designs and develops encryption

The National Technical Research Organisation (NTRO) is modeled after the US National Security Agency and is a specialized technical research and intelligence gathering unit under the administrative control of the Prime Minister's Office.

products for national security applications. The NICRD was the first of its kind in Asia, and has sought to create a pool of cyber security and information security experts for national security purposes.[104] The NTRO also provides funding to the India Consortium Group, a not-for-profit comprised of India's leading information security experts and researchers that often make policy recommendations on cyber-related issues.

The Ministry of Home Affairs (MHS), charged with Indian internal security, also has a series of organizations under its administrative control that have mandates including cyber defense. The Intelligence Bureau (IB) is the lead intelligence body that focuses on internal security. Even though limited information is publicly available on the IB, the MHA gave the nod to the IB in 2015 to create a "cyber security architecture," or wing, that would work independently of the NTRO. This wing plans to include 500 individuals that would work to counter online radicalization from terrorist groups, such as the Islamic State of Iraq and the Levant (ISIS).[105]

Moreover, the newly established National Cyber Coordination Center (NCCC) will coordinate near real-time situational awareness and rapid response to cyber security incidents between intelligence, law enforcement, and defense. The NCCC will also collect, integrate, and scan Internet traffic data from different gateway routers of major ISPs at a centralized location for analysis in order to provide proactive cyber threat detection and defense at a national level. However, as previously mentioned, it is still unclear how the NCCC will share cyber security threat information and to what extent it will work with public and private entities to mitigate those threats.

Within the Ministry of Defence (MoD), two main agencies, outside the armed forces, have missions related to cyber security. The Defence Intelligence Agency (DIA) works to combine the intelligence produced by the three services – the Army, Air Force, and Navy – into actionable information for the military. The DIA controls the Defense Information Warfare Agency, which handles all elements of information warfare, to include psychological operations, cyber war, network security, and electro-magnetic spectrum operations.[106] Moreover, the Defence Research and Development Organisation (DRDO) is the lead defense agency for R&D and testing and evaluation for all fields relevant to national security, including cyber security. The DRDO is involved with the design, development, and production of state-of-the-art sensors, weapon systems, and military platforms, in addition to infrastructure. In one project, the DRDO built two ranges for testing electronic weapons sytems.[107]

While there is no singular national level organization in the military tasked with cyber defense of the nation, each of the military services have included cyber defense – and at times, offense – in their respective military doctrines. The 2004 Indian Army Doctrine, the most recent publicly available doctrine, defines seven different forms of information warfare; however, it does not explicitly state that the Army needs to have this operational capacity.[108] The 2009 Indian Maritime Doctrine also provides a high-level definition of information warfare, including electronic warfare and deception. Unlike the Army Doctrine, however, the Mari-

While there is no singular organization in the military tasked with cyber defense of the nation, each of the military services have cyber defense – and at times offense – in their respective military doctrines.

time Doctrine identifies electronic warfare as a key task for the Indian Navy alongside harbor defense, mine warfare, and other more traditional naval responsibilities.[109] Finally, the 2012 Air Force Doctrine defines both defensive and offensive information operations in addition to cyber warfare. The Indian Air Force (IAF) outlines key cyber threats to the IAF, including infrastructure based attacks, sophisticated malware, and other hardware and software based threats. The IAF concludes by acknowledging that cyberspace presents multiple challenges but also potential warfighting benefits, and that the IAF needs to develop a "well-defined roadmap" for the future.[110]

Outside the official doctrine, each of the military services has sought to enhance cyber capabilities for future conflict scenarios. In 2005, the Indian Army created the Cyber Security Establishment to secure networks at the division level and conduct security audits. The Army has also established a Cyber Security Laboratory at the Military College of Telecommunications Engineering,[111] and two units within its Intelligence Corps to counter foreign cyber espionage attempts targeting Army networks and personnel. Moreover, after the Indian Navy suffered a cyber attack on its Eastern Command headquartered at Viskahapatnam, the service stood up an exclusive cyber warriors cadre – the first military service to establish such a group.[112] Additionally, in 2014, it was reported that the Indian government approved a "Framework for Enhancing Cyber Security of Indian Cyberspace," which is not presently publicly available. The Framework includes the establishment of Cyber Operation Centres (COCs) by each of the defense services, and as a result, each service established interim COCs.[113] The Indian Headquarters Integrated Defense Staff is also responsible for information security and related cyber projects with all three services.[114] Despite all these efforts to develop cyber capabilities, armed forces have taken little action to engage in a cooperative approach to cyber security and operations capability development.

