Kauppalehti

Artikkeli on julkaistu Kauppalehdessä http://www.kauppalehti.fi/.

Martin Kenney: Silicon Valley's Spy Problem

Keskiviikko 02.07.2014 klo 18:50 (päivitetty to 13:57)

The latest revelations are threatening the American IT sector's global dominance, writes Martin Kennedy, Professor at the University of California.

In a recent letter to US President Barack Obama, the CEO of Cisco Systems, John Chambers, requested that the National Security Agency stop intercepting the company's products to install devices for spying on foreign customers. This is the latest in a series of revelations of how US information-technology firms have been enlisted, knowingly or otherwise, in the "war on terror" – revelations that are threatening the American IT sector's global dominance.Since the scale of the NSA's Internet eavesdropping came to light, governments and large companies outside of the United States are questioning the capacity of American IT firms to guarantee their products' security. America's central position in the world's information economy, which seemed secure just two years ago, is now under threat – a fact that should raise serious concerns for every entrepreneur, executive, employee, and venture capitalist in the American industry.There is more than a little irony in this turn of events. America's global IT leadership, after all, can be traced directly to its national security apparatus. Following World War II, and especially after the Soviet Union's launch of the Sputnik satellite in 1957, the US made massive investments in electrical engineering and, later, computer science.Cost-plus contracting allowed what were then small technology firms like Hewlett-Packard and Fairchild Semiconductor to charge the Department of Defense for the price of research and development that none could pay on its own. This enabled the firms to create technology products that eventually created entire new markets and economic sectors.The US government also made massive, continuous investments in university-based research, boosting the country's supply of engineers and scientists. These highly trained people created countless new technologies, including computer graphics, semiconductors, networking equipment, groundbreaking software, and the Internet itself.In fact, the US government remains a critical supporter of scientific and engineering research to this day. In 2012, the defense department invested $1.3 billion in electrical engineering and computer science alone, while the National Science Foundation invested another $900 million. The US military has provided a particularly large amount of funding to university researchers in computer security and encryption.With so many of America's top entrepreneurs, executives, and researchers having received support from the defense department, it is no surprise that Google's founders and executives, for example, have exchanged friendly emails with NSA officials. Professional and personal connections made recruiting corporate leaders to the anti-terror war relatively easy. Few, it seems, considered the potential consequences of their participation.The resulting relationship between Silicon Valley and Washington, DC, is remarkable for its longevity and depth. For example, the database software giant Oracle has been rumored to maintain close ties with the CIA. Similarly, the partly CIA-funded Keyhole, Inc., was among the acquisitions that produced Google Maps. The CIA's Silicon Valley venture-capital operation, In-Q-Tel is meant to ensure that the interests of America's national security apparatus are implanted in technology startups.The consequence of these ties is that America's IT industry has become an

agent of the national security state. This undermines consumers' faith in firms' willingness or ability to guarantee their privacy, while making it difficult for companies to claim the moral high ground when, say, China's government restricts their domestic operations.Given that America's IT sector is so far ahead globally, the impact of these perceptions will remain largely localized in the short term. But, as European and Asian IT firms catch up, America's advantage will gradually deteriorate.Foreign customers' search for alternatives is underway in both existing and emerging industries. For example, Oracle is experiencing a slowdown in the Asia-Pacific region, where its main competitor, the German company SAP, is thriving. And the competition that Cisco faces from Huawei of China is what likely drove Chambers' recent appeal to Obama. In one of the newest IT fields, cloud computing, where US firms are pioneers, firms and entrepreneurs in many countries are exploring the creation of non-US alternatives.Preventing this self-inflicted threat to America's IT preeminence will require strong action by US political leaders, who are responsible for this dangerous trend. First and foremost, Obama, with support from Congress, must demand the release of all information regarding interactions between national security agencies and American IT firms.Furthermore, corporations and privacy advocates should be encouraged to use the court system to challenge government requests to install spy software in commercial products. If the government's agents break privacy laws, at home or abroad, the Department of Justice should prosecute them to the full extent of the law.Given how extensively the NSA's activities have degraded global trust in America's government and IT sector, nothing less than complete transparency is required. It is time for US leaders to place the well-being of the high-tech wealth machine – which cost US taxpayers tens of billions of dollars to build – above the illusory notion that the only route to safety is unfettered access to the world's digital traffic.*Martin Kenney is a professor at the University of California, Davis, and a senior project director at the Berkeley Roundtable on the International Economy at the University of California, Berkeley.*