From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 26 • NUMBER 1 • Fall 2020
$15 SINGLE COPY PRICE

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
7700 LEESBURG PIKE, SUITE 324
FALLS CHURCH, VIRGINIA 22043
WEB: WWW.AFIO.COM * E-MAIL: AFIO@AFIO.COM

Chinese Offensive Intelligence Operations[1]

by Peter C. Oleson

China poses "a more severe counterintelligence threat" to the US than any other country – including Russia, FBI Director Christopher Wray told the Senate Judiciary Committee on July 23, 2019.[2] The entities controlled by the Communist Party of China (CCP) have engaged in an extremely broad-scale, and highly sophisticated, intelligence campaign against the West to promote its military, scientific and economic prowess.

The Internet, a principal tool of modern communications, has made life easier for many things – including spying, conducting information operations, and cyber warfare. While the ARPANet, which over time became the Internet, was conceived to be an open and free environment, allowing people to share information without restriction, that freedom is anathema to authoritarian governments such as the CCP.

While the Chinese have embraced the Internet, the CCP has not. Why? The free exchange of information also allows criticism of the ruling party. So, from a totalitarian point of view, the Internet *MUST* be controlled.

Domestically, the Chinese authorities go to great lengths to prevent access to Internet sites that are deemed "subversive." Nicknamed "the Great Firewall of China," this includes:

- Any content deemed unfavorable to China. Over 18,000 websites
- Gmail, Google, YouTube, Facebook, Instagram (all Google products);
- Many VPN providers; and
- Intermittently, Twitter, Hotmail, and Flickr.[3]

The domestic impact of Chinese government cyber restrictions are clearly intended to stymie any democratic movement. A major focus of the PRC's cyber operations, however, are international. In the cyber arena the Chinese are one of the world's major players. They employ advanced techniques for hacking, traditional and economic espionage, and shaping the information environment. So, what has China done? It has stolen:

- The design of the F-35 fifth generation fighter;
- The Patriot and THAAD surface-to-air missiles;
- Stealth technology related to suppressing infrared signatures;
- The Navy's signal intelligence collection capabilities;
- The W88 and neutron bomb designs;
- Quiet submarine technologies;
- Littoral Combat Ship design, and many other military-related technologies.[4]

Economic cyber espionage has been prolific. Major sectors targeted include computers and robotics, biomedicine and medical technology, pharmaceuticals, manufacturing technology, the energy field, and finance and consumer products. Estimates of the cost of such espionage is in the 100's of billions of dollars per year.[5]

This effort is not just for military or strategic economic superiority, but also commercial advantage. One case involved Dupont, from which China stole the formulas for paint.[6] Another example was Coca Cola's trade secrets for coating the inside of cans.[7] Other vic-

1. This article is derived from comments prepared for a panel on the Chinese cyber warfare threat to democracy at the East-West Center in Honolulu in March 2020, but cancelled due to the Covid-19 pandemic.
2. Cybersecurity 202 (*Washington Post*), July 24, 2019.
3. See "List of Blocked Websites and Apps in China 2020," Travel China Cheaper website, *https://www.travelchinacheaper.com/index-blocked-websites-in-china*. Retrieved April 7, 2020. Updated periodically. Also see *https://cyber.harvard.edu/filtering/china/China-highlights.html* for details on specific blocked sites.
4. See *Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China*, (Cox Report), House of Representatives, May 1999. See also "Hawaii Man Sentenced to 32 Years in Prison for Providing Defense Information and Services to People's Republic of China. Former B-2 Bomber Engineer Helped PRC Design Stealthy Cruise Missile," Office of Public Affairs, US Department of Justice, January 25, 2011; *https://cicentre.com/page/LIN_Edward*; *https://cicentre.com/page/MAK_Chi*; Ellen Nakashima & Paul Sonne, "China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare," *Washington Post*, June 8, 2018.
5. "Primary Targets of Chinese Espionage," Oleson graphic 2020. During an interview with Bill Evanina, director of the National Counterintelligence and Security Center (NCSC) in the weekly Sunday news program *Full Measure* the host cited 2015 losses to Chinese espionage to be $450 million. *http://fullmeasure.news/news/terrorism-security/stolen-secrets*.
6. Del Quentin Wilber, "Stealing White," *Bloomberg Businessweek*, February 4, 2016, *https://www.bloomberg.com/features/2016-stealing-dupont-white/*.
7. Kate O'Keeffe & Anna Viswanatha, "Former Coke Scientist Accused

Primary Targets of Chinese Espionage

IT & Robotic Systems	Transportation / Machinery
Microchips *	High-tech maritime vessel construction *
Semiconductors *	Maritime technology & equipment *
Robotics *	Agricultural machinery
Navigation *	Aerospace technologies & equipment *
Command & control systems *	
Artificial Intelligence (AI) *	**Energy Technology & Equipment**
Distributed computing *	Technologies for renewable energy
High performance computing systems *	Power equipment
	Nuclear power and weapons technologies *
Medicine	
Pharmaceuticals	**Commercial Technologies**
Bioengineering technologies	Manufacturing technologies & R&D

*Dual use civil/military applications

tims include Apple, Alcoa, Austal, and the diamond coated glass developed by Akhan Semiconductor.[8] The breadth of Chinese economic espionage indicates there are no limits to such espionage, if it helps the Chinese economy.

