GlobalResearch
Center for Research on Globalization

Cyberwarfare: Irresponsible China Bashing

By Stephen Lendman
Global Research, May 21, 2014

Region: Asia
Theme: Intelligence, Law and Justice

China bashing reflects official US policy. Washington does it numerous ways.

It's reprehensible. It's confrontational. It's potentially belligerent. Rogue states operate this way.

No nation spies on more nations than America. None more intrusively. None more aggressively. None more lawlessly.

None for more reasons. None in more ways. None more duplicitous about it. None more involved in cybercrime. More on this below.

China is a major US economic, political and military rival. Washington wants it marginalized, weakened and isolated.

It wants its sovereign independence eliminated. It want pro-Western puppet governance replacing it.

It wants its resources plundered. It wants its people exploited. Bashing China risks open conflict. So does pursuing America's overall imperial objectives.

On May 19, Washington declared unprecedented cyberwar on China.

The Justice Department headlined "US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage"

> "First Time Criminal Charges Are Filed Against Known State Actors for Hacking"

A federal grand jury indicted five Chinese Peoples Liberation Army officials. Doing so was unprecedented. It was provocative.

Individuals charged didn't matter. Washington confronted the People's Republic of China directly. It did so by targeting its military.

Charges include "computer hacking, economic espionage and other offenses directed at six American victims in US nuclear power, metals and solar products industries."

They allege conspiracy "to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs)."

Attorney General Eric Holder claimed "economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking."

“The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response,” he said.

FBI Director James Comey claimed “(f)or too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries.”

Assistant Attorney General for National Security John Carlin said:

> “State actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country’s flag.”

Third Department Chinese People’s Liberation Army (PLA) Unit 61398 officials named include Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui.

Alleged companies targeted include Westinghouse, SolarWorld subsidiaries, US Steel, Allegheny Technologies, Alcoa, “the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, (and) Allied Industrial and Service Workers International Union (USW).”

Charges include:

- One count of “conspiring to commit computer fraud and abuse.”
- Eight counts of “accessing (or attempting to access) a protected computer without authorization to obtain information for the purpose of commercial advantage and private financial gain.”
- Fourteen counts of “transmitting a program, information, code, or command with the intent to cause damage to protected computers.”
- Six counts of “aggravated identify theft.”
- One count of “economic espionage.”
- One count of “trade secret theft.”

Xinhua is China’s official press agency. It’s a ministry-level department. It provides electronic and print news and information.

On May 20, it headlined “China strongly opposes US indictment against Chinese military personnel,” saying:

> “China lodged protests with the US side following the announcement, urging the U.S. side to immediately correct its mistake and withdraw the indictment.”
>
> “(T)he position of the Chinese government on cyber security is consistent and clear-cut. China is steadfast in upholding cyber security.”
>
> “The Chinese government, the Chinese military and their relevant personnel have never

engaged or participated in cyber theft of trade secrets."

"The US accusation against Chinese personnel is groundless with ulterior motives."

Evidence shows "terminals of Chinese military access to the internet have suffered from great number of foreign cyber attacks in recent years, and a considerable number of such attacks originated from the United States."

"China demands that the US side explain its cyber theft, eavesdropping and surveillance activities against China and immediately stop such activities."

America is "the biggest attacker of China's cyber space."

US attacks "infiltrate and tap Chinese networks belonging to governments, institutions, enterprises, universities and major communication backbone networks."

"Those activities target Chinese leaders, ordinary citizens and anyone with a mobile phone."

Foreign Ministry spokesman Qin Gang said:

"This US move, which is based on fabricated facts, grossly violates the basic norms governing international relations and jeopardizes China-U.S. cooperation and mutual trust."

Nine or more major online companies cooperate with lawless NSA spying. Google, Microsoft, Yahoo, Facebook, Apple, Skype, YouTube and others are involved.

They do so through NSA's Prism. It gains access to search histories, emails, file transfers and live chats.

