INDO-US COOPERATION ON
INTERNET GOVERNANCE & CYBERSECURITY

OCTOBER 2014
NEW DELHI
INDO-US COOPERATION ON INTERNET GOVERNANCE AND CYBERSECURITY
contents

Introduction 5

Forward Progress
Towards International Treaty on Cybersecurity: A Bilateral Dialogue Between India and the U.S. 11

Cooperation
International Internet Governance 19

Policing
State Responsibility in the Cyber Commons: Deepening the India-U.S. Relationship 26

Partnerships
Steps to Private Sector Cyberspace Security, Prosperity & Freedom 34

Legal Perspectives
The Problem of Jurisdiction 45

Conclusion
Possibility of a Synergy 49

About the Authors 52

About ORF and The Heritage Foundation 56
The May election victory of the Bharatiya Janata Party led by Prime Minister Narendra Modi has opened opportunities for closer collaboration between New Delhi and Washington on a range of security, defense, economic and trade matters. One area that is particularly ripe for deeper engagement is cyber security—an emerging national security issue for both countries in which the level and scope of the threat is expanding quickly. While the U.S. and India have engaged each other on cyber security issues since 2001, when the Indo-U.S. Cyber Security Forum was first established, concrete cooperation to manage the threat remains minimal.

With the third largest population of on-line users, India’s increasing reliance on the Internet means it is also increasingly vulnerable to cyber warfare. The threat comes from criminal hackers, terrorist networks, or nation-states conducting espionage or trying to disrupt critical infrastructure. The implications of cyber warfare for economic and commercial activity, military readiness, and public safety are
India has been among the biggest victims of the global cyber espionage campaign GhostNet that targeted governmental, research, and military organizations.

enormous. Guarding against increasingly sophisticated cyber attacks has thus become a focal point of Indian – as well as the U.S.—national security strategy.

Cyber attacks on Indian infrastructure – both private and public – have become more common in the last few years. India was among the biggest victims of the global cyber espionage campaign GhostNet that targeted governmental, research, and military organizations. Chinese espionage activities are likely responsible for the most serious cyber breaches in India, including the March 2013 hacking of India’s Defense Research and Development Organization (DRDO) computer systems. In June 2012, cyber attacks were reported on the systems of the Indian Navy’s Eastern Command, responsible for maritime activities in the South China Sea.

The U.S. has become more vocal about its concerns with Chinese cyber espionage in America and in May charged five People’s Liberation Army (PLA) officers for computer hacking and economic espionage against U.S. corporations. The Chinese were furious about the charges, vehemently denying them and urging Washington to revoke the indictments.

Another problem both India and the U.S. face is terrorists’ ex-

ploitation of the Internet to spread propaganda, communicate with each other, and recruit members. The Indian domestic terrorist group, India Mujahideen (IM), has been particularly adept at using social media to communicate as well as recruit members. IM members reportedly used Facebook and other chat sites to cryptically communicate with one another, while relying on proxy internet providers and software to hide their actual locations.

India has begun to address its cyber security challenges in a serious way. The Indian government published its first ever National Cyber Security Policy in July of last year. The policy emphasizes research and development of indigenous security technology and enhanced public-private partnership. It further encourages private organizations and companies to adopt more effective IT regulations and infrastructure in conformity with international best practices and calls for developing a workforce of 500,000 cyber specialists over the next five years. India has also created a multi-agency National Cyber Coordination Center and plans to establish a tri-service cyber command within the defense services.

To further boost cyber security, India recently set up the National Critical Information Infrastructure Protection Center (NCIIPC) charged with protecting assets in sectors like defense, finance, energy, and telecommunications. The Indian Computer Emergency Re-
The growing global cyber security challenges demand that India and the U.S. build a better foundation of mutual trust for cooperation on intelligence and counterterrorism.

Response Team (CERT-In) also protects cyber assets in non-critical areas and acts as coordinating agency for any cyber emergencies. The Indian government budgeted around $7 million for cyber security in 2013 compared to U.S. spending of about $751 million.

The previous Manmohan Singh government laid the groundwork for boosting Indian engagement with other nations on cyber issues and participation in international cyber security dialogues. Former National Security Advisor Shiv Shankar Menon said India should pursue development of common standards for security cooperation in cyber space with other major IT powers, rather than attempting to go it alone. The BJP government is expected to take this agenda forward, having identified cyber security as a priority in its 2014 Election Manifesto.

The highlight of U.S.-India engagement on cyber security was the signing of a memorandum of understanding (MOU) between the Department of Homeland Security and India’s Ministry of Communications and Information Technology shortly after the inauguration of the U.S.-India Homeland Security Dialogue in July 2011.

While the reasons for expanding U.S.-Indian cooperation on cybersecurity and internet governance are compelling, there remain obstacles to deepening engagement on such sensitive issues. A spy-

ing scandal in 2006 involving U.S. and Indian officials participating in the cyber security forum put a severe damper on cooperation for several years. Indian officials remain highly suspicious of U.S. motives and believe the U.S. will seek to exploit the cyber security relationship for U.S. intelligence gathering.

The revelations from the Edward Snowden files have only heightened India’s concerns about American intelligence collection. The Snowden files revealed that India was the fifth most tracked nation in terms of intelligence gathering by the U.S. National Security Agency (NSA). Additional information released by Edward Snowden shows that the NSA was authorized by a U.S. court in 2010 to carry out surveillance on the BJP along with five other foreign political organizations, including Egypt’s Muslim Brotherhood and the Pakistan People’s Party (PPP). The Indian Foreign Minister Sushma Swaraj told U.S. Secretary of State John Kerry that NSA spying on the BJP leadership was “completely unacceptable” when he visited India in late July.

The growing global cyber security challenges demand that India and the U.S. seek ways to build a better foundation of mutual trust when it comes to cooperation on intelligence and counterterrorism. As was visible in the investigations that followed the 2008 Mumbai terror attacks, fissures can crop up between the intelligence agencies of both countries. Indian intelligence officials were initially upset that the U.S. had not shared information about terrorist David Headley with them. Later, India’s limited access to Headley revealed.
how much these information exchanges can interfere with sovereign immunities. Both countries need to make a push to adjust domestic laws in order to allow for greater sharing of data about terrorist activities.

The India-U.S. dialogue on cyber security issues is currently focused narrowly on technical issues. The two sides need to expand the dialogue to cover the international dimensions of cyber security. Two factors constrain the prospects for such a dialogue. One, there is vast asymmetry in the cyber capabilities of India and America. Two, movement toward regulation of the cyber domain is a work in progress in both New Delhi and Washington.

Despite many differences, India and the U.S. have a shared interest in developing a sensible framework for regulating security politics in the cyber domain. Both are democracies and are vulnerable to similar threats like terrorism. Both have concerns triggered by the rise of China and Beijing’s approach to international security. There are strong corporate sectors in both countries and there are growing linkages between their IT industries. In the past, India and the United States ended up on opposite sides of drafting international security treaties. They can’t afford to let that pattern reemerge in the cyber domain.
As worldwide concerns on cybersecurity grow, preventing war and regulating conflict in the cyber domain through a treaty have come to the top of the international agenda. The last few years have seen a growing body of effort to bring the cyber domain under international law. It is based on two sets of convictions. One is the historical experience. Every new domain that has emerged over the last few centuries of the modern age—maritime, air and space—have all been brought under international regulation despite the unique complexities that each presented.

