國立政治大學亞太研究英語碩士學位學程

International Master's Program in Asia-Pacific Studies

College of Social Sciences

National Chengchi University

碩士論文

Master's Thesis

# 中國對台灣網路戰爭研究

# *A Study on Chinese Cyber Warfare on Taiwan*

Student: Andrew Yi 易安祖

Advisor: Chien-min Chao, Ph.D. 趙建民教授

中華民國 109 年 6 月

June 2020

DOI:10.6814/NCCU202000853

**Abstract**

Cybersecurity is one of the most pressing issues facing modern, technologically advanced states. Building cyber capabilities has allowed states to execute strategic tasks and achieve goals previously thought impossible in real time. Cyber is the domain of tomorrow and no country has better utilized those capabilities than China. Currently, Taiwan and the United States face the constant threat of cyberattacks from its adversaries, China being chief among those. Because of flaws and weaknesses in both countries' cybersecurity networks, foreign actors seek to utilize cyber capabilities to destabilize society in order to achieve strategic goals. The PRC has been utilizing its cyber capabilities first on Taiwan, and later against other foreign adversaries such as the United States. Experts frequently cite Taiwan as a testing ground for Chinese hacks because of its proximity to the mainland and its cultural similarities. In this thesis, I attempt to answer the question of: what is China's Cyber Warfare Strategy against Taiwan? Taiwan is a strategic goal of the Chinese government, who is willing to go to any lengths short of war to subdue to the island government to its force. The process of conducting this research paper was a daunting task, but I hope to help further the discussion and research of Chinese Cyber-activities by contextualizing China's Political Warfare campaign against Taiwan to better understand their activities. This thesis will explain how the CCP is carrying out a coordinated political warfare campaign that utilizes cyber warfare in order to undermine Taiwan's democracy. It utilizes what publically available English resources are available regarding Taiwan and China's cyber capabilities and relies on translations sources from Chinese. The effectiveness and extent of Chinese activities in Taiwan requires further research and study for accuracy.

**Keywords:** Taiwan, Cyber Warfare, Cybersecurity, Cyber Strategy, Cross-strait Relations, CCP Politics, U.S.-Taiwan Relation



DOI:10.6814/NCCU202000853

## Table of Contents





DOI:10.6814/NCCU202000853

## Chapter 1 – Methodology

### *Research Question*

Taiwan and the United States face an ongoing security threat and the challenge of defending themselves against the CCP's vast cyber capabilities. In its campaign to retake Taiwan by any means necessary, the CCP has resorted to the use of cyber warfare against Taiwan. In its counteroffensive campaign against the U.S., Beijing oftentimes utilizes Taiwan as a testing bed, later using those same techniques in other countries like the United States. Beijing sees cyber warfare as a method of executing a low risk-high reward political warfare campaign in order to subdue Taiwan. With cross-strait tensions at almost an all-time high, this raises the question of:

*What is China's Cyber Warfare Strategy against Taiwan? How are they doing it and why?*

### *Research Method*

This thesis adopts qualitative research methods, specifically utilizing archival methods, collecting and reviewing documents, news articles, and journal publications. Interviews were conducted to provide accurate accounts from government security officials currently working on this issue. Because of the contemporary nature of the research question and hypotheses, this thesis will concentrate mainly on Chinese cyber espionage efforts within the last two decades (post-2000). Additionally, due to the classified nature of this topic, this thesis relies heavily on publicly available resources and will require future study in order to update the results of this thesis.

China's campaign of disinformation, cyber-attacks, and military exercise serve to target the independent and democratic pillars of Taiwanese society in order to eventually force it to submit to a foreign power. Disinformation can serve to undermine the legitimacy and authority of public officials while military activities can harm morale among citizens and government officials. It can also serve to undermine the current institutional strength that Taiwanese government currently upholds. The current COVID-19 Global Pandemic also leaves Taiwan vulnerable to the spread of misinformation due to the nature of the information sphere where accuracy is of utmost priority above all else.



