



China Demands High-level Silicon Valley Attendees at Seattle Conference

The Chinese invitation extended to senior executives at major Silicon Valley firms was no invitation <u>but a command</u>: Be there, or lose any chance to exploit business opportunities in China.

The annual Seattle conference in the past has been primarily directed to midlevel management at companies such as Amazon, Apple, Microsoft, Google, and Facebook. But this year, taking advantage of China's President Xi Jinping's planned visit with President Obama, the date of the conference was moved up, and the invitation/command was extended to the senior executive officers. The carrot offered was a presentation by Xi himself.



The threat was reiterated, for anyone who didn't get the message, in an interview the *Wall Street Journal* did with Xi:

Together, China and the United States account for one-third of the world economy, one-fourth of the global population, and one-fifth of global trade.

If two big countries like ours do not cooperate with each other, just imagine what will happen to the world.

Message delivered: Be there, or miss out. After all, U.S. companies invested more than \$60 billion in China last year, and total trade between the two countries topped \$600 billion.

As Atlantic Council Senior Fellow Jason Healey pointed out, "It's not really voluntary. They [those senior executives] are absolutely expected to be there, and be there in force."

Dutifully, they showed up: Satya Nadella of Microsoft, Tim Cook of Apple, Jeff Bezos of Amazon, John Chambers of Cisco Systems, along with 11 other high-level executives.

They were greeted by President Xi, who was generosity and optimism personified. Xi claimed that, despite recent rumors of a slowdown in China, his country would maintain "relatively high" growth for a long time. This would, for those not paying attention, create huge opportunities to companies willing to play along and ignore any concerns they might have over the current cyberwarfare being waged by his country on those very same companies he was addressing.

That cyberwarfare is massive and continuing. One good example, although certainly not the only one, is Operation Aurora, which began in mid-2009 and was disclosed by Google in January 2012. Google's memo identified the source as China's People's Liberation Army (PLA), which had aimed its attacks at 34 companies, including Adobe Systems, Juniper Networks, Yahoo, Symantec, Northrop Grumman, Morgan Stanley, and Dow Chemical. Research by McAfee Labs uncovered the purpose of Operation



Written by **Bob Adelmann** on September 24, 2015



Aurora: to gain access to and potentially modify source codes at these companies so it could steal secret and vital intellectual property useful for the Chinese companies competing with them.

On May 19, 2014, the U.S. Department of Justice announced that a federal grand jury had indicted five PLA officers *in absentia* for stealing confidential business information and intellectual property from those firms and for planting malware on their computers.

A congressional advisory group has declared that China is "the single greatest risk to the security of American technologies," noting that "there has been a marked increase in cyber intrusions originating in China ... targeting U.S. government and defense-related computer systems." The *Washington Post* explained that those intrusions are so sophisticated that computer users are unaware that they are being spied upon: The infected attachment is disguised as an e-mail from a familiar contact, fooling him into opening it and setting off a program that infects his computer. It's so elegant that the malware is hidden by "rootkits," which prevent the user from being aware that his computer has been infected and vital data stolen.

President Xi said little about these concerns to the top executives he commanded to attend in Seattle, but reminded them instead that if they wanted to continue to exploit the Chinese market they must play by new rules. In July Xi's dictatorship passed a national security law that now requires technology being used within the country to be "secure and controllable" — defined as being open to surveillance by his government security officials. Beijing is now pressing companies wishing to continue to do business there to sign a pledge promising to store data within the country in a manner that would comply with the new law. Experts claim that going along with such a law would not only eliminate privacy for their customers but could also open those companies' computer source codes to intrusive inspections by Xi's technicians and spies.

Adam Segal, a Chinese cyberpolicy expert and senior fellow at the Council on Foreign Relations, explained the pickle these companies having willingly placed themselves in, by agreeing to sleep with the enemy:

U.S. companies have lots of conflicting interests. While they want the cyber hacking to end, they also do a huge amount of business in China and they want that to continue and grow.

As the saying goes: When one sleeps with big dogs, he gets big fleas.

Photo of Silicon Valley: $\underline{\text{Coolcaesar}}$

A graduate of an Ivy League school and a former investment advisor, Bob is a regular contributor to The New American magazine and blogs frequently at www.LightFromTheRight.com, primarily on economics and politics.





Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



Subscribe

What's Included?

24 Issues Per Year
Optional Print Edition
Digital Edition Access
Exclusive Subscriber Content
Audio provided for all articles
Unlimited access to past issues
Coming Soon! Ad FREE
60-Day money back guarantee!
Cancel anytime.