All of them were inevitably securitized; yet, a set of rules and norms have been negotiated for each domain by the international community. The other is the assessment no single country can address on its own all the security challenges that the cyber domain presents. Therefore a measure of international cooperation in the cyber realm, many believe, is a necessity. As international negotiations on a cybersecurity treaty advance incrementally, there is need for a sustained
The idea of a formal treaty to regulate cyber warfare draws mixed responses. For an entirely different set of reasons India and the U.S. are both ambivalent towards cybersecurity treaties.

and purposeful engagement between India and America. This paper explores some of the challenges of constructing such a dialogue.

The U.N. Group of Governmental experts established by the Secretary General has provided a valuable forum for discussion on cybersecurity issues in the last few years among major powers. In a report submitted in August 2013, the GGE presented a number of propositions agreed by consensus among its members. The GGE asserted that the traditional principles of international law are applicable to the cyber domain, thereby bridging an important debate. Given the difficulties of delimiting state boundaries and affixing state responsibilities in the cyber domain, many had argued that the traditional international law is not of much value in regulating of cyberspace. Technological diffusion and the capacity of individuals and non-state actors to inflict considerable damage have also been viewed as limiting the possibility of inter-state agreements. In cyberspace, the GGE held, states should comply with the prohibition on the use of force, respect territorial sovereignty, and the principle of settling disputes by peaceful means in much the same way as in the physical world. The right, specified in Article 51 of the U.N. Charter, to self-defense including the use of force would apply if a cyber attack reached the level of an ‘armed attack’. The report, however, refrained from spelling out when this could be the case.

The report offered a set of recommendations on the principles of responsible behavior in cyber space, proposed a slew of confidence
building measures such as exchange of information on national cyber policies, sharing knowledge on best practices, promotion of regional consultations, and expansion of cooperation in law enforcement and international assistance for capacity building. While the recommendations of the report are a step forward, translating them into treaty language will not be easy. The devil as they say is always in the detail. Yet, the idea of a formal treaty to regulate cyber warfare draws mixed responses in both Washington and Delhi. For an entirely different set of reasons, some of which are rooted in their strategic culture, India and the U.S. are both ambivalent towards cybersecurity treaties.

For America, the question is about sustaining its extraordinary lead in cyber technologies and its freedom of operation in the cyber domain. Many in the U.S. see regulation and arms control will end up constraining America while allowing its rivals and others catch up. Opponents of cyber arms control also point out that while the U.S. is compelled by its laws to abide by international agreements, other countries may not be so fastidious. This approach on the right is contested by the multilateralists in the American establishment who believe U.S. should take the leadership in regulating cyber space because, American technological primacy is likely to be short-lived in the cyber domain. They also argue that the U.S. is far more vulnerable than its adversaries given the centrality of cyber-space in the advanced U.S. economy. This also makes the U.S. more
susceptible to asymmetric warfare. Therefore cyber arms control is a useful way of limiting potential threats and serves American interests over the long term.

These arguments prevailed under President Barack Obama, who moved beyond the previous administration’s opposition to multilateralism in cyber space. Since then the U.S. has been more open to engagement with the other powers in various U.N. and other forums. This does not mean there is a domestic consensus in America on the best approach to cyber security. The divide between unilateral and multilateral approaches within the U.S. is deep. The history of arms control reminds that these differences limit the U.S. room to negotiate agreements and implement those that have been agreed upon in multilateral forums. This in turn makes other nations wary of engaging the U.S. on security negotiations.

India too has an unresolved tension between multilateralism and unilateralism in dealing with international treaties. Given the liberal internationalist orientation of its national movement, India was a strong votary of international institutions, multilateralism and the development of norms in the global arena. Some of the security challenges it faced and the negative experience of taking the Kashmir question to the United Nations Security Council had dampened this enthusiasm for multilateralism but has not eliminated it as a major element in its approach to global issues.

Over the decades, India has taken the lead in multilateral negoti-
atations, including those relating to security and arms control. India’s emphasis was on three D’s—disarmament, development and non-discrimination. This emphasis on universalism won India many plaudits from the liberal internationalists around the world. The problem, however, was India’s idealist approach ran afoul of realpolitik at the international level and its security imperatives at the national level. India which initiated the debate on nuclear non-proliferation in the Eighteen Nation Disarmament Conference at Geneva in the 1960s, found itself at odds with nuclear non-proliferation treaty (NPT) that was finalized in 1968. Similarly on the question of a comprehensive test ban treaty, India was a great champion of the concept but was utterly isolated when the treaty came into being in 1996.

India’s current positions at the international level on cybersecurity are largely derived from the Foreign Office’s inherited traditions of its multilateralism, deeply influenced since the 1970s by the North-South dimension. The national security establishment in Delhi, however, is conscious of the urgent imperative of building domestic capabilities. The realists there have no time for grand-standing on the global stage on cyber issues. India’s approach to international security issues in the past was dominated by principles of equity and non-discrimination. As a potential power in its own right, however, India might have to carve out a path that is bound to diverge from its traditional approaches to international security. As in the nuclear domain, so in the cyber realm, India’s national interests may not be
Despite being a democracy, **internal security considerations often put India at odds with the U.S.** and on the same side as Russia and China on some aspects of cyber regulation.

aligned with the collective positions of the South. India’s primary challenge is to bring in a measure of pragmatism to its engagement on cybersecurity issues that can effectively combine its traditional tenets of internationalism with the strategic dynamic unfolding in the cyber domain.

As the weakest of the major powers, India must learn to nimbly navigate the dynamic among the great powers on cybersecurity issues. In the past India used to urge great powers to abide by norms in the management of security challenges, but was deeply perturbed by any collaboration between the major powers. For example, India was deeply concerned about bilateral nuclear arms control between Washington and Moscow and the implications of their joint championship of the nonproliferation regime. Today India worries about the potential consequences of a cyber security treaty that might emerge out of bilateral negotiations between America and China. India must also be conscious of the fact that technological change and rise of new powers generates pressures for rewriting the international rules.

India has indeed stepped up its engagement with the major powers on cybersecurity issues. This engagement was hobbled by the weak governments in Delhi that were unable to overrule individual departments in the making of important policies. With a strong central government now in place under the leadership of Narendra Modi, considerations of national security and power balances are
likely to have a greater salience in India’s international approach to
cyber issues. As the cyber domain draws attention from the Modi
government, India must necessarily look for building functional coa-
litions to secure its own interests in the global arena. Any which way
that India looks at cybersecurity issues, the U.S. looms large. De-
spite being a democracy, internal security considerations often put
India at odds with the U.S. and on the same side as Russia and China
on some aspects of cyber regulation. But broader considerations of
international regime building on cybersecurity and the new com-
pulsions for security partnership between Delhi and Washington in
Asia, Indian Ocean and beyond demand substantive consultations
between Delhi and Washington.

