US hypocritically denounces Chinese Internet spying

Thomas Gaist
9 March 2015

President Barack Obama issued criticisms and threats this week against the Chinese government over its "anti-terrorism" legislation, requiring technology companies operating in China to install special backdoors in their security systems and hand over encryption keys to Beijing.

In a staggering display of imperialist hypocrisy, Obama denounced the Chinese regime for seeking policy changes that closely parallel data-sharing arrangements already implemented by the US government and US tech firms over the past decade. Obama threatened to break off economic ties with China unless US firms are granted exemptions protecting their security systems from being compromised by Chinese intelligence.

"Those kinds of restrictive practices I think would, ironically, hurt the Chinese economy over the long term because I don't think there's any U.S. or European firm, any international firm that can credibly get away with that wholesale turning over of data, personal data over to a government," Obama said.

Beijing's proposed legislation, Obama continued, "would essentially force all foreign companies, including US companies, to turn over to the Chinese government mechanisms where they can snoop and keep track of all the users of those services."

"We have made it very clear to them that this is something they are going to have to change if they are to do business with the United States," Obama said. "As you might imagine, tech companies are not going to be willing to do that."

The hypocrisy of the American president is staggering. While the Chinese Stalinist regime is undoubtedly stepping up spying and Internet censorship aimed above all at the Chinese working class, the fact remains that Washington is the chief snooper and violator of privacy in the world. It presides over the most comprehensive surveillance system in human history.

For years, US internet and communications firms have turned over electronic data about citizens of the United States and of the world wholesale to US intelligence agencies, including the NSA. Through overlapping wiretapping and data mining programs, US intelligence collects and sifts through virtually all communications data stored on corporate servers worldwide.

Beginning with the Foreign Intelligence Surveillance Act (FISA) of 1978, the US Congress, executive branch and judiciary have overseen and sanctioned the erection of a parallel court system which rubber-stamps the vast majority of direct, warrantless requests for bulk data submitted by the government to the companies.

In the immediate aftermath the September 11 attacks, the Bush administration launched data mining operations inside central AT&T facilities as part of a secret contract with the company, seizing all telephone and internet data passing through AT&T hardware. By 2007, all of the leading US technology and communications transnationals, including Microsoft, Google, Yahoo and Facebook, granted the US government virtually unfettered access to their central servers as participants in the NSA's PRISM program.

NSA slides leaked by whistle-blower Edward Snowden boasted that PRISM gives the agency "extensive, in-depth surveillance on live communications and stored information" from the systems of participating "corporate partners." This includes real-time and archival search access to emails, online video and voice chats, Skype calls and social media data.

Significantly, the Chinese Communist Party (CCP)

defended its legislation by insisting that it is only copying the wholesale Internet spying carried out by Washington.

"This approach is also common with international practice and will not affect the legitimate interests of Internet firms." Fu Ying, spokesperson for the National People's Congress (NPC) said last week. "In reality, the U.S., U.K., and other Western countries have spent many years demanding that tech companies disclose their encryption methods."

Indeed, the CCP's demand for backdoors and access keys to corporate encryption and cybersecurity systems is virtually identical to those demanded by FBI Director James Comey in speeches given last year at the Brookings Institute and elsewhere.

Comey denounced even the most minimal safeguards to limit government surveillance of data stored on new generations of smart phones, insisting that Washington be granted backdoor access to all counter-surveillance technologies used by data and communications firms. Under Comey's leadership, the FBI pushed aggressively for expanded powers to install sophisticated surveillance malware on US-based computers without any legal or warranting process.

According to the *Washington Post*, the Chinese legislation is intensifying a "serious rift between Washington and Beijing over cyberspace." The US media is abetting the anti-China drive by promoting fear campaigns based on unsubstantiated allegations about Chinese hacking and cyber-warfare against US firms and institutions.

Similar efforts to drum up hysteria against alleged Chinese hacking were severely discredited shortly after they emerged in the spring of 2013, when documents leaked by NSA whistleblower Edward Snowden showed conclusively that illegal US surveillance programs are targeting not only China's basic Internet infrastructure, but the population of the entire world.

Snowden revealed elaborate hacking, sabotage and infiltration operations run by the NSA, CIA and Pentagon targeting Chinese academic, military and corporate institutions. This is part of a broader agenda announced in 2011 with Washington's "pivot to Asia," aimed at isolating China in Asia and threatening it with war.

Since then, the Obama administration has tightened a US military encirclement of China that includes massive naval, air and ground deployments throughout the North Pacific Ocean, while rallying an anti-China military bloc including Japan, Vietnam, and South Korea to ratchet up the pressure on China's southern and eastern flanks.

Even as Obama blasted the proposed legislation, the *Beijing Morning Post* reported this week that the US Navy is conducting blanket spying against the Chinese coast, tracking the movement of all Chinese vessels.

There are indications that official fears about US political and strategic pressure are a main driver of the CCP's new data mining protocols. These protocols require Chinese state agencies to closely monitor financial flows to non-governmental organizations (NGOs), including foreign activist, non-profit, and other "civil society" groups.

Such organizations have been used extensively to organize CIA-backed regime change operations in countries in Europe and the former USSR, including Serbia, Georgia, and Ukraine.

Chinese leaders justified their new surveillance laws by citing separatist groups in China's Western provinces, some of which receive backing from the CIA and other US government agencies.