After suffering a series of breaches at the Naval Eastern Command and the DRDO, chiefs of the Indian Army, Navy, and Air Force submitted a draft proposal to establish a cyber warfare tri-command to the MoD. While the draft proposal was submitted in 2013, the MoD still remains undecided on whether to establish a dedicated cyber command.[115]

CRI 2.0 BOTTOM LINE

According to the CRI 2.0 assessment, India is still in the early stages of developing a path toward cyber resilience and cyber readiness, and is currently partially operational only in one of the seven CRI essential elements.

The findings in this analysis represent a snapshot in time of a dynamic and changing landscape. As India continues to develop and update its economic (digital agenda) and national cyber security strategies, policies, and initiatives to reflect a more balanced approach that aligns its national economic visions with its national security priorities, updates to this country profile will reflect those changes and monitor, track, and evaluate substantive and notable improvements.

The CRI 2.0 offers a comprehensive, comparative, experience-based methodology to help national leaders chart a path towards a safer, more resilient digital future in a deeply cybered, competitive, and conflict prone world. For more information regarding the CRI 2.0, please see: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

Legend

●	**Fully Operational**
◐	**Partially Operational**
○	**Insufficient Evidence**

IDI Rank		NRI Rank	GDP Rank	National Strategy	Incident Response	E-Crime & Law Enforcement	Information Sharing	Investment in R&D	Diplomacy & Trade	Defense & Crisis Response
131	India	89	7	○	○	○	○	○	◑	○

ENDNOTES

1. Biswarup Sen, "Digital Politics and Culture in Contemporary India: The Making of an Info-Nation," (New York, NY: Routledge, 2016): 71-72.

2. *Ibid.*

3. Institute for Defense Studies and Analyses, "IDSA Task Force: India's Cyber Security Challenge," (March 2012): 19.

4. International Telecommunications Union, "Percentage of individuals using the internet," (2015).

5. World Bank, "World Development Report 2016: Digital Dividend," Washington, DC: *World Bank* (2016): 7-8.

6. "India Internet Users," *Internet Live Stats*, July 1, 2016, http://www.internetlivestats.com/internet-users/india/.

7. Ministry of Communications and Information Technology, "National e-Governance Plan," http://meity.gov.in/content/national-e-governance-plan.

8. Unique Identification Authority of India, "UIDAI Background," https://uidai.gov.in/about-uidai.html.

9. Unique Identification Authority of India, "State/UT wise Aadhaar Saturation: Annexure 1," https://uidai.gov.in/images/news/aadhaar_saturation_15082016.pdf.

10. Ministry of Electronics and Information Technology (MeitY), "Digital India: About the Programme," http://www.digitalindia.gov.in/content/about-programme, and "Digital India: Programme Pillars," http://www.digitalindia.gov.in/content/programme-pillars.

11. This is based on a World Bank report that noted that a 10 percent increase in mobile and broadband penetration can deliver increases in per capital gross domestic product of 0.81 percent to 1.38 percent, respectively in developing countries. For statistics, see: Deloitte, "Digital India: Unleashing Prosperity," *Deloitte* (2015): 3.

12. "Digital India: PM Modi Says India Can Play a Big Role in Cyber Security Globally," July 2, 2015, *NDTV*, http://www.ndtv.com/india-news/digital-india-pm-modi-says-india-can-play-a-big-role-in-cyber-security-globally-777319.

13. NASSCOM, "IT-BPM Overview," http://www.nasscom.in/indian-itbpo-industry.

14. NASSCOM, "eCommerce Snapshot," http://www.nasscom.in/ecommerce.

15. Dhruva Jaishankar, "Internet Freedom 2.1: Lesson's from Asia's Developing Democracies," *German Marshall Fund* (March 2015): 13.

16. "Digital India: PM Modi Says India Can Play a Big Role in Cyber Security Globally," July 2, 2015, *NDTV.*

17. Venkatesh Ganesh, "India lagging Lagging in cyber Cyber security Security awarenessAwareness," The Hindu BusinessLine, August 29, 2016, http://m.thehindubusinessline.com/info-tech/india-lagging-in-cyber-security-awareness/article9046626.ece.