The current India-U.S. dialogue on cyber security issues is cur-
rently focused narrowly on technical issues. This needs to be ex-
panded to cover the international dimensions of cyber security. Two
factors constrain the prospects for such a dialogue. One, there is
vast asymmetry in the cyber capabilities of India and America. Two,
the national policy towards on international regulation of the cyber
domain is work in progress in both Delhi and Washington. These
realities, however, do not reduce the imperative for the Indo-U.S.
dialogue on cybersecurity. Despite many differences, India and the
U.S. have a shared interest in developing a sensible framework for
regulating security politics in the cyber domain. Both are democra-
cies and are vulnerable to similar threats like terrorism. Both have
Both India and the United States have concerns triggered by the rise of China as an economic and political power and Beijing’s approach to international security.

Concerns triggered by the rise of China and Beijing’s approach to international security. There are strong corporate sectors in both countries and there is a growing integration between their IT industries. In the past, India and the United States ended up on opposite sides of drafting international security treaties. They can’t afford to let that pattern reemerge in the cyber domain.
A ny contemporary discussion on Internet Governance must necessarily respond to some key inquiries. First must be the on the role and responsibility of institutions tasked to look into (some aspects of) this sector under the United Nations (U.N.) framework, their competence and capacity to respond to the multi-layered governance the internet demands and if other multilateral frameworks must evolve in this sector to more efficiently manage the digital domain.

The second question has to be on the participation of various categories of stakeholders as we develop and evolve key rules, norms, codes and principals that will help us better manage the demands of businesses, citizens and governments on and from the sector. And how we ensure that any one set of stakeholders do not unfairly bias the nature and form of digital flows, communication and commerce.

The third central enquiry must be on how nations respond to the whole nation of sovereignty, jurisdiction and territory in the digital space and therefore how does the notion of global governance rec-
The fact is that the U.N. is the most legitimate body in global governance today, and has been used as such to debate topics as wide ranging as climate, war and human rights.

And finally for the purpose of this research we must discuss how could a U.S. and India partnership in the digital space satisfactorily navigate the above debates in a manner that benefits both and strengthens an open, inclusive and equitably governed Internet.

The role of the United Nations, and its capacity to be able to respond to the particular and peculiar challenges of the digital age need to be weighed. The fact is that the U.N. is the most legitimate body in global governance today, and has been used as such to debate topics as wide ranging as climate, war and human rights. But it is limited when it comes to the governing the internet as it does not have the processes to assimilate both breath of activities within this area, and the fast moving technologies that constantly re-shape governance challenges. The shape of any single U.N. platform to govern internet processes will also be a challenge: currently a decentralized structure to internet governance has developed because the internet exists on parallel planes. There are bodies to look at challenges of infrastructure, domain registry, content and freedom of expression and so on. Not all of them are binding in nature, but feed into the larger processes and bodies that exist today.

This challenge can be highlighted by reaction to a proposal from India in 2011, suggesting that global internet governance be moved under a U.N. body, which could meet twice a year. It was met with stiff opposition from much of the internet community. On its part, the U.S.
has consistently remained on the other side of the debate; putting its weight behind the decentralized internet governance mechanisms that exist today. There is also the point that non-government actors, which includes business and civil society, need more space than a single U.N. platform would allow; given that every citizen of the world is either a stakeholder or soon to become a stakeholder in cyberspace.

And the prominence India has given to the U.N. in this field might have been oversold; after all, in the past, just like the U.S., India has also taken a realist approach to the U.N. When necessary and crucial, both countries have opted to ‘go it alone’, for example, the U.S. during the time of the Iraq war, and India at the time of the Bangladesh war. This hypocrisy is common to both countries, who have reaffirmed the centrality of the U.N. when it has suited them. Therefore, India’s perceived affinity towards the U.N. on internet governance matters is certainly not a matter set in stone.

There is also the case of cyber security, a subset of global internet governance. The growing number of cyber crimes and cyber threats make it impossible for countries to wait for a global governance mechanism to develop to solve these issues. For example, all countries have not ratified the Budapest Convention, drafted to look at the subject of cyber crime. Instead, many countries have looked to each other for bilateral and multilateral agreements to share best case practices, technology, information on terrorist activities and coordination between law enforcement officers.
Given that only a minority of the Indian population is online, the government will not let any civil society and/or business ‘representatives’ to capture policy making spaces, and speak for ‘Indians’.

However, the U.N. will always remain a valuable platform because of its demonstrated legitimacy as a common arena for sovereign nations to deliberate. This is the reason the Group of Governmental Experts (GGE), operating under the aegis of the U.N., has been successful in working on state responsibility and ‘norms of cyberspace’ through the meetings. Having said this, the GGE might well be expanded from the current structure of 13 countries participating to a Digital 20; however, it will most likely remain under the U.N. rubric, with active support from both India and the U.S.

This is also the reason that a multistakeholder process for global internet governance processes that deal with the internet’s critical infrastructure and jurisdictional issues which shape the global cyber market, are unlikely to be supported by India. The reason lies in legitimacy of representation. Given that only a minority of the Indian population is online, the government will not allow any civil society and/or business ‘representatives’ to capture policy making spaces, and speak for ‘Indians’. Nor is Indian civil society and business so mature as to be given an equal say along with the government of India, which is still grappling with questions of access, security and last mile connectivity for its people. At the same time, given the amount of businesses and CSOs that are funded by U.S. and other countries, currently active in pushing MSM in India, the government is suspicious of what could be construed as interventionism in national decisions.
These are some of the guiding reasons why India will not blindly accept a multistakeholder model at the international level. The U.S., on the other hand, has companies and civil society organizations who have been engaging with the global internet for decades. U.S. companies are giants in the cyberspace, looking for newer markets to expand into. Their success is the success of the U.S. economy, and therefore, to a large extent, the two stakeholders find their interests aligned. The same can be said for many CSO, often funded by government or business, who fight for the U.S. ideals of freedom of expression and human rights for internet users.

In fact, the biggest technology companies in the online universe are from the U.S. Critical infrastructure of the internet, such as root servers and domain names fall under U.S. jurisdiction. The data servers, on whose geographic location, jurisdiction is defined, are more often than not, based in the U.S.. In fact, the U.S. dominance is not threatened in the least by most of the multistakeholder platforms that exist, because the fundamentals are set in its favour. In this regard, the U.S. mirrors India’s propensity for sovereignty, even though it pays out in a very different manner on the global stage.

There is also further pause to be given to the role of the private sector in internet governance. The internet was created to be a open network, where information would be shared freely. It did not have laws restricting trade and knowledge transfer. This allowed U.S. companies to grow manifold and access newer markets. Now, the
India might seem to cast a suspicious glance at the intentions of the US private sector, but it is only so that it can grow its own. Both countries want free trade and vibrant markets.

same companies would like to restrict, either through laws or technological solutions, the same benefits to smaller players. Therefore, a stringent intellectual property regime is emerging. Net neutrality is contested. For countries like India, who have millions of small and medium entrepreneurs waiting to make their own millions online, fair playing rules are essential. The government has the responsibility to be able to provide its citizens a robust internet environment that lets them be producers, not just consumers of the global digital market. Therefore, India might seem to cast a suspicious glance at the intentions of the U.S. private sector, but it is only so that it can grow its own. Both countries want free trade and vibrant markets.

