> It is clear that the world community is at a crossroads in its collective view of the internet and of the most optimal environment for the flourishing of the internet in this century. The internet is a global phenomenon that is providing enormous personal, social, and economic benefits to consumers, citizens, and societies in all areas of the world. It has grown exponentially over the past decade and continues to flourish and adapt to human needs everywhere. The entire world has benefited from this growth, and the developing countries are seeing higher growth rates than the developed world. The infrastructure of the global internet is shifting rapidly away from the transatlantic routes that formerly carried most traffic. The internet is becoming more regional and national and less centered in the U.S. and other Western countries. This is a welcome development.
>
> All of the benefits and growth of the internet have come as a result not of government action or of intergovernmental treaty. They are an organic expression of consumer demand and societal needs, along with other multi-stakeholder governance. We have every expectation that the internet will continue to grow and provide enormous benefits worldwide. The United States will continue to uphold and advance the multi-stakeholder model of internet governance, standards development, and management. No single organization or government can or should attempt to control the internet or dictate its future development.[15]

U.S. Efforts to Enhance Cybersecurity and to Counter International Theft of Trade Secrets

In February 2013, the U.S. administration announced separate, but related, initiatives to combat cyberattacks on critical U.S. infrastructure and to stop the theft of trade secrets.[1] The actions reflect growing concern at what officials see as increasingly pervasive penetration of U.S. private and government institutions, notably by hackers based in China.[2] In mid-February, Mandiant, a U.S. cybersecurity firm, released a sixty-page study[3] alleging that a unit of China's Peoples Liberation Army based in Shanghai, designated as P.L.A. Unit 61398, was responsible for massive thefts of data and trade secrets from U.S. and other firms. The report's conclusions are reportedly consistent with those of other private and government investigators.[4] (China's defense ministry challenged the Mandiant study; an official spokesman insisted that that "Chinese military forces have never supported any hacking activities."[5])

Protecting Critical Infrastructure. In February 2013, President Barack Obama issued a multipart executive order that, inter alia, directs U.S. government agencies to increase and expedite the sharing of information about cyberthreats to U.S. operators of power grids, pipelines, and

[15] U.S. Dep't of State Press Release, World Conference on International Telecommunications—Remarks by Ambassador Terry Kramer, U.S. Head of Delegation (Dec. 13, 2012), *at* http://www.state.gov/e/eb/rls/rm/2012/202040.htm.

[1] *See* David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies*, ASIL INSIGHTS (Mar. 20, 2013), *at* http://www.asil.org/insights130320.cfm.

[2] Craig Timberg & Ellen Nakashima, *China Has Hacked Most Washington Institutions, Experts Say*, WASH. POST, Feb. 21, 2013, at A1; David E. Sanger, *In Cyberspace, New Cold War*, N.Y. TIMES, Feb. 25, 2013, at A1.

[3] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (undated), *at* http://intelreport.mandiant.com/?gclid=CL7TkOenz7UCFeRlOgodZRIAvQ.

[4] David E. Sanger, David Barboza & Nicole Perlroth, *China's Army Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 19, 2013, at A1; William Wan & Ellen Nakashima, *Chinese Cyberspying Hits More Than 140 Targets, Report Says*, WASH. POST, Feb. 20, 2013, at A8.

[5] David Barboza, *China Denies Allegations of Conducting Cyberwarfare*, N.Y. TIMES, Feb. 21, 2013, at B2.

other critical infrastructure.[6] The order is fundamentally domestic in orientation,[7] but its introductory paragraphs indicate senior officials' concern at the threat to U.S. national security posed by cyberattacks.

> *Section 1. Policy.* Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.
>
> *Sec. 2. Critical Infrastructure.* As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[8]

Protecting Trade Secrets. A second, but related, area of U.S. government activity involves a multipart initiative to combat theft of U.S. companies' trade secrets by foreign competitors or governments.[9] In February 2013, the White House released a 141-page policy document prepared by several U.S. agencies setting out international and domestic measures intended to strengthen protection of trade secrets from theft. These measures include enhanced bilateral and multilateral diplomatic efforts, promotion of voluntary best practices, increased domestic law enforcement, and strengthened domestic legislation.[10] Victoria Espinel, the U.S. intellectual property enforcement coordinator, summarized the background and elements of this effort.