China has used the cyber realm to support the aggressive recruiting of spies, both in the US and elsewhere. LinkedIn is an important source for Chinese intelligence. "Instead of dispatching spies to the US to recruit a single target, it's more efficient to sit behind a computer in China and send out friend requests to thousands of targets using fake profiles," stated Bill Evanina, director of the National Counterintelligence and Security Center (NCSC).[9] China's theft in 2015 of 23 million personnel records of Americans with security clearances is believed to be another source of identifying potential agents to recruit. Those who work or have worked for US intelligence or law enforcement have been targets. Cases include Kun Shan Chun, an FBI electronics technician in New York City; CIA case officers Jerry Chun Shing Lee and Kevin Mallory, and DIA employee Ron Hansen.[10] In Australia, China tried to plant a spy in Parliament.[11]

It has also used human agents to insert malware to enable cyber operations. One example is the recent case of Yujing Zhang, who was arrested trying to penetrate Mar-a-Lago with malware on her person.[12]

With so many electronic components produced in China for telecommunications products there is a legitimate concern about the integrity of the supply chain. The introduction of "back doors"[13] or other malware can turn one's cellphone into a spy device.[14] There is considerable concern over Huawei's aggressive pushing of 5G technologies and the potential threats to privacy its products have. Huawei's association with past cases of industrial espionage is a cause of concern.[15] (See sidebar on page 12: "Huawei and the 5G Issue.") Also of concern is China's 2017 National Security Law that mandates that Chinese companies cooperate with the government, which includes the PLA and Ministry of State Security, both prolific cyber hackers.[16]

China has used the point of presence of China Telecom sites to hijack Internet traffic, routing messages via China instead of via the most efficient route as called for by Internet protocols. This enables the copying and collection of massive amounts of data.[17] "A point of presence is a major point of connection where a long-distance telecommunications carrier... connects to a local network and picks up local traf-

of Stealing Trade Secrets for Chinese Venture," *Wall Street Journal*, February 14, 2019. *https://www.wsj.com/articles/chinese-born-u-s-citizen-charged-with-stealing-trade-secrets-11550177074*.

8. Erik Schatzker, "Huawei Sting Offers Rare Glimpse of the US Targeting a Chinese Giant," *Bloomberg Businessweek*, February 3, 2019. *https://www.bloomberg.com/news/features/2019-02-04/huawei-sting-offers-rare-glimpse-of-u-s-targeting-chinese-giant*.

9. FP Security Brief Plus, August 29, 2019.

10. See Press release, US Attorney for the Southern District of New York, January 20, 2017; Office of Public Affairs, "Justice News," Department of Justice, May 1, 2019 and September 24, 2019.

11. Giovanni Torre, "Australia investigates 'China plot to plant spy in Parliament' as Scott Morrison insists 'not naïve' to threat," *The Telegraph*, November 25, 2019. *https://www.telegraph.co.uk/news/2019/11/25/australia-investigates-china-plot-plant-spy-parliament-scott/*.

12. Jane Musgrave, "Chinese woman who trespassed at Donald Trump's Mar-a-Lago has been sentenced to prison, will be deported," *Palm Beach (Fla.) Post*, November 25, 2019. *https://www.usatoday.com/story/news/nation/2019/11/25/yujing-zhang-mar-a-lago-trespasser-prison/4303532002/*.

13. "Backdoor is an undocumented way of gaining access to a program, online service or an entire computer system. A backdoor will bypass normal authentication mechanisms." (Angie Beal, "Backdoor access," *https://www.webopedia.com/TERM/B/backdoor.html*.)

14. Kelly Sheridan, "Chinese Malware Found Preinstalled on US Government-funded Phones," *InformationWeek*. *https://www.darkreading.com/threat-intelligence/chinese-malware-foun...unded-phones/d/d-id/1336771?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple*.

15. Tim Lee, "US indicts Huawei for stealing T-Mobile robot arm, selling US tech to Iran," *ArsTECHNICA*, 1/28/2019. *https://arstechnica.com/tech-policy/2019/01/us-indicts-huawei-for-stealing-t-mobile-robot-selling-us-tech-to-iran/*.

16. Murray Scott Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*. July, 20, 2017. *https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense*.