18. "Cyber frauds cost India $4 billion," The Hindu, October 23, 2013, http://www.thehindu.com/business/Economy/cyber-frauds-cost-india-4-billion/article5261594.ece.

19. Press Trust of India, "Internal Security Will be a Big Challenge for India: Ajit Doval," NDTV, October 31, 2015, http://www.ndtv.com/india-news/internal-security-will-be-a-big-challenge-for-india-ajit-doval-1238573.

20. Department of Electronics and Information Technology, "Digital India," http://www.cmai.asia/digitalindia/pdf/Digital-India-DeITY-Details.pdf.

21. Dilip Kumar Mekala, "The government needs to be more serious about India's cyber security," Force, July 2015, http://forceindia.net/MuchtoWorryAbout.aspx.

22. Abhishek Bhalla, "Modi government gets cracking on cyber espionage," Mail Today, June 28, 2016, http://indiatoday.intoday.in/story/modi-govt-gets-cracking-cyber-espionage/1/702377.html.

23. SD Pradhan, "Cyber security: Need for an overall national cyber strategy," The Times of India, January 18, 2016, http://blogs.timesofindia.indiatimes.com/ChanakyaCode/cyber-security-need-for-an-overall-national-cyber-strategy/.

24. Dhruva Jaishankar, "Internet Freedom 2.1: Lesson's from Asia's Developing Democracies," *German Marshall Fund* (March 2015): 8.

25. Vijay Mohan, "Fresh wave of cyber attacks hits India," The Tribune, February 11, 2016, http://www.tribuneindia.com/2010/20100212/main7.htm.

26. Pukhraj Singh, "Thinking Offensively!", Seminar: The Monthly Symposium, October, 2016, http://www.india-seminar.com/2013/650/650_pukhraj_sing.htm .

27. Ministry of Communications and Information Technology, "National Cyber Security Policy," *Department of Electronics and Information Technology* (July 2, 2013): 2.

28. *Ibid,* 3.

29. In July 2016, the Ministry of Communications and Information Technology was bifurcated into the Ministry of Communications and Ministry of Electronics and Information Technology (MeitY). For more information on MeitY, see: http://meity.gov.in/.

30. Muktesh Chander, "National Critical Information Infrastructure Protection Centre (NCIIPC)," National Technical Research Organisation, http://www.slideshare.net/CERCatIIITD/national-critical-information-infrastructure-protection-centre-nciipc.

31. Geetha Nandikotkur "India Opens Cyber Coordination Centre" April 13, 2015, http://www.bankinfosecurity.asia/india-opens-cyber-coordination-centre-a-8100.

32. Melissa Hathaway's interview with Arvind Gupta, Deputy National Security Advisor, at the *Cyber 360: A Synergia Conclave,* Bangalore India, September 29, 2015.

33. The Gazette of India, "The Information Technology Act of 2008," Indian Ministry of Law and Justice, (February 5, 2009): 14, http://meity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf.

34. Pukhraj Singh, "In Cyberspace Warfare, India is Still Shooting in the Dark", The Quint, February 26, 2016, https://www.thequint.com/opinion/2016/02/25/in-cyberspace-warfare-india-is-still-shooting-in-the-dark.

35. Muktesh Chander, "National Critical Information Infrastructure Protection Centre (NCIIPC)," *National Technical Research Organisation*, http://www.slideshare.net/CERCatIIITD/national-critical-information-infrastructure-protection-centre-nciipc.

36. National Technical Research Organisation, "National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter, and Responsibilities," http://www.slideshare.net/CERCatIIITD/national-critical-information-infrastructure-protection-centre-nciipc.

37. Indian Computer Emergency Response Team, "Welcome to CERT-In," http://www.cert-in.org.in.

38. The Gazette of India, "The Information Technology Act of 2008," (February 5, 2009), and "The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013," (January 16, 2014), http://meity.gov.in/sites/upload_files/dit/files/G_S_R%2020%20(E)2.pdf.

39. Department of Information Technology, "RFD: Results-Framework Document for ICERT 2011-2012," (2012), http://www.cert-in.org.in/Images/CERT-In_RFD2011-12.pdf.