DOI:10.6814/NCCU202000853

## Introduction

The Taiwan Strait has long been a flash point in the Asia-Pacific region since the Nationalists retreated to Taiwan after their defeat by the Communists. Since the 1950's, tensions have cooled and boiled over the decades, with advancements in warfare and technology completely reshaping the landscape of the battlefield. Today, Taiwan is facing a major cybersecurity threat at the hands of the PRC. The internet has become ingrained in nearly every aspect of modern society; everything from e-commerce, social media, multinational corporations, even government institutions and bureaucracies are inextricably linked to the internet, leaving them vulnerable to cyber-attacks.

In 2011, the Center for a New American Security published a report stating "the ability to leverage cyberspace is one of the 21st century's most important sources of power. State and non-state actors can use this power to achieve financial, military, political, ideological or social objectives in cyberspace or the physical world."[1] Both the United States and Taiwan have a long history of cyber-attacks, with Taiwan's Democratic Progressive Party's website in particular being hacked twice. In 2013, The National Security Bureau (NSB) detected 7.2 million hacking incidents alone, 239,000 of which were attacks. Additionally, in the first half of 2016 alone, the NSB itself was the target of 17,600 cyberattacks, averaging a total of 12 per day; most of which are believed to have originated in China.

Because of the widespread integration of the internet in nearly all facets of industry, government, and military, countries like Taiwan and the United States are under constant assault in cyberspace. As these attacks grow in intensity, the risk of catastrophic incidents with consequential social effects rapidly increases. The same 2011 report by the Center for a New American Security emphasized three traits of cyber security that [American] leaders must grapple with in order to craft effective policies: speed and the collapse of distance; magnitude and intensity; and low barriers to entry. The capabilities within cyberspace were totally

[1] Robert E. Khan, Mike McConnell, Joseph S. Nye, Peter Schwartz, Nova J. Daly, Nathaniel Fick, Martha Finnemore, Richard Fontaine, Daniel E. Geer, David A. Gross, Jason Healey, James A. Lewis, M. Ethan Lucarelli, Thomas G. Mahnken, Gary McGraw, Roger H. Miksad, Gregory J. Rattray, Will Rogers, and Christopher M. Schroeder, *America's Cyber Future: Security and Prosperity in the Information Age*, Center for a New American Security, 2011. 20-31. www.jstor.org/stable/resrep06319.7.



DOI:10.6814/NCCU202000853

unimaginable just decades ago, but now the speed and collapse of distance—something we had originally taken as a luxury—is now one of the most formidable security challenges not only to the United States, but to every nation.

In cyberspace, foreknowledge is limited because information moves from origin to destination almost instantaneously. As a result, cyber-attacks are not constrained by geographic proximity. Targets remain constantly vulnerable to attacks and have little to no time to prepare for them.[2] Magnitude and intensity emphasizes that small actions can have enormous effects. For the past decade, China has emphasized the strategic importance of cyberspace. In 2006, the PLA Daily called cyberattacks a serious threat to national security. Cyber operations reshape the security environment by eroding traditional, geographical boundaries.[3] China believes that it must seize strategic opportunities to ensure a stable security environment in what they consider the "fifth-dimension of the battlefield."[4] According to Michael Kolton, a U.S. Army Foreign Area Officer (FAO) specializing in China, some PLA theorists believe information age warfare requires militaries to conduct a new hybrid-form of warfare that combines cyber power and firepower.[5] By this argument, the PLA believes that a joint cyber force is necessary to fight and win future wars as cyber operations are critical for national defense.

Traditional Clausewitzian theory[6] on warfare no longer applies to the current 21st century battle ground. The shortcomings of Clausewitzian theory when applied to traditional military theory presents four challenges: anonymity, object permanence, measurable results, and rapid digital execution.[7] In short, cyber technology allows for the execution of decisive operations never previously thought possible. Cyber-attacks and offense have the complete advantage of anonymity; gaining measurable results; at an extremely fast rate; with minimal consequences and

[2] Ibid.
[3] Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017): 119-54. www.jstor.org/stable/26267405.
[4] Ibid.
[5] Ibid.
[6] Carl Philipp Gottfried Von Calusewitz (1780-1831) was a Purssian general and military theorist whose theories on war are frequently studied and researched by military historians and strategists
[7] Jan Kallberg, "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review* 1, no. 1 (2016): 113-28. www.jstor.org/stable/26267302.