17. Chris Demchak & Yuval Shavitt. *Military Cyber Affairs*, Vol. 3, Issue 1, 2018.

fic – or transit traffic – to move it onwards towards its various destinations." China Telecom has points of presence in New York, Washington, DC, Miami, Chicago, Dallas, Los Angeles, San Jose, and Seattle, as well as in Canada and throughout Europe, Africa, South Asia, Southeast Asia, and Australia.[18] Recent cyber security investigations have revealed that APT 41, a Chinese state sponsored hacking group, has compromised more than a dozen international telecommunications firms, stealing SMS messages, for the purpose of tracking individuals of high interest.[19] Due to its activities China Telecom's license to operate in the US is under review by the Federal Communications Commission at the urging of the Departments of Defense, State, and Justice.[20]

Influence operations are meant to shape the perceptions of individuals, groups, and/or the public at large. Russia is the most active participant using many methods, including social media. However, the US has become concerned with the spread of pro-Chinese propaganda in the US and has directed a reduction in "news" employees from 160 to 100 total for Chinese press organizations Xinhua, CGTN, China Radio, *China Daily* & *People's Daily*.[21]

One avenue of concern is the dissemination of propaganda through Chinese "institutes" on American campuses. While China does some of the same as Russia, its approach to influence operations appears much broader. It includes favorable press, i.e., propaganda. But also, much more.

China's Thousand Talents Program is aimed at encouraging and recruiting the best talent worldwide to support China. The emphasis is on science, technology, engineering, and manufacturing (STEM). Financial rewards and peer pressure are used to obtain advanced technologies, including often evolving trade secrets, from laboratories and university research centers. The line between cooperation and economic espionage is often murky. Several indictments in the US have been issued in recent months for experts who hid their involvement with China while engaged in US Government-funded R&D, for example:

- Harvard professor Charles Lieber, chair of the department of Chemistry and Chemical Biology;[22]
- Turab Lookman, a former Los Alamos National Laboratory, an expert in computational materials science;[23] and
- Feng Tao, a University of Kansas associate professor of chemical engineering and nanoscience.[24]

Beijing targets ethnic Chinese students abroad. There are over 360,000 in the US. Again, the emphasis is on STEM. The purpose is to encourage them to return to China. But in some cases, it has been to encourage them to get US Government or contractor jobs with a security clearance. The obvious purpose is for future espionage.[25]

The Chinese government has established and funded over 500 "institutes" or research bodies in many universities worldwide. There are 86 in the US. While the professed purpose is to develop friendship, institute staff have been involved in spying on Chinese students abroad and other espionage activities.[26] The Vrije Universiteit of Brussels shut its Confucius Institute in 2019 after 13 years.[27] Other universities that have or are doing the same include the University of Chicago, Penn State, Tulane, Texas A&M, NC State, Michigan, (a total of 33 in the US) and abroad, the Université of Lyon in France, Stockholm University, and the University of Leiden in the Netherlands.

Cyber techniques used by the Chinese include phishing and spear-phishing; approaches via Linked-

18. Air Force Cyber College graphic.

19. Dan Goodin, "Strange snafu misroutes domestic US Internet traffic through China Telecom," *ArsTECHNICA*, 11/6/2018. *https://arstechnica.com/information-technology/2018/11/strange-snafu-misroutes-domestic-us-internet-traffic-through-china-telecom/*. Catalin Cimpanu, "For two hours, a large chunk of European mobile traffic was rerouted through China," *ZDNet*, June 7, 2019. *https://www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/*. Zak Doffman, "Chinese Hackers Just Gave Us All A Reason To Stop Sending SMS Messages," *Forbes*, November 3, 2019. *https://www.forbes.com/sites/* zakdoffman/2019/11/03/chinese-hackers...st-gave-us-all-a-reason-to-stop-sending-sms-messages/#479186a478c1.

20. Steven J. Vaughn-Nichols, "DOJ urges FCC to revoke China Telecom's license," *ZDNet*, April 99, 2020. *https://www.zdnet.com/article/doj-urges-fcc-to-revoke-china-telecoms-license/*.

21. Lara Jakes and Marc Tracy, "US Limits Chinese Staff at News Agencies Controlled by Beijing," *New York Times*, March 2, 2020. *https://www.nytimes.com/2020/03/02/world/asia/china-journalists-diplomats-expulsion.html*.

22. "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases," *Justice News*, January 28, 2020.

23. Scott Wyland, "Ex-LANL scientist pleads guilty to lying to government," *Santa Fe New Mexican*, January 24, 2020. *https://www.santafenewmexican.com/news/local_news/ex-lanl-scientist-pleads-guilty-to-lying-to-government/article_85c1b06c-3ec6-11ea-b962-obde11da0101.html*.