It's gotten directly from US provider servers. Doing so facilitates mass surveillance. NSA spies globally. Its activities reveal rogue agency lawlessness.

NSA targets China intensively. It lawlessly hacks its computer and telecommunications networks.

It focuses on strategically important information. It does so through its ultra-secret China hacking group.

It conducts cyber-espionage. Huang Chengquing is Beijing's top Internet official. China has "mountains of data," he said.

It reveals widespread US hacking. It's designed to steal government secrets. NSA's Tailored Access Operations (TAO) in involved.

It's ultra-secret. Most NSA personnel and officials know little or nothing about it. Only those with a need to know have full access.

TAO operations are extraordinarily sensitive. They penetrate Chinese computer and telecommunications systems.

They've done so for nearly 16 years. They generate reliable intelligence. They learn what's

ongoing in China.

They obtain what Washington most wants to know. It's done by surreptitious hacking.

It cracks passwords. It penetrates computer security systems. It decrypts successfully. It steals hard drive data.

In October 2012, Obama authorized cyber-attacks. He did so by secret presidential directive.

His Offensive Cyber Effects Operations (OCEO) "offer(s) unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."

Washington "identif(ies) potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power."

Domestic spying works the same way. Anything goes defines policy. Constitutional protections don't matter. Or US statute laws. Or international ones. Or relations with other nations.

Washington rules alone apply. TAO's mandate is penetrating, destroying, damaging, or otherwise compromising targeted sites.

It's the largest, most important NSA Signal Intelligence (SIGINT) Directorate component.

Well over 1,000 military and civilian computer hackers, intelligence analysts, targeting specialists, computer hardware and software designers, and electrical engineers are involved.

Their job is identifying sensitive computer systems and supporting telecommunications networks. Their mandate is penetrating them successfully.

They exceed the capability of other US intelligence gathering agencies. Their activities expand exponentially.

China knows what's going on. So do Russia and other nations. They're acutely aware of NSA activities. They knows the threat. They take appropriate countermeasures.

Cyber-attacks constitute war by other means. Doing so compromises freedom. It risks confrontation. It threatens world peace.

It doesn't matter. America operates solely for its own self-interest. For control. For economic advantage.

For being one up on foreign competitors. For information used advantageously in trade, political, and military relations. NSA's get it all mandate explains.

June 5 is a landmark date. It marks the first anniversary of Edward Snowden revelations. He connected important dots for millions.

He revealed lawless NSA spying. He did so in great detail. He's the gift that keeps on giving.

Western nations collaborate irresponsibly. They do so with major corporations. Privacy no longer exists.

There's no place to hide. Big Brother watches everyone. Spying goes way beyond protecting national security.

All electronic communications can be monitored, collected and stored. Legal restraints are absent.

Obama heads the most rogue administration in US history. He exceeds the worst of his predecessors. Congress and American courts permit the impermissible.

Mass US surveillance is standard practice. It's global. It's all- embracing. It targets world leaders. It's after everything and everyone of possible interest.

No constraints exist. No standards. Rogue states operate this way. America is by far the worst.

Bashing China turns a blind eye to US high crimes. They're too egregious to ignore.

America is a pariah state. It exceeds the worst in world history. It risks global confrontation. Stopping it matters most.

It bears repeating what previous articles stressed. Today is the most perilous time in world history. World peace hangs in the balance.

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net.

His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III."

http://www.claritypress.com/LendmanIII.html

Visit his blog site at sjlendman.blogspot.com.

Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network.

It airs three times weekly: live on Sundays at 1PM Central time plus two prerecorded archived programs.

http://www.progressiveradionetwork.com/the-progressive-news-hour

---

Articles by: Stephen Lendman

About the author:

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net. His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III." http://www.claritypress.com/LendmanIII.html Visit his blog site at sjlendman.blogspot.com. Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network. It airs three times weekly: live on Sundays at 1PM Central time plus two prerecorded archived programs.