DOI:10.6814/NCCU202000853

costs. In many ways, cyber capabilities have evolved faster than the frameworks leaders rely on to employ them. The past decade has seen China and the United States lead the discussion on how states should govern their citizens online. Chinese and American views of military deterrence differ, and divergent theories of cyber warfare underscore the importance of ongoing U.S.-China efforts to build norms of behavior in cyberspace.[8] Today's embryonic military cyber doctrines carry risks of bilateral misunderstandings, especially when militaries operationalize cyber deterrence strategies.[9]

The Taiwan Strait has historically been a flash point, and any conflict between China and Taiwan almost certainly involves America due to the Taiwan Relations Act, which obligates the White House to provide defensive arms and services to Taiwan, and to maintain U.S. military capacity to respond to any Chinese use of force against the island (though it is not a binding mutual defense treaty). Cyber tactics are just another tool utilized by the mainland in its effort to reclaim Taiwan. There is growing evidence that Taiwan has long been a testing ground for Chinese cyber capabilities before eventually being turned on the United States.[10] For at least a decade, Taiwanese internet security specialists have observed a recurring pattern: innovative, highly targeted data theft attacks appear in both government and industry systems in Taiwan, and within a few months, these same methods frequently turn up in the wake of attacks against the United States and other large countries.[11]

Though China has had an extensive history of cyberwarfare, the threat and concern seems to be higher than ever. Beijing feels an immense anxiety with Taipei's democracy right at its doorstep. China's ballistic missile buildup has been attributed to an attempt to discourage the island nation from taking steps towards independence, and to deny U.S. military presence in that area of the Pacific; specifically, the Taiwan Strait. Taiwan's most strategic ally happens to be

[8] Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017): 119-54. www.jstor.org/stable/26267405.
[9] Ibid.
[10] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*, (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.
[11] Harry Krejsa, and Hannah Suh. *Report*. Center for a New American Security, 2017. Accessed March 26, 2020. www.jstor.org/stable/resrep06143.



DOI:10.6814/NCCU202000853

the United States, the one state that China sees as challenging its supremacy in Asia. China seeks to undermine Taiwan's democracy and civil society on all fronts, including its international relationships. Only once it has exhausted all options (or when an opportune moment presents itself) will the PLA proceed with a full scale invasion.[12] Since the beginning of the COVID19 global pandemic, China has been ramping up its pressure against Taiwan with military exercises and threating rhetoric.[13] This research project comes at a timely manner and will be focusing on China's cyber campaign against Taiwan. As interstate conflicts evolve, it is important that we assess what China's cyber capabilities and strategy are moving forward in order to better fortify defenses in the event of future attacks.

## Chinese Views of Cyber

In order to analyze China's cyber warfare strategies, we must first understand how the Chinese and the Chinese Communist Party view cyber. Chinese definitions of cyber and cybersecurity to this day remain vague and broad, much like the majority of other cyber-related terms and concepts in Western academic literature. According to Michael D. Swaine of the Carnegie Endowment for International Peace, authoritative Chinese sources do not provide a detailed definition of cybersecurity with PRC government statements largely referring in general terms to the growth of the Internet, the increasing dependence of many nations on cyber-based activities, the dangers posed by cyber-attacks, and the need for governments to provide more supervision over the internet.[14] He continues by saying that such general statements, combined with more detailed discussions from non-authoritative sources, suggest that most Chinese conceive of cybersecurity in a similar manner to observers in other countries.[15] Essentially, many Chinese citizens share the same concerns as their Western, democratic counter parts in regards to cybersecurity such as: "efforts to crash, slow, or paralyze vital cyber based infrastructure; the

[12] Ian Easton, *The Chinese Invasion Threat: Taiwan's Defense and American Strategy in Asia*. (Manchester: Eastbridge Books, 2019).
[13] Bonnie Glaser, and Matthew P. Funaiole. "China's Provocations Around Taiwan Aren't a Crisis," *Foreign Policy*, May 15, 2020. https://foreignpolicy.com/2020/05/15/chinas-provocations-around-taiwan-arent-a-crisis/.
[14] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *The Carnegie Endowment for International Peace*, September 20, 2013.
[15] Ibid.