Ultimately, the domestic approaches of individual nation states in the areas sovereignty, jurisdiction and territory in the digital space will guide their approach to global governance. China, for example, has built its own critical infrastructure and can function independently of any global arrangements. The U.S., on the other hand, has its jurisdiction extend to ICANN, the body that assigns IP addresses and domain names across the world wide web. The question for Swing States such as India then becomes – will they be allowed to co-manage critical resources and retain their territory in the digital space? Or does the current system force them to follow another country’s lead? Would they rather invest in their own critical infrastructure, allowing them to engage with the global internet at will?

Given these points of departure, and certainly, convergence, it
would be mutually beneficial for the U.S. and India to explore a bi-
lateral treaty that paves the way for sovereign nations to sign agree-
ments for mutually beneficial trade. Such a treaty could also iron out
any issues of jurisdiction that might occur, as has been done in the
dual taxation policies. The co-sharing of critical infrastructure could
also be addressed. Such an agreement, for two of the most digitally
important countries of the world, would be a natural evolution.
Two countries who share so many common values; democracy, rule of law, freedom of expression, liberty, multiculturalism, freedom of religion, have not yet been able to operationalize a strategic partnership that would define the 21st century. Instead, that ‘big idea’ which could form the basis for the next phase of the U.S.-India relationship has seemed elusive. Indian strategic thinker, C. Raja Mohan, suggested in 2010 that this need not be the case, and the basis of this partnership could be the protection of the global commons – oceans, air, outer space and cyber. In this backdrop of the instability of these commons, and the growing pressure on U.S. ability to secure these spaces, Mohan suggests that since free flow of information and trade across these global commons is vital for both economies, India could serve as a natural ally for the U.S.\(^1\). Admittedly, this is not an easy task, especially in the area of

---

1 C Raja Mohan. ‘India, the United States and the Global Commons.’ Centre for a New American
the cyber domain. Misapprehensions about U.S. dominance, their capabilities and intent as revealed by the Snowden disclosures cast a shadow over common areas of interest. Yet both countries seem to understand there is much to be gained from closer collaboration, especially given the increasing intensity of threats to their digital boundaries, and State Responsibility in controlling the proliferation of such activities.

Globally, accusations citing cyber attacks from across borders are becoming increasingly common. In fact, many countries who been vocal about being the victims of cyber attacks, have been at times been perpetrators themselves. For example, the United States, which has in May 2014, indicted members of the Chinese military for engaging in acts of hacking and spying on U.S. businesses and entities, has itself being accused of launching the virus Stuxnet in 2010 (in collaboration with Israel) on Iran's nuclear centrifuges, destroying one-fifth of them. And in turn, Iran has been accused of ‘non-stop cyber attacks’ on major computer systems in Israel. There is also the 2014 case of Russian hackers attacking U.S. bank J.P. Morgan and stealing sensitive data to sell in the global black market. Some analysts suggest that these actions are in retaliation to Western economic sanctions against Russia. Therefore some common, global understanding of the rules of

---


Experts have pointed out that countries should share their military doctrines on how they will use cyber techniques for offensive purposes, to achieve international stability in cyberspace.

State behavior in cyberspace is needed. Currently, under Article 51 of the U.N. Charter, States, individually or collectively, have the right to defend themselves should an ‘armed attack’ occur. There is much work being done in the area of international law to understand the terms ‘armed act,’ ‘acts of aggression’ and ‘force’ when it relates to cyber, as there is no international consensus on the issue. And as witnessed in the U.S. case, acts of espionage (which have been attributed to the State, in this case China) are short of a cyber attack, but still considered to have significant consequences on the economy. Under these circumstances, and others that have preceded it, the global conversation has been veering towards chalking out rules of cyberspace.

Two schools of thought have emerged. The first is a solution put forward by China, Russia and a few other countries, is to have an international code of conduct with a view to protecting the information security. This has been formalized in the Eurasian grouping called the Shanghai Cooperation Organization. The members are China, Russia, Uzbekistan and Tajikistan, among others. India has observer status at the SCO and is up for full membership. Their 2009, Yekaterinburg Declaration stated: “the SCO member states stress the significance of the issue of ensuring international information security as one of the key elements of the common system

---

of international security.” In 2013, Russia and China submitted an ‘International Code of Conduct for Information Security’ to the United Nations4. The code dwells on information security in a few parts, including – “…curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment.”

This is the point of departure for many other nations, who are less concerned with ‘information security,’ often seen as securitization of free speech. Instead, prefer to focus on ‘network security’, that is, keeping the critical resources that keep cyberspace functioning protected. This is also the stated point of view of the U.S. To that end, some experts have pointed out that countries should share, to some extent, their military doctrines on how they will use cyber techniques for offensive purposes, to achieve international stability in cyberspace5. This also leads into the very pertinent question of what constitutes an act of war in cyberspace. Here, an argument has been made for the international community to shape ‘norms;’ to shape behavior and limit conflict in cyberspace. This view has been worked on at the United Nation's Group of Governmental Experts meetings, and has included U.S. and its NATO allies, India, and even

Experts have criticized the Talinn Manual’s narrow view of State Responsibility, saying that it gives the initiative to attackers, implying that large-scale cyber-intrusions are possible.

China. The third meeting of the GGE in June 2013 released its report, which concluded that, ‘international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment’. The non-binding exercise seeks to derive norms from existing laws. It also states: States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs.

Presently, the Tallinn Manual, produced by NATO (North Atlantic Treaty Organization) in 2013, seeks to examine how existing international norms apply to cyber ‘warfare’. It states in Rule 11 that “a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.” These operations are to be measured according to a variety of factors: severity, immediacy, directness, invasiveness, measurability of effects, military character of the cyber operation, extent of State involvement, and presumptive legality.


However, some experts have criticized its narrow view of State Responsibility, saying that it gives the initiative to attackers, sending the message that huge numbers of cyber-intrusions are possible with impunity. The question they ask is that does this encourage cyber-aggressive states to push the envelope\(^8\). The growing concern, understandably, is the protection of their critical infrastructure which are vulnerable to cyber attacks from all quarters. This is concern for the U.S. and India alike.

The reality is that even if digital forensics could trace the origin of a cyber attack, it can be extremely difficult to get States to even acknowledge there is non-state activity emanating from their territories. Indian security experts feel that in some cases, there will be a genuine lack of capacity to control cyber events on one’s soil; in other cases, some states could deliberately build ambiguity to mask their role. Another question worth considering is that the State complicit in a cyber attack either by financial or other forms of assistance?

Offline, India’s own experience with Pakistan, with an aim to control international terrorism, has not been very positive. The country maintains plausible deniability in supporting terror groups operating in Afghanistan and India, and the international system has

been unable to compel Pakistan to change its behavior. Add to this scenario, a statement made by India’s Minister for Communications and Information Technology to Parliament in July 2014: cyber attacks on India originate in the UAE, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the U.S.