40. Indian Computer Emergency Response Team, "Welcome to CERT-In," http://www.cert-in.org.in.

41. Indian Computer Emergency Response Team, "Annual Report," http://www.cert-in.org.in.

42. PTI, "Cashless push: Computer Emergency Response Team to check cyber frauds," The New Indian Express, February 1, 2017, http://www.newindianexpress.com/business/union-budget-2017/2017/feb/01/cashless-push-computer-emergency-response-team-to-check-cyber-frauds-1565845.html.

43. The Cyber Appellate Tribunal allows any person that may be aggrieved by an order by the Controller of Certifying Authorities, or by an adjudicating officer, to file an appeal before the Tribunal. For more information, see: Ministry of Electronics and Information Technology, "Cyber Appellate Tribunal," http://meity.gov.in/content/cat.

44. Government of India, Ministry of Communications and Information Technology, "Unstarred Question No: 4671, Answered On: 22.04.2015, Budgetary Allocation to Counter Cybercrime, Bharatendra Singh," *Lok Sabha*, (April 22, 2015).

45. The Gazette of India, "The Information Technology Act of 2008," Indian Ministry of Law and Justice, (February

5, 2009): 14, http://meity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf.

46. Amit Choudhary and Dhananjay Mahapatra, “Supreme Court strikes down Section 66A of IT Act which allows arrests for objectionable content online,” The Times of India, March 24, 2015, http://timesofindia.indiatimes.com/india/Supreme-Court-strikes-down-Section-66A-of-IT-Act-which-allowed-arrests-for-objectionable-content-online/articleshow/46672244.cms.

47. “National Encryption Policy draft withdrawn: 13 things to know,” The Times of India, September 22, 2015, http://timesofindia.indiatimes.com/tech/tech-news/National-Encryption-Policy-draft-withdrawn-13-things-to-know/articleshow/49056912.cms.

48. “Criticisms forces government to roll back its draft encryption policy,” The Indian Express, September 23, 2015, http://indianexpress.com/article/india/india-others/government-withdraws-draft-national-encryption-policy-after-furore/.

49. Press Information Bureau, “Surveillance System,” Government of India, March 9, 2011, http://pib.nic.in/newsite/erelease.aspx?relid=70747.

50. Arunabh Saikia, “Why most cybercrimes in India don’t end in conviction,” Live Mint, July 29, 2016, http://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html.

51. Advanced Center for Research, Development, and Training in Cyber Laws and Forensics, “Academic Programs,” National Law School of India.

52. The Data Security Council of India (DSCI) is an industry organization that was founded to promote data protection and to develop and implement security and privacy best practices for all Indian industries that operation information systems. DSCI was established by the National Association of Software and Services Companies (NASSCOM).

53. National Association of Software and Services Companies (NASSCOM) is a trade association covering the Indian Information technology and business process outsourcing industries.

54. Data Security Council of India, “Cyber Labs,” https://www.dsci.in/taxonomypage/283.

55. Melissa Hathaway’s interview with Nandkumar Saravade, CEO of the Data Security Council of India (DSCI) Mumbai, India, September 22, 2015.

56. Ministry of Communications and Information Technology, “Unstarred Question No: 5763, Answered On: 29.04.2015, Cyber Training, Janardan Singh Sigriwal,” *Lok Sabha*, (April 29, 2015).

57. Internet Democracy, “Watchtower: Mapping the Indian Government’s Cyber Institutions,” https://internetdemocracy.in/watchtower/ and Central Bureau of Investigation, “Divisions in CBI,” http://cbi.nic.in/aboutus/div.php.

58. Prashant Bakshi, “Security Implications for a Wired India: Challenges Ahead,” *Strategic Analysis* (2001): 114.

59. Press Trust of India, “New cyber-control hub to check pornography, online trolls”, The Times of India, July 18, 2016, http://timesofindia.indiatimes.com/india/New-cyber-control-hub-to-check-pornography-online-trolls/articleshow/53269223.cms.

60. CERT-In, “Welcome to Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra), http://www.cyberswachhtakendra.gov.in.

61. “Government facility in 3 months to clean malware from mobiles, PCs,” The Economic Times, May 24, 2015, http://economictimes.indiatimes.com/tech/software/government-facility-in-3-months-to-clean-malware-from-mobiles-pcs/articleshow/47404157.cms.