DOI:10.6814/NCCU202000853

promulgation of information or images harmful to polity, society, or the economy (such as pornography, false or misleading commercial information, and the advocacy of violent political revolution); espionage; the theft of proprietary commercial data or information; and specific actions designed to weaken the capacity of the state to defend itself through military and other means.[16] Beyond these general concerns, the PRC, for many years, has placed a strong emphasis on the challenges posed by cyber activities that threaten existing domestic social and political stability, as well as the sovereignty of the nation-state. Both Swaine and Kolton mention how many non-authoritative sources, especially military, introduce the concept of "cyber sovereignty," and advocate the need for a government to identify the boundaries and constraints in which a state can protect itself against cyber threats.

Dr. Lu Jinghua of the Center of U.S.-China Defense Relations at the PLA Academy of Military Science's (AMS) describes cyber sovereignty as the foundation for a new international code of conduct for cyberspace (*wangluo kongjian xingwei zhunze)* in which the principle of sovereignty enshrined in the UN Charter extends to cyberspace.[17] While the West applauds freedom on the Internet, the CCP worries about its latent potential to destabilize social and political order. To support their contention that the internet poses a major threat to the sovereign authority of nation-states, many Chinese academic researchers frequently cite the disruptive impact on Middle Eastern governments of social networking websites such as Twitter, as well as various blogging websites.[18] The supposedly negative impact of such activities in the aftermath of the Iranian presidential elections and social unrest in Xinjiang, is often offered as specific examples.[19] According to Swaine, this viewpoint leads to a more state-centric orientation towards cybersecurity compared to Western democratic nations; and reflects the long-standing

[16] Ibid.

[17] Lü Jinghua, [吕晶华], "Gongtong goujian heping anquan kaifang hezuo de wangluo kongjian," [共同构建和平安全开放 合作的网络空间] (Jointly building a peaceful and safe cyberspace through open cooperation) *PLA Daily*, October 18, 2016, http://www.81.cn/jfjbmap/content/2015-10/18/content_126334.htm.

[18] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *The Carnegie Endowment for International Peace*, September 20, 2013.

[19] Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017): 119-54. www.jstor.org/stable/26267405.



DOI:10.6814/NCCU202000853

Chinese concern with social disorder, along with the related need for a strong, supervisory state to uphold societal norms and to preserve social harmony.[20] Research by the RAND Corporation suggests that the Color Revolutions and Arab Spring fueled the CCP leadership's growing concern over the battle of hearts and minds and brought back memories of the fall of the Soviet Union.[21] In October 2011, then-President Hu Jintao said, "We must clearly see that international hostile forces are intensifying the strategic plot of Westernizing and dividing China, and ideological and cultural fields are the focal areas of their long-term infiltration."[22] This is where views regarding internet governance begin to diverge between China and the West. To the Chinese, foreign policy begins at home, and the majority of the PRC's efforts over recent decades to use information in order to achieve political goals and to shape public opinion through propaganda has been focused first on defending the regime and secondarily on swaying foreign audiences.[23] Kristin Shi-Kupfer, expert on China's digital politics and media policy for the Mercator Institute for China Studies, characterizes the Chinese system of rule as "governance through information control," and argues that "the Chinese government has recognized that its needs a comprehensive social media strategy if it is to win the 'battle for public opinion.'"[24] These differing perspectives and opinions lead the Chinese government to see itself in perpetual competition (or even constant war), with the United States and greater Western community in the ideological space.[25] Although the U.S. and China agree on the importance of cyberspace, they fundamentally diverge on the prerogatives a country should enjoy in the virtual world.