The question then, for India and the U.S. is how can the global governance regime induce other States to reduce threats from their own borders. Norms that constrain cyber attacks is one strategy. This is also where their ‘big idea’ – of protecting the cyber commons – could, in part, be met with another strategy. Closer cooperation for technological solutions will complement the political solutions. Knowledge exchanges between their CERTs (Computer Emergency Response Teams), war games, educational, scientific and research cooperation, and other safeguards could help build formidable digital borders that rogue States and groups would not want to risk infiltrating.

Cooperation also includes strengthening the India-U.S. Counter Terrorism Initiative, established in 2009, which is continuing through India-U.S. strategic dialogue meets. However, there are some bottlenecks that need to be ironed out. As was visible in the

investigations that followed the horrific 2008 terror attacks, fissures can crop up between the intelligence agencies of both countries. At first, Indian intelligence agencies cried fowl that the U.S. had not shared information about terrorist David Headley with them. Later, India’s limited access to Headley revealed how much these information exchanges are susceptible to sovereign immunities. Both countries need to make a definite push to fix national legislation in order to share data about terrorist activities, unhindered by domestic laws. This is essential to safeguard this growing digital partnership.

Closer cooperation on digital forensics—and identifying the source of attacks—would, in the longer term, help simplify the application of international law in cyberspace. It would also provide a much-needed deterrent to States indulging in economic espionage and cyber crimes. A framework of cooperation is the order of the day, to keep stable and secure, the networks both countries so heavily rely on.
The U.S. and India face significant cybersecurity threats that jeopardize critical infrastructure, the freedoms that democracies exercise online, and the economic viability of businesses. The cybersecurity status quo is unstable, especially when considering the enormous and growing scope of these threats, particularly to the private sector. To mitigate these threats, this chapter provides a framework for legislative action that harnesses the power of U.S. and Indian industry and ingenuity, while safeguarding the freedoms and privacy of individual citizens. Through dynamic and cost-effective solutions, our respective law makers can make cyberspace a safer and more productive place.

The latent nature of this threat leads many in the private sector to forgo investment in security because it has not yet harmed their organization or because they mistakenly believe that they have nothing a cyber adversary would want. More important, they misunderstand that their own cyber insecurity has collateral effects on others—ef-
fects for which they are responsible. There is, therefore, a role for the central government to encourage actions that will improve the overall cybersecurity posture. That role, however, is not to set mandatory regulations. As the U.S. Government Accountability Office (GAO) has found, such an approach would be more like an anchor holding back U.S. entities while not providing additional security11.

India and the U.S. should reject a regulatory approach and adopt legislation that will actually improve cybersecurity. Such legislation must be able to adjust to the continuously developing challenge that is today's cyber environment. Additionally, any legislation must provide robust protection for privacy and individual freedoms. There are five key components that need to be included in truly effective cyber legislation:

1. Enabling information sharing instead of mandating it;
2. Encouraging the development of a viable cybersecurity liability and insurance system;
3. Creating a private-sector structure that fosters cyber-supply-chain security ratings;
4. Defining limited cyber self-defense standards for industry;
5. Advocating for more private-sector efforts to promote general awareness, education, and training across America;

**Regulation is not the Answer**

Proponents of a regulatory approach believe that regulation will improve the general cybersecurity posture. The problem is that heavy-handed government regulation is a 19th-century solution for a 21st-century problem. It simply will not help. Such proponents claim that “doing anything” is better than “doing nothing.” In fact, the regulatory approach can make matters worse than doing nothing. A network of regulations will force a slow and static compliance culture on the most dynamic technology the world has ever known. It will set a standard that will do nothing more than offer an invitation to adversaries in cyberspace. They will know that regardless of what that standard is, they only need to exceed it by the slightest bit to do severe damage. This clearly will not suffice if the goal is to improve the national cybersecurity posture instead of “just doing something” so that politicians and the public can feel better.

Regulation, particularly federal regulation, is slow, cumbersome, and static. Once in place, regulations are very difficult to remove or even change. This is exactly the wrong approach for dealing with the fast-moving and incredibly dynamic field of cybersecurity. Cybersecurity regulations will already be outdated on the day they are issued—and quick updates will not be possible. Faced with a slow, static standard, hackers, whether working independently or for another government, will easily circumvent the standard.

**There Is a Real Issue Here**

While there is disagreement over the correct role of the federal government in cybersecurity, there is little disagreement that something
must be done to improve the cybersecurity. The threats that India and the U.S face from adversaries in the cyber realm are real and daunting. Indeed there are three tiers of cyber threats to consider. First, cybercrime hits many Indians and Americans in the form of identity theft, phishing, or cyber vandalism. These crimes are usually committed by individual criminals, so-called hacktivists, or criminal organizations, and represent the most common form of cyber threat. Next is the threat of cyber espionage. Espionage pursues large, important targets, such as military blueprints or proprietary business plans, and is often state-sponsored. Finally, while cybercrime and espionage are serious problems, the U.S. and India also face a threat from cyber warfare. The ability to impair the functioning of critical systems, as a stand-alone attack or in connection with a kinetic attack, is a worrisome proposition. Taking down communications, transportation, or other systems would severely impair the U.S. response to a physical attack, increasing the damage sustained.

Nearly everyone understands that, for such serious problems, the respective federal governments have a role to play. Cyber legislation should contain the following six major components if it is to actually lower risk to private sector businesses and be sufficiently flexible to avoid a static culture of compliance.

**Information Sharing is the Key**

The first element of any legislation must be to enable and foster information sharing between the public and private sectors, and among private-sector entities themselves.
Effective information sharing is a critical and fundamental part of today’s cybersecurity measures. Various organizations and government agencies collect and analyze information regarding cyber threats and vulnerabilities. Examples of the types of shared information include analysis of a completely new cyber-attack that penetrated an entity’s system, or the discovery of a hole in the coding of a piece of software. This information is helpful to all cybersecurity actors as it allows them to prepare for these threats and patch or disable offending software.

Unfortunately, critical data on threats and vulnerabilities often remains locked within each company or organization due to different concerns and fears. These include fear of liability if shared information turns out to be wrong or causes unintended damage; concerns that sharing information could put proprietary information within the reach of Freedom of Information Act (FOIA) requests by competitors; and worries that shared information might be used against a company by regulators.

Our governments have their own rules, concerns, and processes that inhibit information sharing on its part. While these processes must be respected, they should not be considered sacrosanct. For example, the government is reluctant to share intelligence for fear of revealing classified “sources and methods.” This reluctance should be overcome by more appropriate classification of information and providing more clearances to appropriate personnel in the private sector. By opening up the process, industry’s confidence, trust, and ability to work with the government will improve, increasing oppor-
tunities for private and public collaboration.

There are four steps that can be taken to enable and encourage the needed cyber information sharing. First, we must remove barriers to voluntary private-sector sharing. Voluntary sharing will also allow organizations with manifest privacy concerns to simply avoid sharing their information, while still receiving helpful information from the government and other organizations.

