The Heritage Foundation

ISSUE BRIEF

No. 4697 | MAY 1, 2017

Trump–Modi Agenda for Next Steps in U.S.–India Cybersecurity Cooperation

James Jay Carafano, PhD, Walter Lohman, David Inserra, Dean Cheng, Riley Walters, Paul Rosenzweig, and Steven P. Bucci, PhD

Malicious cyber activity from other states and non-state actors shows no sign of abating anytime soon. Both the U.S. and India have been working on behavioral norms in cyber space—an effort that should be sustained. Bad actors, however, do not respect norms. The U.S. and India need to take more proactive measures to keep cyberspace free, safe, and prosperous. Further, they can take additional steps together to set the standards for global cyber behavior, benefiting both countries and advancing the cause of regional stability.

In 2014, The Heritage Foundation and a New Delhi–based think tank Observer Research Foundation (ORF) produced a research study titled "Indo-U.S. Cooperation on Internet Governance and Cyber Security," which made the case that India and the U.S. build a foundation of mutual trust and cooperation in the cyber field.[1] Those recommendations could form part of an active bilateral agenda. President Trump and Prime Minister Modi could hold their first face-to-face meeting as early as next month. This meeting should conclude with a commitment to a joint agenda that includes cyber issues.

This paper, in its entirety, can be found at
http://report.heritage.org/ib4697

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

Framing the Challenge

One of the key findings of the joint Heritage/ORF study was that harmonizing domestic law and processes while promoting free-market principles and strong rule of law including individual privacy protections is complex and difficult. The Indian market has sought entry to the Internet through a variety of low-cost devices with low security standards, different from the U.S. market. These differences in standards present challenges for a U.S.–India joint agenda. However, if the thrust of the Indo–U.S. interaction focuses on providing low-cost devices with high security standards, coupled with knowledge-sharing platforms, U.S.–India interactions on these issues might be more fruitful.

The U.S. and India have much to gain from deepening their cooperation in cybersecurity. If both sides work towards a unified approach to the challenges facing the cybersecurity world, it would signal that the digital leaders are ready to take on the responsibility to craft a more secure—yet paradoxically more open—cyberspace.

President Trump and Prime Minister Modi should agree to pursue a joint cybersecurity policy that avoids a cumbersome and expensive regulatory approach, and instead 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 public-private partnerships to facilitate sharing.** Entities that share cybersecurity information need certain protections, such as 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 expediently 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. Such a system ultimately 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.** A nonprofit organization will assess the surety of an organization's supply chain and then grant these ratings. With such ratings available, 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 for cybersecurity. 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. Awareness, education, and training must be a major priority, not a minor ancillary effort.

The Way Forward

The U.S. should put some concrete proposals on the table to jump-start this agenda. Possible proposals include the following:

- **Internationalize the SAFETY Act.** The Support Antiterrorism by Fostering Effective Technologies (SAFETY) Act is an important tool to ensure the U.S. has the necessary security products to better prepare for, prevent, and mitigate the effects of terrorist attacks against the U.S. But the act has been sparingly used to encourage the development of cybersecurity products. The U.S. should make it clear that the SAFETY Act covers cybersecurity products, and seek to collaborate with allies and partners in expanding the program. Doing so will make the U.S. even better prepared to face the threats confronting the nation. India might consider developing a similar regime and the two countries could then look at developing reciprocity agreements for accepting SAFETY Act certification.

- **Establish a joint working group to discuss ways to push back against nation-state hackers that seek to steal intellectual property, undermine political institutions, or in other ways harm the security and prosperity of both the U.S. and India.** While the U.S. has so far indicted a handful of nation-state agents for hacking, the U.S. should work with India and other allies to punish such hacking that harms their respective nations. Doing so in a united fashion will be more powerful than individual countries acting alone or not at all. Sharing concepts, assessments, and best practices would be fruitful step.

- **Formalize the U.S.–India–Israel Trilateral Dialogue.** These countries already partner a great deal on cyber issues. Bringing the three of them together in a formal dialogue would jump-start cooperation and employ the capabilities and innovation that each bring to the table.

Agreeing on broad principles and initiating some practical, achievable pilot programs would spark

[1] Steven P. Bucci, Lisa A. Curtis, Mahima Kaul, C. Raja Mohan, Paul Rosenzweig, and Samir Sara, "Indo–U.S. Cooperation on Internet Governance and Cyber Security," The Heritage Foundation and Observer Research Foundation, October 2014, https://samirsaran.files.wordpress.com/2014/10/indo-us-cooperation-on-internet-governance-and-cyber-security1.pdf (accessed April 25, 2017).

cooperation between the U.S. and India on cyber matters and the broader strategic relationship between the nations. In their upcoming meeting, President Trump and Prime Minister Modi should commit to a joint agenda that includes these crucial steps.

*—**James Jay Carafano, PhD,** is Vice President for the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, and E. W. Richardson Fellow, at The Heritage Foundation. **Walter Lohman** is Director of the Asian Studies Center, of the Davis Institute. **David Inserra** is Policy Analyst for Homeland Security and Cyber Security in the Douglas and Sarah Allison Center for Foreign Policy, of the Davis Institute. **Dean Cheng** is a Senior Research Fellow in the Asian Studies Center. **Riley Walters** is a Research Associate in the Allison Center. **Paul Rosenzweig** is a Visiting Fellow in the Davis Institute. **Steven P. Bucci, PhD,** is a Visiting Fellow in the Allison Center.*