[20] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations." The Carnegie Endowment for International Peace, September 20, 2013.
[21] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR2713.html.
[22] Ibid.
[23] Ibid.
[24] Kristin Shi-Kupfer, "Governance Through Information Control," *China Monitor*, No. 26, Mercator Institute for China Studies, (January 19, 2016).
[25] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends.* (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.



DOI:10.6814/NCCU202000853

Both authoritative and non-authoritative sources emphasize the "ideological" dimension of cyber and its impact on the stability of society. Cyber capabilities have the potential to disrupt societal stability, and undermine regime legitimacy and the PRC is extremely aware of this fact. According to Swaine, for many Chinese, and especially authoritative and quasi-authoritative observers, the government should take a more direct, activist, and ideological role when governing their citizens online.[26] One observer in the *Liberation Army Daily* stated, "raising the ideological and moral standard of the citizens [is] a basic standard for achieving the unification of cyber freedom and cyber self-discipline."[27] Essentially, the ideology and authority of the PRC government must also be reflected in China's digital landscape. In order to protect China's sovereignty, the internet in China must reflect socialist "cyber culture" and resist "ideological infiltration by political instigation."[28] Beijing remains firm on its position that individual states should have the right to independently choose their system of cyber governance, and rejects the idea of an open internet. On December 16, 2015, Xi Jinping called upon the international community to "respect the right of individual countries to independently choose their own path of cyber development and model of cyber regulation and participate in international cyberspace governance on an equal footing."[29] Additionally, in a critique of the U.S., Xi said, "Existing rules governing cyberspace hardly reflect the desires and interests of the majority of countries."[30] Kolton cites Colonel Ye Zheng of AMS who explains the Chinese perspective of cybersecurity:

> To achieve cybersecurity requires 'cyber rules.' Rules are the basis of order, and order is the basis of security. The core of cybersecurity is to establish cyber rules and implement them. Without cyber rules, activities in cyberspace will be out of control, cybercrimes will be rampant, and cybersecurity will be harmed. Cyberspace is now in a disordered state because no actions have been taken to

[26] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," The Carnegie Endowment for International Peace, September 20, 2013.
[27] Ibid.; Jing Nanxiang, "Cyber Freedom and Cyber Self-Discipline," *Liberation Army Daily*, December 20, 2011, from "Summary: JFJB on Cyber Freedom and Cyber Self-Discipline for PRC Netizens," translated by OSC, CPP20111221088010.
[28] Ibid.
[29] Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017): 119-54. www.jstor.org/stable/26267405.
[30] Ibid.



DOI:10.6814/NCCU202000853

develop cyber rules and there is no international consensus about how to work out the rules.[31]

China has incorporated political, economic, diplomatic, and military tactics to defend its sovereignty; oftentimes at ideological odds with the greater Western community. In hopes of retaining control and establishing stability among its populace, China has built up one of the world's most sophisticated capacities for human- and machine-enabled key-word blocking and censorship and has also used such new technologies and platforms in innovative ways to shape the domestic and foreign flow of information.[32] While many observers had hoped that the wider exposure to information that the internet and social media provides would lead China down a less state-centric path of internet governance, the CCP has doubled down on its control of its citizens online and incorporated new technologies in order to expand its influence. This conflicting perspective in regards to internet governance, coupled with the negative perception that China paints of the West, has led many Chinese thinkers to assume that China is in a zero-sum ideological competition with the West.[33]

This perspective of constantly being at odds with one another, has led to antagonistic sentiment aimed at each other from both China and the West. Though China has been widely accused of engaging in cyber espionage tactics by the international community, it has typically met such accusations with a defensive posture, usually by denying allegations. From the Chinese perspective, the U.S. government has already engaged in a massive propaganda campaign against China and other countries.[34] In April 2013, President Xi asserted in a secret document that "Western forces hostile to China and dissidents within the country are still constantly infiltrating the ideological sphere" specifically arguing that regime opponents "have stirred up trouble about disclosing officials' assets, using the Internet to fight corruption, media controls

[31] Ibid.; Ye Zheng, "From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond," translated by Yang Fan, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, (London: Oxford Scholarship Online, April 2015), 132, doi:10.1093/acprof:oso/9780190201265.001.0001.
[32] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends* (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.
[33] Ibid.
[34] Ibid.