Second, those entities that share information about cyber threats, vulnerabilities, and breaches should have legal protection. The fact that they shared data about an attack, or even a complete breach, with the authorities should never open them up to legal action. This is one of the biggest hindrances to sharing today, as it seems easier and safer to withhold information than to share it, even if it will benefit others. Strong liability protection is critical to expanding information sharing.

Third, the information that is shared must be exempted from Governmental systems like the U.S. FOIA requests and use by regulators. Without such protection, a competitor can get its hands on potentially proprietary information through a FOIA action. Alternatively, if information is shared with a regulator, it will dampen voluntary sharing, since organizations will fear a backlash from regulators, who could use shared information to penalize a regulated party or tighten rules.

Fourth, the government must be compelled to share information and intelligence with the private sector much more quickly and completely than it currently does. If that is not done, the private sector will never build any confidence that it is truly a partner in the fight to
Our respective law enforcement, military, and intelligence communities are not capable of addressing all cyber breaches and attacks that occur across the growing network of the cyber realm.

Maintain the security of computer networks.

**Cyber Insurance Will Encourage Responsibility**

The creation of a workable liability system often naturally leads to the development of an insurance system against liability. The insurance function allows a further spreading of risk in a way that fosters broad private-sector responsiveness. With enough data, insurance companies routinely and efficiently price the comparative costs and benefits of preventative actions and require cost-effective protective measures as a condition of insurance. Indeed, in maturing markets, insurance companies often take the lead in setting reasonable standards of care.

**Cyber-Supply-Chain Security Is Essential**

One of the biggest holes in the global cyber system is in the area of supply chain security, especially hardware and key infrastructure components.

Once malicious hardware has been built into a chip, a hardware attack can be initiated and act in a wide variety of ways. An attack can be internally triggered, based, for example on the arrival of a particular calendar day. Alternatively, an external trigger could be hidden within data sent by an attacker. More complex hybrid triggers could also be used. For example, a malicious circuit hidden within a GPS chip could be configured to attack only when the chip is located in a specific geographical area after a certain date.

This risk must be mitigated without impairing the highly effective global system that keeps cutting-edge technology affordable and
accessible to most people. The American Open Group consortium, an organization focused on improving businesses through IT standards, has developed the most viable model to deal with the supply chain, and it should be adapted by Congress. An effective cyber policy should establish a nonprofit organization that will evaluate and accredit technology companies’ supply chain security, even to the point of giving them grades.

For example, if a company has outstanding supply chain security across its entire global process, it would receive a high grade. Another firm might have a less comprehensive system and only receive a middling grade. Those companies with the highest grades would be able to charge higher prices for their technical equipment and software than companies with lower grades. This has the benefit of giving the consumer a way to “vote” on the level of security he or she feels is adequate and make better risk-based decisions on the acquisition of technical equipment. If an organization needed multiple systems for a certain budgeted amount, it might have to buy from a company with a lower grade. Again, market forces would push companies to have better security in order to have a competitive advantage, while allowing the consumer to make more informed choices.

**Cyber Self-Defense To Utilize All Assets**

Presently, there are no well-defined rules to tell businesses what they can and cannot do to establish self-defense mechanisms in the cyber domain. Our respective law enforcement, military, and intelligence communities are not capable of addressing all cyber breach-
Enable cyber information sharing by removing ambiguities, providing strong protections to sharers, and establishing a public-private partnership to facilitate sharing.

Awareness, Education, and Training Is Often Forgotten

The public in our two countries recognize that there is a problem with securing the cyber domain. They hear about it regularly on the news, and know, abstractly, that it is there. The difficulty is that they receive mixed messages. What the public lacks is consistent, accurate, and up-to-date information. More must be done by the private sector and local organizations to bring this issue to the attention of the public.

There must also be a viable program of professional base-level training that is encouraged for the general non-IT workforce. Nearly every job now involves the use of digital devices in some aspect of work. The general workforce must receive continuing education that goes beyond the present systems that accomplish little beyond checking off a box. These cyber “survival skills” should employ a dynamic curriculum, developed by the private sector, which keeps the...
workforce current and prevents it from being easily victimized. Any legislation should acknowledge this and encourage meaningful but dynamic training from nongovernmental sources.

**A Cybersecurity Policy that Works**

The U.S. and India should both pursue a unified cybersecurity policy that avoids a cumbersome and expensive regulatory approach and includes the five key elements that will produce truly dynamic cybersecurity defenses. Such an approach should:

- Enable cyber information sharing by removing ambiguities, providing strong protections to sharers, and establishing a public-private partnership to facilitate sharing. Entities that share cybersecurity information need certain protections. These protections include exempting all shared information from information search requests and regulatory use, and providing information sharers with strong liability protection. Effective information sharing requires the government to share fully and in a timely manner with the private sector through a public-private partnership.

- Promote the development of a viable cybersecurity insurance system. Liability for irresponsible cybersecurity actions should be established. Ultimately, such a system returns cybersecurity liability to those who are largely responsible for cybersecurity losses. The natural establishment of a cyber insurance community will then assist in the administration of risk assessments and foster improved security methodologies.

- Encourage the creation of cyber-supply-chain security ratings. Such
ratings should be granted by a nonprofit organization that will assess the surety of an organization’s supply chain. By promoting such ratings, consumers will be able to make risk-based decisions and support better security by tying it to their profit motive.

- Clarify boundaries and standards for cyber self-defense. The terms of an entity’s right to self-defense must be set within reasonable limits. Such terms would allow entities with the correct capabilities to take active measures to protect themselves without usurping the responsibility or authority of the government.

- Advocate more private-sector awareness, education, and training for the general population. Such an effort will ensure that the public becomes an asset, not a liability, in the struggle. Making the public more aware, without hype or feel-good security measures, is a start. Ongoing cyber education for the general workforce must also be promoted through standardized yet dynamic education programs, most likely originating in the private sector. This must be a major priority, not a minor ancillary effort.

Cybersecurity is one of the most critical issues we face today. The threats are real and the need is pressing. Despite the best intentions of those involved, a regulatory basis simply will not work. It will not improve security and may actually lower it by providing a false level of comfort and tying the private sector down with outdated regulations. Cyberspace’s dynamic nature must be acknowledged and addressed by policies that are equally dynamic, and that leverage market forces.
In the United States there is a real estate saying: The value of a home is based on “Location, location, location.” What is true of real estate is equally true of critical aspects of cybersecurity and computing services. It is an amazingly intricate question simply to determine whose law will apply to a dispute. Often the physical location of a piece of data or information is critical in determining which sovereign nation controls that data. Likewise the physical location of a criminal or a victim may determine the applicable law. And sometimes the laws will conflict, placing law-abiding citizens and corporations under inconsistent obligations. As a consequence one significant need it for a coordinated approach to the law of cyber crime and cyber jurisdiction.

The increase of legal uncertainty and jurisdictional problems is, to some degree, inevitable. In these times of economic constraint, users around the globe will seek solutions that promise savings, low overhead, and maintenance-free networks associated with remote

data storage or access. But one cost is often overlooked – the uncertainty of law and jurisdiction. This uncertainty is inherent in the distributed nature of a cloud-based service systems. Almost by definition, cloud-based adaptation takes advantage of the dispersed, globalized nature of the Internet.

