Journal of Strategic Security

Volume 14 | Number 4 Article 9

Les Opérations D'Influence Chinoises: Un moment machiavélien Paul Charon and Jean-Babtiste Jeangéne Vilmer Paris: Institut de Recherche Stratégique de l'École militaire (IRSEM), 2021.

Edward M. Roche PhD, JD
Institute for Cyber Arms Control and Affiliate Researcher, Columbia Institute for Tele-Information,
emr96@caa.columbia.edu

pp. 111-115

Recommended Citation
Roche, Edward M. PhD, JD. "Les Opérations D'Influence Chinoises: Un moment machiavélien Paul Charon and Jean-Babtiste Jeangéne Vilmer Paris: Institut de Recherche Stratégique de l'École militaire (IRSEM), 2021.."
Journal of Strategic Security 14, no. 4 (2021) : 111-115.
DOI: https://doi.org/10.5038/1944-0472.14.4.1993
Available at: https://digitalcommons.usf.edu/jss/vol14/iss4/9

Les Opérations D'Influence Chinoises: Un moment machiavélien Paul Charon and Jean-Babtiste Jeangéne Vilmer Paris: Institut de Recherche Stratégique de l'École militaire (IRSEM), 2021.

Les Opérations D'Influence Chinoises: Un moment machiavélien Paul Charon and Jean-Babtiste Jeangéne Vilmer Paris: Institut de Recherche Stratégique de l'École militaire (IRSEM), 2021. ISBN: 978-2-11-155493-1 641 pps.

Review by Edward M. Roche, PhD, JD
Institute for Cyber Arms Control
Affiliate Researcher, Columbia Institute for Tele-Information

Les Opérations D'Influence Chinoises is the most complete description ever published about Chinese information warfare against the West. The authors, Charon and Jeangéne Vilmer, work at France's leading military think-tank, the *Institut de Recherche Stratégique de l'École militaire* (Military School Strategic Research Institute). This breathtaking study is complete with 200 pages of case studies on Chinese manipulation of information as regards Taiwan, Hong Kong, Singapore, Sweden, and Canada. Their analysis is stunning.

The sole purpose of China's information warfare is to increase its influence in the world. It uses three vectors: public opinion warfare, psychological warfare, and battles using international law. Operations are coordinated primarily by the Ministry of Security, a vast organization having 18 directorates, some of which use clandestine methods for overseas intelligence gathering and influence operations.

The Department of Propaganda oversees ideology and shapes the dominant discourse by controlling mass media and restricting freedom of expression and critical thinking—not only in China, but overseas as well. One important tool is the United Front Labor department, which targets ethnic minorities, intellectuals, religious organizations, overseas Chinese, and political parties in Hong Kong, Macao, and Taiwan. A Department of International Liaisons maintains connections with foreign political parties and works to build public opinion in favor of China while engaging in intelligence gathering. The Communist Youth League (80 million members) has a separate propaganda channel using social networks and even a rap group (CD Rev) which manufactures continual anti-American messages. There also is the "610 Office" employing approximately 15,000

persons organized solely for the purpose of exterminating the Falun Gong movement and its ideas worldwide.

The People's Liberation Army maintains a Strategic Support Force, including a Department of Network Systems for cyber activities. This includes "Unit 61716", the Public Opinion, Warfare, Psychological Warfare and Law Warfare "311 Base". It conducts research on information warfare against Taiwan and the United States. Current research efforts are focusing on use of Artificial Intelligence for manipulation of public opinion. The 311 Base also operates Units 61070 and 61198, which focus on network communications, psychological warfare, and Taiwan. They work through a "nebula of platforms" that the authors call "relays". These include the China Association for International Friendly Contact, which operates a training center and a fake hotel for the purpose of cultivating relationships with elites from foreign countries.

These are the high-level organizations directing Chinese propaganda ("information warfare") operations. The strength of this study is its identification of and detailed research on the subsidiary organizations that are recruited into these efforts: The Voice of the Strait, China Huayi Broadcasting Corporation, China Association for Friendly International Contact, US-China Sanya Initiative, China Association for Promotion of Chinese Culture, Haifeng Publishing House, and the China-United States Exchange Foundation.

Other tools include databases such as the Global Tone Communications Technology Co. Ltd (GTCOM). This is a big data processing company that uses Artificial Intelligence to analyze 10 terabytes of data per day imported both legally and illegally from the World Wide Web, online forums, Twitter, Facebook, WeChat and many other Internet sources. It is operated by the Department of Propaganda.

China collects massive amounts of data on foreign individuals, including Americans. For example, its Overseas Key Information Database (OKIDB) has information on 2.4 million persons, including their photographs, and 650,000 organizations. It also links in 2.3 billion press articles, and 2.1 billion social media posts. This work is funded by the People's Liberation Army and Ministry of State Security through the Shenzhen Zhenhua Data Information Technology Company. The work has a focus on politicians,

https://digitalcommons.usf.edu/jss/vol14/iss4/9
DOI: https://doi.org/10.5038/1944-0472.14.4.1993

public sector employees, academics, business persons, scientists, and think tanks outside of China. Social network analysis is used to construct personal profiles and professional connections. Against the backdrop of how China is collecting and analyzing this kind of information, it is notable that in early 2014, approximately 21.5 million personnel records from the U.S. Officer of Personnel Management were exfiltrated by China. These included persons with security clearances and data on their background checks. This information is used to aid Chinese security, intelligence, and information operations.