DOI:10.6814/NCCU202000853

and other sensitive topics, to provoke discontent with the party and government."[35] That paradigm had a dramatic shift in 2013, when China assumed a more assertive stance, now directing accusations against the West, particularly the United States, for its global surveillance efforts.[36] In 2013, Edward Snowden leaked highly classified information from the National Security Agency (NSA) regarding the United States' global surveillance program, many of which were run by the Five Eyes Intelligence Alliance; ultimately putting the spotlight on the United States' cyber activities abroad. Kolton argues that China and Russia exploited the global controversy surrounding the Snowden leaks in order to push their own agenda and model of internet governance.[37] Beijing now points the finger at the United States for its cyber activities and has demanded explanations over reports of the NSA spying on Huawei.[38] Additionally, in 2012, the White House conducted its own security review of Huawei, but found now clear evidence of Huawei spying on behalf of the Chinese government; further contributing to the controversy surrounding the U.S. cyber activities.[39] Emilio Iasiello, a private strategic cyber intelligence analyst, argues that "while the U.S. seemed to have an upper hand and international support regarding suspected Chinese cyber espionage, China has successfully regained some of its public facing pride. China continues to promote itself as a cyber victim as well as a cyber security partner."[40] As China further solidifies its role as an international super power, the struggle to control information about the CCP has extended to global public opinion, and the internet is only the latest battlespace.



[35] Ibid.
[36] Emilio Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," *Journal of Strategic Security* 9, no. 2 (2016): 45-69. www.jstor.org/stable/26466776.
[37] Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017): 119-54. www.jstor.org/stable/26267405.
[38] Emilio Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," *Journal of Strategic Security* 9, no. 2 (2016): 45-69. www.jstor.org/stable/26466776.
[39] Ibid.
[40] Ibid.



DOI:10.6814/NCCU202000853

Yet, despite all this effort and devotion of resources, China's information operations today are immature compared with those of the United States.[41] Though China is believed to have threatening cyber capabilities already at its disposal, there are many challenges that come with developing cyber security. Cyber warfare encompasses far more areas than just military and intelligence gathering, therefore it is logical to measure a country's cyber capabilities based on additional factors. These factors include but are not limited to: technological research and development (R&D) and innovation capabilities; information technology industry companies; internet infrastructure scale; influences of internet websites; internet diplomacy and foreign policy capabilities; cyber military strength, and comprehensiveness of cyberspace strategy.[42] If evaluated based on these criteria, then China's cyber power largely lags behind that of the U.S., especially in terms of R&D.[43] Shi-Kupfer states that "China's leadership struggles with credibility in social media," and believes China is still learning how to convey propaganda online in a way that is less stilted and more effective.[44] The CCP's Central Discipline Inspection Commission confirmed this finding in June 2016 when it heavily criticized the Party's Propaganda Department for distributing news propaganda that was poorly targeted and insufficiently effective.[45] According to the ICT Development Index (IDI), a composite index that combines 11 indicators that monitor and compare developments in information and communication technology which is utilized to compare developments in ICT over time, China ranked 80th, 81st, and 82nd among 176 states in 2017, 2016, and 2015 respectively. China struggles with low influence on the global internet partially due to the fact that its primary

[41] Jon R. Lindsay. "Exaggerating the Chinese Cyber Threat." Belfer Center For Science and International Affairs, May 2015. https://www.belfercenter.org/sites/default/files/files/publication/linsday-china-cyber-pb-final.pdf.
[42] Liu. Jinghua, "What Are China's Cyber Capabilities and Intentions?" *IPI Global Observatory*, (March 22, 2019). https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/.
[43] Ibid.
[44] Kristin Shi-Kupfer, "Governance Through Information Control," China Monitor, No. 26, *Mercator Institute for China Studies*, (January 19, 2016).
[45] "China's Propaganda Department Not Good Enough at Propaganda—Gov't," *Hong Kong Free Press*, (June 9, 2016). https://hongkongfp.com/2016/06/09/pin-desktop-chinas-propaganda-department-not-good-enough-propaganda-govt/.