> Trade secret theft can cripple a company's competitive advantage in foreign markets, diminish export prospects around the globe, and put American jobs in jeopardy. The President is committed to preventing the theft of corporate trade secrets. As he clearly expressed in his State of the Union Speech, "we cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."
>
> The Strategy that we are releasing today coordinates and improves U.S. Government efforts to protect the innovation that drives the American economy and supports jobs in

[6] Exec. Order, Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[7] Michael Daniel, *Improving the Security of the Nation's Critical Infrastructure*, WHITE HOUSE BLOG (Feb. 13, 2013), *at* http://www.whitehouse.gov/blog/2013/02/13/improving-security-nation-s-critical-infrastructure?utm_source=related.

[8] Exec. Order, *supra* note 6.

[9] Ellen Nakashima, *White House Launches Effort to Deter Theft of Trade Secrets*, WASH. POST, Feb. 21, 2013, at A11.

[10] U.S. Defense Security Service, Administration Strategy on Mitigating the Theft of Trade Secrets (Feb. 2013), *at* http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

the United States. As the Strategy lays out, we are taking a whole of government approach to stop the theft of trade secrets by foreign competitors or foreign governments by any means—cyber or otherwise.

- First, we will increase our diplomatic engagement. Specifically, we will convey our concerns to countries where there are high incidents of trade secret theft with coordinated and sustained messages from the most senior levels of the Administration. We will build coalitions with countries that share our concerns to support our efforts. We will urge foreign law enforcement to do more. And we will use our trade policy tools to press other governments for better protection and enforcement.
- Second, we will support industry-led efforts to develop best practices to protect trade secrets and encourage companies to share with each other best practices that can mitigate the risk of trade secret theft.
- Third, [the U.S. Department of Justice] will continue to make the investigation and prosecution of trade secret theft by foreign competitors and foreign governments a top priority.[11] Additionally, the FBI and the intelligence community will provide warnings and threat assessments to the private sector on information and technology that are being targeted for theft by foreign competitors and foreign governments.
- Fourth, President Obama recently signed two pieces of legislation that will improve enforcement against trade secret theft. But we need to continue to make sure our laws are as effective as possible. So, moving forward, we will conduct a review of our laws to determine if further changes are needed to enhance enforcement. If changes are necessary, we will work with Congress to make those changes lasting and comprehensive.
- Lastly, we will increase public awareness of the threats and risks to the U.S. economy posed by trade secret theft.[12]

Jackson-Vanik Amendment Repealed; Magnitsky Provisions Draw Russian Ire and Termination of Adoption and Anticrime Agreements

In December 2012, the U.S. Congress overwhelmingly adopted, and President Obama approved, legislation[1] ending application of the Jackson-Vanik amendment to Russia and Moldova. The legislation allows the United States to extend "Permanent Normal Trade Relations" to Russia in compliance with U.S. obligations following Russia's entry into the World Trade Organization.[2] (The Jackson-Vanik amendment to the Trade Act of 1974[3] was adopted

[11] [Editor's note: *see* U.S. Dep't of Justice Press Release, Attorney General Eric Holder Speaks at the Administration Trade Secret Strategy Rollout (Feb. 20, 2013), *at* http://www.justice.gov/iso/opa/ag/speeches/2013/ag-speech-1302201.html.]

[12] White House Press Release, Launch of the Administration's Strategy to Mitigate Theft of U.S. Trade Secrets (Feb. 20, 2013), *at* http://www.whitehouse.gov/blog/2013/02/19/launch-administration-s-strategy-mitigate-theft-us-trade-secrets.

[1] The Russia and Moldova Jackson-Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012, Pub. L. No. 112-208, 126 Stat. 1496 (2012).

[2] Andrew E. Kramer, *U.S. Companies Worry About Impact of Russia Joining W.T.O.*, N.Y. TIMES, Aug. 22, 2012, at B5; Jeremy W. Peters, *Senate Passes Russian Trade Bill, with a Human Rights Caveat*, N.Y. TIMES, Dec. 7, 2012, at B4.

[3] Codified at 19 U.S.C. §2432(a).