62. Priyanka Pugaokar, “Maha Govt Invests 1000 Cr In ‘Cyber Maharashtra’ Project,” *ChannelTimes.com*, August 28, 2016, http://www.channeltimes.com/story/maha-govt-invests-1000-cr-in-cyber-maharashtra-project/.

63. Sridhar Raavi, “AP – First in India to have 24X7 Cyber Security”, Mirchi9, November 30, 2014, https://www.mirchi9.com/politics/ap-first-in-india-to-have-24x7-cyber-security/.

64. Express News Service, “Telangana government formulates cyber security policy”, The New Indian Express, September 16, 2016, http://www.newindianexpress.com/states/telangana/2016/sep/16/Telangana-government-formulates-cyber-security-policy-1520023.html.

65. Ministry of External Affairs, “Mutual Legal Assistance Requests,” http://www.mea.gov.in/mlatcriminal.htm.

66. Council of Europe, “Convention on Cybercrime,” *Council of Europe* (2001): 20.

67. PTI, “India likely to join Shanghai Cooperation Organisation within a year,” The Indian Express, June 14, 2016, http://indianexpress.com/article/india/india-news-india/india-likely-to-join-shanghai-cooperation-organisation-within-a-year-2852341/.

68. The Gazette of India, “The Information Technology Act of 2008,”14.

69. Indian Computer Emergency Response Team, “Welcome to CERT-In,” http://www.cert-in.org.in and National Technical Research Organisation, “National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter, and Responsibilities,” http://www.slideshare.net/CERCatIIITD/national-critical-information-infrastructure-protection-centre-nciipc.

70. Ministry of Communications and Information Technology, “National Cyber Security Policy,” *Department of Electronics and Information Technology* (July 2, 2013): 9-10.

71. Government of India, Ministry of Communications and Information Technology, "Unstarred Question No: 4671, Answered On: 22.04.2015, Budgetary Allocation to Counter Cybercrime, Bharatendra Singh," *Lok Sabha,* (April 22, 2015).

72. DSCI, "CBI, NASSCOM-DSCI signs MoU to fight Cyber Crimes," November 23, 2010, https://www.dsci.in/node/529.

73. DSCI and Government of India, "Recommendations of Joint Working Group on Engagement with the Private Sector on Cyber Security," (2012), https://www.dsci.in/sites/default/files/Data%20Security%20Council%20of%20India%20(DSCI)%20-Recommendations%20of%20JWG.pdf.

74. Institute for Development and Research in Banking Technology, "Indian Banks- Center for Analysis of Risks and Threats (IB-CART)," http://www.idrbt.ac.in/ib-cart.html.

75. The Indian Ministry of Power in its overview of the power sector includes: coal, gas, oil, hydro, nuclear, and renewable power sources. Ministry of Power, "Power Sector at a Glance ALL INDIA," http://powermin.nic.in/en/content/power-sector-glance-all-india.

76. Government of India, Ministry of Communications and Information Technology, "Unstarred Question No: 91, Answered On: 14.07.2014, Cyber Attack Terrorism, Bhartruhari Mahtab Hansraj Gangaram Ahir, *Lok Sabha,* (July 14, 2014).

77. Ministry of Electronics & Information Technology, "Strategic Approach," http://meity.gov.in/content/strategic-approach.

78. World Trade Organization, "International Trade Statistics 2015," *World Trade Organization* (2015): 140.

79. World Bank Group, "Ease of Doing Business in India: 2016 data," http://www.doingbusiness.org/data/exploreeconomies/india/.

80. Dhruva Jaishankar, "Internet Freedom 2.1: Lesson's From Asia's Developing Democracies," *German Marshall Fund* (March 2015): 15.

81. Ministry of Commerce and Industry, "Welcome to e-Biz," https://www.ebiz.gov.in/home/.

82. Melissa Hathaway's interview with Ravi Ranjan, Managing Director of Start-up Warehouse, Kolkata, India, September 24, 2015, and "1000 Startups" http://10000startups.com/.

83. Ministry of Communications and Information Technology, "National Cyber Security Policy," *Department of Electronics and Information Technology* (July 2, 2013): 4.