DOI:10.6814/NCCU202000853

languages are not widely used on the internet outside the country.[46] Chinese languages are only used by 1.7 percent of all websites, while 53.9 percent use English.[47]Additionally, according to multiple sources, China has weak network security and is vulnerable to frequent cyber-attacks such as distributed denial of service attacks (DDoS) attacks.[48] A frequently cited report published in February 2019 by Beijing Knownsec Information Technology found; China suffered the highest rate of DDoS attacks in the world in 2018 – an average of over 800 million a day, with scanning and backdoor intrusions making up the majority of the attacks.[49] About 97 percent were conducted by domestic hackers with a growing percentage coming from overseas, mostly from the U.S., South Korea, and Japan.[50] Accurately assessing China's cyber capabilities is crucial in a time where information accuracy is in question. Comprehensive and objective assessment of China's cyber power is in urgent need in order to properly build a fortified cyber defense.

Though China's cyber capabilities may not be on par with its Western counterparts, there is room for improvement and the CCP appears to have resolved to redouble its efforts and devote even more resources to information control and messaging.[51] This suggests that China's has the potential to become increasingly sophisticated in their cyber capabilities and messaging in the years ahead. Under Xi Jinping, China appears to have identified the improvement of propaganda content, delivery, and reception as increasingly important goals.[52] *Hostile Social Manipulation,* a report published by the RAND Corporation researching and documenting the role of targeted social media campaigns, sophisticated forgeries, cyberbullying and harassment of individuals, distribution of rumors and conspiracy theories, and other tools and approaches to cause damage

[46] Liu Jinghua, "What Are China's Cyber Capabilities and Intentions?" *IPI Global Observatory*, (March 22, 2019). https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/.
[47] Ibid.
[48] Ibid.; Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," The Carnegie Endowment for International Peace, September 20, 2013.
[49] Ibid.
[50] Ibid.
[51] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*. (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.
[52] Ibid.



DOI:10.6814/NCCU202000853

to a target state, places a particular emphasis on the role of Taiwan when discussing China's hostile social manipulation activities stating:

> Taiwan has often borne the brunt of China's foreign propaganda, and it appears that the Chinese government may be targeting Taiwan with its most aggressive and most advanced social manipulation efforts. Taiwan has been subjected to the PLA's clearest intimidation, the most likely case of Chinese disinformation, the most obvious case of Chinese netizens supporting CCP propaganda on foreign social media, and China's first extrajudicial punishment for social media posts outside of China (levied against a citizen of Taiwan). China is likely to expand the use of some or all of these tactics beyond Taiwan in the coming years. The U.S. government could benefit from increasing its dialogue and cooperation with its Taiwanese counterparts on countering Chinese social manipulation operations, both to support Taiwan's democracy and to better understand and prepare for future Chinese efforts around the world.[53]

In the wake of the hysteria caused by the COVID19 global pandemic, misinformation has become rampant online. A variety of conspiracy theories have emerged with some even being promoted by government officials in the United States and China. Zhao Lijian, a Chinese foreign ministry spokesman, has repeatedly promoted the idea that COVID-19 might have originated in the United States with a number of Chinese embassies and social media users amplifying and echoing his claims.[54] Likewise, several U.S. politicians such as Republican senators Tom Cotton and Ted Cruz have supported other baseless claims about the origin of the virus. Additionally, new reports in Taiwan have claimed that organizations like the National Security Bureau in Taiwan have dealt with misinformation regarding COVID-19. The issue of cyber-security in Taiwan is of upmost priority to in order to ensure the legitimacy of its democracy.

[53] Ibid.
[54] Shayan Sardarizadeh, and Olga Robinson, "Coronavirus: US and China Trade Conspiracy Theories," *BBC News*. BBC, April 26, 2020. https://www.bbc.com/news/world-52224331.