24. "University of Kansas Researcher Indicted for Fraud for Tailing to Disclose Conflict of Interest with Chinese University." *Justice News*, August 21, 2019. *https://www.justice.gov/opa/pr/university-kansas-researcher-indicted-fraud-failing-disclose-conflict-interest-chinese*.

25. Ben Wolfgang, "'Academic espionage:' China suspected of flooding US with students to access sensitive programs," *The Washington Times*, August 22, 2019. *https://www.washingtontimes.com/news/2019/aug/22/china-academic-espionage-deploys-students-us-acces/*.

26. "How Many Confucius Institutes Are in the United States?," *National Association of Scholars*, February 12. 2020.

27. Ian Allen, "Belgian university shuts down Chinese-funded institute due to espionage claims," *IntelNews*, 12/12/19. *https://intelnews.org/2019/12/12/01-2686/*.

Huawei and the 5G Issue

A major issue is related to the next generation of wireless telecommunications technology, generally referred to as "5G." 5G promises greatly expanded upload and download speeds. As James Lewis, a cyber expert at the Center for Strategic and International Security (CSIS), stated "5G could be the start of another round of innovation and growth similar to what we saw with the arrival of the internet." Some experiments have demonstrated speeds of 1 gigabit per second. The Chinese firm Huawei has been aggressively pushing its 5G technology to countries worldwide. As Lewis testified to the Senate Committee on Commerce, Science and Transportation on March 4, 2020, "there is broad agreement with the US on the risks of using Huawei." Huawei is seen as a surrogate for the Chinese government and its intelligence services. China has "a long record of unscrupulous behavior." It has been indicted for economic espionage by the US. It is also believed to have been involved in helping the Chinese government and African rulers spy on citizens. While the US, Japan, and Australia have banned Huawei from participating in 5G upgrades in their national networks, other countries, mostly for economic reasons, have resisted banning the company. Its products are less expensive due to massive Chinese government subsidies. China has threatened retaliation against businesses if various countries ban Huawei, such as the German automotive industry. As Lewis told Congress "the root of the 5G problem is Chinese espionage and Chinese predatory economic practices."

In;[28] invitations to visit and speak at Chinese universities; inserted malware; appeals to supporting the 'mother country'; extortion – often threatening harsh treatment of family members in China; and other tricks. In early 2020, Chinese cyber espionage appeared to increase, according to the cybersecurity firm FireEye.[29]

Xi's 2015 promise to curtail Chinese economic hacking was "empty." In China there are more than a dozen Advanced Persistent Threats, or APTs, active in cyber espionage.[30] We in the United States have been rather slow in responding to Chinese use of aggressive cyber operations.

Since 1995 there have been in the US 44 cases prosecuted of Chinese economic espionage. Some by the government, some by Chinese competitors. The Justice Department has become aggressive going after Chinese operatives, especially since 2011.[31] For example, senior MSS officer Yanjun Xu was arrested in Belgium and extradited to US for stealing aviation trade secrets from US firms.[32] The FBI has over 1,000 open investigations of Chinese economic espionage.[33]

In conclusion, in an article in *Foreign Affairs*, scholar Michael Beckley noted China has been experiencing a slowdown in its economic growth since 2008. (The Covid-19 pandemic is likely to have a severe impact on the Chinese economy.) He observed "when rising powers have suffered… slowdowns in the past, they become more repressive at home and more aggressive abroad." Today China does not feel secure.[34]

China is unlikely to undermine American democracy, per se. But one cannot conclude the same for other countries more susceptible to Chinese influence operations. However, China's cyber and human espionage have already damaged the American economy and altered the relative military balance of power. Thus far, the Communist government has not paid a significant price for its actions, but that may be changing.

Peter C. Oleson is the senior editor of the *Intelligencer.*

EDITOR's NOTE: This article was written before the US Government ordered the closing of the Chinese consulate in Houston.

28. A good example is the Kevin Mallory case. *https://cicentre.com/page/MALLORY_Kevin*.
29. Christopher Bing and Raphael Satter, "US cyber security experts see recent spike in Chinese digital espionage," *ABS-CBN News*, March 26, 2020. *https://news.abs-cbn.com/spotlight/03/26/20/us-cyber-security-experts-see-recent-spike-in-chinese-digital-espionage*.
30. MITRE ATT&CK, *https://attack.mitre.org*.
31. See *https://cicentre.com/page/case_economic*.
32. "A Sting Operation Lifts the Lid on Chinese Espionage," *On Security*, Stratfor, October 16, 2018.
33. Director Wray testimony to the Senate Committee on the Judiciary.
34. *Foreign Affairs*, Nov-Dec 2019 issue. See also "China Won't Back Down on Cyber Espionage Anytime Soon," *Assessments*, Stratfor, July 6, 2018.