84. Information Security Education and Awareness (ISEA), "About ISEA," http://isea.gov.in/isea/home/index.jsp.

85. Ministry of Electronics and Information Security, "Call for R&D project proposals in Cyber Security area," http://meity.gov.in/sites/upload_files/dit/files/in%20Cyber%20Security%20area.pdf.

86. Shiksha, "Cyber Security/IT Security Courses in India," http://it.shiksha.com/it-cyber-security-courses-in-india-categorypage-10-127-1-0-0-1-1-2--none-1-0.

87. Virendra Singh Rawat, "IIT Kanpur to host global cyber security challenge," Business Standard, August 8, 2016, http://www.business-standard.com/article/current-affairs/iit-kanpur-to-host-global-cyber-security-challenge-116080801015_1.html.

88. Venkatesh Ganesh, "India lagging in cyber security awareness," The Hindu BusinessLine, August 29, 2016, http://m.thehindubusinessline.com/info-tech/india-lagging-in-cyber-security-awareness/article9046626.ece.

89. "Nasscom task force to make India hub for cybersecurity research," *ETTelecom*, May, 26, 2015, and Melissa Hathaway's interview with Venkathesh Murthy, Director of the DSCI Cyber Labs, Advanced Center on Research and Development and Training in Cybersecurity Law and Forensics, National Law School of India University, Bangalore, India, October 1, 2015.

90. Melissa Hathaway's interview with Nandkumar Saravade, CEO of Data Security Council of India (DSCI), Mumbai, India, September 22, 2015, and Remarks by Nandkumar Saravade at the *Cyber 360: A Synergia Conclave*, Bangalore India, September 29, 2015.

91. Ministry of External Affairs, "About Us: Administration," http://mea.gov.in/divisions.htm.

92. Internet Democracy, "Watchtower: Mapping the Indian Government's Cyber Institutions," https://internetdemocracy.in/watchtower/.

93. Full speech by AK Doval at the annual *Hindustan Times Summit*, held in November 2014, https://www.youtube.com/watch?v=eccxX_H_8OQ.

94. Ministry of External Affairs, "Annual Report 2013-2014," *Ministry of External Affairs* (2014): xviii.

95. Indian Ministry of External Affairs, "Joint Communiqué of the 14th Meeting of the Foreign Ministers of the Russian Federation, the Republic of India and the People's Republic of China," April 18, 2016, http://mea.gov.in/bilateral-documents.htm?dtl/26628/Joint_Communiqu_of_the_14th_Meeting_of_the_Foreign_Ministers_of_the_Russian_Federation_the_Republic_of_India_and_the_Peoples_Republic_of_China.

96. U.S. Embassy & Consulates in India, "Framework for the US-India Cyber Relationship," https://in.usembassy.gov/framework-u-s-india-cyber-relationship/.

97. Ministry of Commerce and Industry, "International Trade," http://commerce.gov.in/#.

98. "Ufa Declaration," 7th BRICS Summit, Ufa, Russian Federation, July 9, 2015, http://mea.gov.in/Uploads/PublicationDocs/25448_Declaration_eng.pdf.

99. "GOA Declaration," 8th BRICS Summit, Goa, India, October 16, 2016, http://brics2016.gov.in/upload/Goa%20Declaration%20and%20Action%20Plan.pdf.

100. New Development Bank, "Genesis," http://ndb.int/genesis.php.

101. Kirtika Suneja, "RCEP countries agree to Indian demand on services, investment negotiation," The Economic Times, November 8, 2016, http://economictimes.indiatimes.com/news/economy/foreign-trade/rcep-countries-agree-to-indian-demand-on-services-investment-negotiations/articleshow/55305824.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

102. Asit Ranjan Mishra, "India to talk tough at RCEP trade meet," Live Mint, November 2, 2016, http://www.livemint.com/Politics/mOzWKi4gvcNzK7KkBTqJWI/India-to-talk-tough-at-RCEP-trade-meet.html .

103. RS Bedi VrC, "NTRO: India's Technical Intelligence Agency," Indian Defence Review, April 23, 2015, http://www.indiandefencereview.com/spotlights/ntro-indias-technical-intelligence-agency/.