But the Internet has a real world physical presence with its fiber optic transmission lines and server farms. Every data storage facility is located somewhere. And when that “somewhere” is not in the United States, Americans run the increased risk that the data stored overseas will be subject to the sovereign control of the country where the data is located. Likewise, for Indian companies whose data is stored overseas. If, as some say, geography is destiny, principles of good governance and caution require agreement between countries to better control their own destiny.

But today, there is no international standard that governs the question of data sovereignty. Nor is any multi-lateral institution likely to sponsor an agreement of this nature in the near future. Rather, disputes about the control of data are resolved on a case-by-case basis, often turning on geography and/or economic factors. Hence the time is ripe for an Indo-U.S. dialogue on the definition of and jurisdiction over cyber crime.

To date, however, the legal frameworks of the U.S. and India tend as much to diverge as they do to converge. While both see cyber intrusions as criminal in nature, their approaches differ and their assertions of jurisdiction will as often compete as they will cooperate.
The foundation of Indian criminal cyber law is the Information Technology Act of 2000 as amended in 2008. That law defines ‘Computer’ broadly to virtually any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities and therefore any high-end programmable gadgets like even a washing machine or switches and routers used in a network can all be brought under the definition. The 2008 amendments added “communications devices” to the scope of the law to insure that iPads or other similar devices on Wi-fi and cellular models were protected. Indian law, by contrast with American law, goes on to criminalize a series of particularized acts: offences such as the sending of offensive messages through communication service, misleading the recipient of the origin of such messages, dishonestly receiving stolen computers or other communication device, stealing electronic signature or identity such as using another persons’ password or electronic signature, cheating by personation through computer resource or a communication device, publicly publishing the information about any person’s location without prior permission or consent, cyber terrorism, the acts of access to a commuter resource without authorization, such acts which can lead to any injury to any person or result in damage or destruction of any property, while trying to contaminate the computer through any virus like Trojan etc.

American law has similar broad coverage. The Computer Fraud and Abuse Act (CFAA) does not speak with such specificity. Instead it makes it a crime to knowingly access a protected computer without authorization or exceeding authorized access – a definition that
more or less covers each of the areas specified under Indian law.

More interestingly, American law purports to have a wide jurisdiction. It begins by a protected device as any computer which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States. In effect, virtually every computer is within the scope of the law because virtually all communications on the network are interstate in nature. Indeed, given degree to which international traffic transits American servers this jurisdictional grant covers many computers in India and elsewhere around the globe.

By contrast, under Indian law the scope of territorial jurisdiction is confused and not satisfactorily addressed. Jurisdiction grants are identified as part of the judicial process and in identifying police powers, but without defining clearly the locus of the offense. Since cyber crimes are essentially borderless, this may lead to competing assertions of jurisdiction within India and between India and other nations.

The core of the problem then is that cyber crime is geography-agnostic, borderless, territory-free and generally spread over territories of several jurisdiction. At a minimum Indo-U.S. cooperation should attempt to define mutually agreed upon criteria for addressing issues that are of potentially joint concern. More ambitiously, they should seek to harmonize the approach to cyber crime and other security related issues and, in the end, create a joint task force structure for mutual assistance.
Ultimately, any agreement that emerges out of a U.S.-India conversation must first take into account the differing realities of these two countries. These have been written about: the differing sizes of the cyber markets and maturity of businesses in this domain as well as the differences in the stages of innovation, military preparedness, cyber capacity, overall connectivity, and even the state of the critical infrastructure industries. The different phases of evolution of the U.S. and Indian cyber domains have come to shape their respective policy approaches.

For the U.S., the market must be allowed to breathe and innovate in order to maintain the conditions that have so far helped the growth of the cyber industry. The U.S. is, therefore, keenly pushing values and policy imperatives that enable the internet to remain a free trade zone. Any cyber security policy decisions must protect U.S. government and businesses, while at the same time, not restrict their growth. The U.S. government is focusing much of its attention on
There should be a **digital agreement that apportions the jurisdiction across the value chain**, right from the time the digital communication is initiated to where the data rests.

Despite these differences in approach, the two countries are interested in addressing similar challenges, including cyber terrorism, the need for cyber security specialists, and the growing threat of cyber attacks. Both countries need to harmonize their approaches towards cyber crime, set standards of cyber security, and set out guidelines and protections for information sharing.

A dialogue on the issues mentioned is a healthy first step to securing cyberspace for ordinary users, businesses and the government. Settling the issues of cross-jurisdiction pertaining to cyber crime could be an area where the U.S. and India take the lead.

There should be a digital agreement that apportions the jurisdiction across the value chain, right from the time the digital communication is initiated to where the data rests. Shared jurisdiction should take into account various factors of cause and effect in a manner similar to the dual taxation policy that exists. This effort could build on the work done in the Budapest Convention.

There also is a need to address current internet governance struc-
tures. The question raised about ICANN’s jurisdiction is a pertinent one. Whereas currently U.S. jurisdiction applies, this may be unacceptable in the long run to India and other powers. The U.S. and other countries must consider whether moving ICANN under international law could help create broader consensus among nations.

The rise – and subsequent threat – from China brings both countries closer. So does the ever-growing threat of cyber attacks from non-state actors. Both countries have been working on norms of behavior in cyber space, an effort that should be sustained.

The question of harmonizing domestic law and processes might prove to be more complex, as India is at a nascent stage of its internet proliferation. Given that the Indian market will adopt the internet on a variety of low cost devices with low security standards, the government might well have to step in to ensure security standards. This is quite different from the U.S. market. Therefore, it could be an uphill challenge for U.S. companies to persuade Indian lawmakers to change their strategy. However, if the thrust of the Indo-U.S. interaction focuses on providing high security with low cost products, coupled with knowledge-sharing platforms, the two countries’ interactions on these issues might be more fruitful.

The U.S. and India have much to gain in deepening their cooperation in cyber security. If both sides work toward a unified approach to the challenges facing the cyber security world, it would signal that the digital leaders are ready to take on the responsibility to craft a more secure – yet more open – cyberspace.
Dr. Steven P. Bucci

Dr. Steven P. Bucci is the Director, Allison Center for Foreign and National Security Policy Studies. He is also Senior Fellow at the Heritage Foundation for all issues involving Homeland Security and Defense. He serves as a Subject Matter Expert for Cyber Security, Special Operations, and Defense Support to Civil Authorities. Bucci brings over 30 years of leadership at the highest levels of our Government in response to all security threats to America.

Bucci assumed the duties of the Military Assistant to the Secretary of Defense Donald H. Rumsfeld on 1 July 2001, saw the 9/11 attacks, the War on Terrorism, and led a team of 25 US military experts to Baghdad to directly assist the Coalition Provisional Authority. He daily reviewed all intelligence for the Secretary.