Private Chinese citizens are forced to help in these operations. Article 7 of the Intelligence Law binds all Chinese companies—public and private—as well as citizens to "support, assist and cooperate in national intelligence efforts." China's private sector is used extensively in these operations. For example, the Chinese company that constructed the Headquarters of the African Union loaded it with hidden microphones and hacked computer systems for a comprehensive eavesdropping operation that lasted from 2012 until 2017 when the operation was exposed by the French. In Africa, Chinese companies have aided in the construction of 186 government buildings and have constructed at least 14 sensitive government telecommunications networks.

The authors document how China uses Confucius Institutes to extend influence into higher education in the United States (and elsewhere) and buys off leading professors with generous grants. China works to influence Western think tanks and create their own. Another program is aimed at general culture and exerting influence over foreign cinema ("Hollywood") and video.

The penetration of smartphones worldwide has amplified the possibilities for exploitation. Social media platforms such as WeChat, Weibo, and TikTok also are part of the campaign. China uses armies of Internet trolls and astroturfing to generate consensus and pro-China public opinion throughout the web and social media. Spam is heavily used. The report notes that in 2017 more than 10,000 fake Twitter accounts were linked to the Chinese government.

The authors see this massive propaganda and subversion operation as modeled on the concepts developed in Russia during the 1920s. They

assess that this approach has been updated and vastly improved by the Communist Party of China, primarily by adoption of innovative technology, more aggressive and overt overseas actions, a giant geographic scale and stunning linguistic scope. They provide several examples comparing Chinese and Russian operations.

An entire chapter with specificity is devoted to Chinese disinformation operations in connection with Covid-19. For example, in the "Infektion" ("Denver") disinformation campaign waged by Russia against the United States, the objective was to spread the idea that the AIDS virus was designed by the United States government against Afro-American populations and homosexuals. The authors trace this campaign, which started in 1983, through seven phases. Later, they provide in well-documented detail the Chinese Covid-19 campaign designed to attribute the virus to U.S. biological warfare operations and match the steps taken by China to the exact same model as had been used by Russia years before. The level of detail is astonishing.

The authors show how the Chinese Covid disinformation campaign linked together a sequence of memes starting January 20, 2020 with an interview on the Zvezda (Russian) television channel. The disinformation was spread a week later in Inner Mongolia using the Kuaishou app, then was sent out by Chinese diplomats. This was followed in February by the Global Times, and "useful idiots" in TV Asahi, Helsinki Times, and the New Zealand Herald. In February a Chinese epidemiologist said at a government-organized press conference that the virus may not have originated in China. This was magnified by the Chinese Embassy in South Africa, and tweets questioning the involvement of the US military. Think tanks, experts, and others gradually were employed in this disinformation campaign, many through social media such as WeChat. Eventually it entered the mainstream press. The authors conclude that:

> "It is still too early to assess the effectiveness of the operation, the effects of which can be felt for years . . . The future will tell us to what extent the belief in an American manufacture of the virus was able to take root . . . The operation . . . contributes . . . to the weakening of democratic societies by an insidious questioning of the nature of their institutions" (p. 605, transl. by author).

https://digitalcommons.usf.edu/jss/vol14/iss4/9
DOI: https://doi.org/10.5038/1944-0472.14.4.1993

The discussion of the Covid campaign is only one of many examples in this comprehensive study. What the authors describe is a massive campaign that dwarfs anything comparable in the United States. The scale of Chinese operations goes far beyond mere manipulation of social media as detailed in the two seminal studies about the 2018 US Presidential Election: *Network Propaganda* by Benkler, Faris and Roberts at Harvard, and *Computational Propaganda* by Woolley and Howard (Eds.) at Oxford. The Chinese effort involves its own mass media (Xinhua, CCTV, China Daily, Global Times, China Radio International) as well as influence operations against "Mainstream Media" in the West by cultivation of writers, and acquisition of ownership. Making large payments to newspapers for advertising is another tactic.

It is difficult to appreciate the true scale of China's psychological warfare and Social Media based Information Imperialism. It is happening not only in the West, but also throughout Asia, Latin America, and Africa as well, and in all major world languages. China can win every time because it can recruit millions of persons in the effort.

Les Operations d'Influence is a crucial contribution to strategic literature. It is the most important study of public diplomacy in decades. The level of detail, documentation, precision of thought and organization puts this study at the top of its class. It is superior to anything published on this topic in the United States. It should be read by every person following national security who is interested in seeing how the new reality of cyber-based information warfare is shaping current events.