104. Ashok Das, "Key security outfit now near Hyderabad," Hindustan Times, May 7, 2007, http://www.hindustantimes.com/india/key-security-outfit-now-near-hyderabad/story-UZz98GoeIXjaHheFU6CfKK.html, Internet Democracy, "Watchtower: Mapping the Indian Government's Cyber Institutions," https://internetdemocracy.in/watchtower/.

105. Vijaita Singh, "MHA nod for cyber security wing under the IB," The Indian Express, June 18, 2015, http://indianexpress.com/article/india/india-others/mha-nod-for-cyber-security-wing-under-ib/.

106. Vinod Anand, "Debate," Institute for Defence Studies and Analyses: Journal of Defence Studies (2008), http://www.idsa.in/jds/2_2_2008_IntegratingtheIndianMilitary_VAnand.

107. Center for Strategic and International Studies, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Organization and Doctrine," *UNIDIR Resources* (2011): 74.

108. Headquarters Army Training Command, "Indian Army Doctrine," (October 2004): 20-22.

109. Indian Navy, "Indian Maritime Doctrine: Naval Strategic Publication 1.1," (2009): 52 and 92, http://www.indiannavy.nic.in/sites/default/files/Indian-Maritime-Doctrine-2009-Updated-12Feb16.pdf.

110. Indian Air Force, "Basic Doctrine of the Indian Air Force, 2012," (2012): 131-134.

111. Center for Strategic and International Studies, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Organization and Doctrine," *UNIDIR Resources* (2011): 72.

112. "Indian Navy creates exclusive cyber warriors cadre," Deccan Herald, July 12, 2012, http://www.deccanherald.com/content/263791/indian-navy-creates-exclusive-cyber.html.

113. Security Risks, “Security Issues with South Asia: Cyber Security Threats Enhanced,” Security Risks Monitor, December 3, 2014, http://www.security-risks.com/security-issues-south-asia/iw-cyber-security/cyber-security-threats-enhanced-3936.html.

114. Indian Air Force, “Basic Doctrine of the Indian Air Force, 2012,” (2012): 132.

115. Vivek Raghuvanshi, “India Still Unsure on Need for Cyber Command,” *DefenseNews,* December 8, 2014.

ABOUT THE AUTHORS

Melissa Hathaway is a leading expert in cyberspace policy and cybersecurity. She serves as a Senior Fellow and a member of the Board of Regents at Potomac Institute for Policy Studies and is a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs. She served in two Presidential administrations where she spearheaded the Cyberspace Policy Review for President Barak Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. She developed a unique methodology for evaluating and measuring the level of preparedness for certain cybersecurity risks, known as the Cyber Readiness Index. She publishes regularly on cybersecurity matters affecting companies and countries. Most of her articles can be found at the following website: *http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html*.

Chris Demchak is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. Her research areas are digital resilience, cyber conflict, and the structures and risks of cyber space. She designed a digitized organization model known as "Atrium" that helps large enterprises respond to and accommodate surprises in their systems. She is also the author of *Wars of Disruption and Resilience: Cybered Conflict, Power and National Security*.

Jason Kerben is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. He also serves as senior advisor to multiple Departments and Agencies in matters related to information security and cyber security. In particular, he focuses on legal and regulatory regimes that impact an organization's mission. He develops methodologies and approaches to assess and manage cyber security risk and advises on a myriad of specific cybersecurity activities including international principles governing information and communications technologies, identity and access management, continuous diagnostics and mitigation and cyber insurance.

Jennifer McArdle is a Non-Resident Fellow at the Potomac Institute for Policy Studies and an Assistant Professor of Cybersecurity at Salve Regina University in Newport, RI. Jennifer's academic research and publications focus on cyber conflict, escalation management, and military innovation. She is a PhD candidate in War Studies at King's College London.

Francesca Spidalieri is a subject-matter expert at the Potomac Institute for Policy Studies' Cyber Readiness Index Project. She also serves as the Senior Fellow for Cyber Leadership at the Pell Center, at Salve Regina University, and as a Distinguished Fellow at the Ponemon Institute. Her academic research and publications focus on cyber leadership development, cyber risk management, cyber education, and cyber security workforce development. She also published a report, entitled *State of the States on Cybersecurity*, that applies the Cyber Readiness Index 1.0 at the US state level.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org