He was next appointed to serve as the Deputy Assistant Secretary of Defense, Homeland Defense and Defense Support to Civil Authorities. Bucci worked for three years for the IBM Corp. He is also an adjunct professor at George Mason Univ. in Leadership, and an Associate Professor at Long Island Univ. in Terrorism Studies and Cyber Security Policy.

Lisa A. Curtis

Lisa Curtis is Senior Research Fellow for South Asia in the Asian Studies Center at the Heritage Foundation. Since joining Heritage in August 2006, Curtis has appeared on major broadcast networks, including CNN, Fox News, PBS, and BBC, to comment on developments
in South Asia and testified over a dozen times before Congress on issues related to U.S. policy toward India, Pakistan, and Afghanistan. Her commentary has appeared in The Los Angeles Times, U.S. News and World Report, Foreign Policy, National Public Radio, and National Review Online, and in South Asian publications such as The Mint, India Outlook, The Friday Times, The News, and Express Tribune.

Before joining Heritage, she was Professional Staff Member of the Senate Foreign Relations Committee, handling the South Asia portfolio for then Committee Chairman, Senator Richard Lugar (R-IN). Curtis also served as Senior Advisor in the State Department’s South Asia Bureau (2001-2003); as an analyst in the Central Intelligence Agency (1998 – 2001); and as a diplomat in the U.S. embassies in Islamabad and in New Delhi (1994 to 1997).

Mahima Kaul, heads the Cyber and Media Initiative at the Observer Research Foundation, New Delhi and is also the editor of its monthly Cyber Monitor. The Initiative provides a vibrant platform for discussing internet policy issues in India. She is also Fellow at ORF. She is also an India Project Advisory Committee Member for Association for Progressive Communications (APC) and the European Union’s project “Advancing Internet Freedoms” which looks at internet freedom in India, Pakistan and Malaysia.

She has formerly worked at the Indian Express, produced programming for Al Jazeera, PBS and CCTV, as well as worked with the Digital Empowerment Foundation and Video Volunteers- NGOs using ICTs to enable social change in India. She regularly writes on internet related issues, and has been published at ORF, Index on Censorship, Internet Rights, Wall Street Journal, Mint among others. She was a panellist at the Stockholm Internet Forum, 2014, was nominated to the ORF- ZEIT-Stiftung Ebelin und Gerd Bucerius ‘Asian Forum for Global Governance’ in 2013 and was awarded an Emerging Leaders Fellowship at the Australia India Institute at the University of Melbourne in 2012.
Dr. C. Raja Mohan

Dr. Raja Mohan is a Distinguished Fellow at ORF and is leading the Strategic Studies Initiative of the Foundation. He is also a foreign affairs columnist for ‘The Indian Express’, a Visiting Research Professor at the Institute of South Asian Studies, Singapore, and a Non-Resident Senior Associate at the Carnegie Endowment for International Peace, Washington DC. Dr. Mohan served as the Diplomatic Editor and the Washington Correspondent of ‘The Hindu’ and the Strategic Affairs Editor of ‘The Indian Express’.

He is currently a member of India’s National Security Advisory Board and has served there earlier during 1998-2000 and 2004-06.


Paul Rosenzweig

Paul Rosenzweig is the founder of Red Branch Consulting PLLC, a homeland security consulting company, and a Senior Advisor to The Chertoff Group. Mr. Rosenzweig formerly served as Deputy Assistant Secretary for Policy in the Department of Homeland Security. He is a Distinguished Visiting Fellow at the Homeland Security Studies and Analysis Institute, serves as a Professorial Lecturer in Law at George Washington University, is a Senior Editor of the Journal of National Security Law & Policy, and a Visiting Fellow at The Heritage Foundation. He is a member of the American Bar Association Standing Committee on Law and National Security and a Contributing Editor of the Lawfare blog. In 2011 he was a Carnegie Fellow in National Security Journalism at the Medill School of Journalism, Northwestern University, where he now serves as an Adjunct Lecturer.
Mr. Rosenzweig is a cum laude graduate of the University of Chicago Law School. He has an M.S. in Chemical Oceanography from the Scripps Institution of Oceanography, University of California at San Diego and a B.A from Haverford College. Following graduation from law school he served as a law clerk to the Honorable R. Lanier Anderson, III of the United States Court of Appeals for the Eleventh Circuit.


Samir Saran

Samir Saran is Vice President at the Observer Research Foundation. He is the chair of Cyfy 2014, an annual property that is India’s premier international event on cyber security and cyber governance, bringing together government, industry, academia and civil society. He is also the editor of the CyFy journal. Samir is an International Fellow of the International Cyber Policy Centre at the Australian Strategic Policy Institute.

He frequently speaks about cyber security and governance at leading institutions including recently at the Naval War College, Goa, India and the National Defence University, Washington DC.

Apart from his academic publications, Samir is a prolific writer and contributes regularly to Indian and international newspapers. His upcoming publications include a joint research project between ORF and the Heritage Foundation, “Indo-US Cooperation on Internet Governance and Cyber Security” and “India, Internet Governance, and the International Telecommunication Union; A complex grey zone” for the Council on Foreign Relations.
Observer Research Foundation (ORF) is a not-for-profit, multidisciplinary public policy think tank engaged in developing and discussing policy alternatives on a wide range of issues of national and international significance. Some of ORF’s key areas of research include international relations, security affairs, politics and governance, resources management and economy and development. The fundamental objective of ORF is to influence formulation of policies for building a strong and prosperous India in a globalised world.

ORF pursues these goals by providing informed and productive inputs, in-depth research and stimulating discussions. Set up in 1990 during the troubled period of India’s transition from a protected economy to its new engagement with the international economic order, ORF examines critical policy problems facing the country and helps develop coherent policy responses in a rapidly changing global environment.

As an independent think tank, ORF develops and publishes informed and viable inputs for policymakers in the government and for the political and business leadership of the country. It maintains a range of informal contacts with politicians, policymakers, civil servants, business leaders and the media, in India and abroad. ORF publications are distributed widely to government officials and legislators, business leaders, journalists and academics. ORF’s principal research divisions are: Centre for International Relations, Institute of Security Studies, Centre for Economy and Development, Centre for Resources Management, and Centre for Politics and Governance. Headquartered in New Delhi, ORF has chapters in Chennai, Mumbai and Kolkata. More information about the Foundation is available at our website orfonline.org.
Founded in 1973, The Heritage Foundation is a research and educational institution—a think tank—whose mission is to formulate and promote conservative public policies based on the principles of free enterprise, limited government, individual freedom, traditional American values, and a strong national defense.

We believe the principles and ideas of the American Founding are worth conserving and renewing. As policy entrepreneurs, we believe the most effective solutions are consistent with those ideas and principles. Our vision is to build an America where freedom, opportunity, prosperity, and civil society flourish.

Heritage’s staff pursues this mission by performing timely, accurate research on key policy issues and effectively marketing these findings to our primary audiences: members of Congress, key congressional staff members, policymakers in the executive branch, the nation’s news media, and the academic and policy communities.
INDO-US COOPERATION ON INTERNET
GOVERNANCE & CYBERSECURITY

The Heritage Foundation
heritage.org

orfonline.org