DOI:10.6814/NCCU202000853

## Chapter 2 – The Importance and Need for Cyber Theory

The advancement of technology and cyber in the 21st century has led the international community into uncharted territory in nearly every sense. Everything from e-commerce, cryptocurrency, smart phones, 5G, and even cyber warfare, is leading to an age of uncertainty in the world. The internet has the advantage of delivering information nearly instantaneously while also providing anonymity. States over the last decade have learned to weaponize the internet through with the ability to execute covert operations with measurable results. According to Dr. Jan Kallberg, Cyber Policy Fellow at the Army Cyber Institute at West Point:

> In a militarized internet, it is convenient to rely on traditional military theory transposed into cyber. It works as an intellectual short cut, but the traditional military thinking fails to acknowledge the unity tenets of cyber. Traditional military theory applied to cyber conflict has four challenges: anonymity, object permanence, measurable results, and rapid digital execution. In a Clausewitizian world, these challenges were non-existent.[55]

Kallberg firmly believes that there is a need for theory in order to understand the unknown and uncertain; cyber is no exception. Current theories surrounding political warfare and assessing an adversary's capabilities do not account for the advantages that cyber provides compared to traditional warfare methods. It is common knowledge that computers are not limited to human speeds, computing millions upon millions of real time data. Even if we solved the challenges of anonymity, the lack of object permanence, and the absence of measurable results, computerized machine speed would eradicate any influence of human leadership.[56] In reality, the cyber-attacks would be over before any leadership personnel were able to understand the strategic landscape. To conquer this massive hurdle of predicting something that is instantaneous, Kallberg believes that there must be a fundamental rethinking of cyber warfare theory in order to better understand the extremely dynamic landscape. Theory is an overarching way of combining ideas,

---

[55] Jan Kallberg, "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review* 1, no. 1 (2016): 113-28. www.jstor.org/stable/26267302.
[56] Ibid.



DOI:10.6814/NCCU202000853

phenomena, and facts, in a generalized form, in order to try and explain specific outcomes.[57] Theory's strongest tenant is predictability; theory can serve as guidance to prepare for future events and ensure these outcomes are favorable; theories are created to better understand the world.[58]

In recent decades, the public discourse surrounding cyber warfare has created an atmosphere of uncertainty and the belief that everyone is vulnerable to cyberattacks.[59] Additionally, the downplaying of cyber-attacks and data breaches increases the belief that a cyber war is unlikely to happen; creating an almost paradoxical climate. Western states are anxious about their vulnerabilities to cyber-attacks yet they downplay the economic and social damage it can have on their societies. The notion that cyber cannot be a tool for war is itself dated and naïve. The international community has not witnessed a cyber war; therefore, it is vital that the study of cyber warfare theory be expanded in the coming years to prevent the possibility or at least limit the destructive ability of one. According to Kallberg, strategic cyber discourse in recent years has a limiting central theme that cyber can only support and enable existing military and geopolitical operations.[60] Existing cyber theory is simplistic and doesn't account for capabilities that could possibly develop in 30 to 40 years, and instead bases its analysis on current capacities. Kallberg states, "the main risk in the current cyber discourse focuses on cyber as purely an enabler of joint operations." This is a result of traditional perceptions of war, and in order to advance the discussion of cyber warfare theory, then the shortcomings of current theory must be addressed. Kallberg lists some shortcomings in current cyber warfare theory:

1. Lacking understanding of the reserved asymmetry of the conflict, where a state can attack domestic public entity and individual citizens,
2. Ignoring the absence of object permanence,
3. The belief that cyber conflicts solely will be match between military networks,
4. That digital interchange is conducted according to our concept of ethics and norms,

[57] Ibid.
[58] Ibid.
[59] Ibid.
[60] Ibid.



DOI:10.6814/NCCU202000853

5. Absence of acceptance of the rapid time frame interchanges will occur,
6. Reliance of non-existent measure of effectiveness (MOE),
7. Weak comprehension of the imminent future's automated computational speed conducted harvest of vulnerabilities and execution of attacks, and
8. The impact of artificial intelligence in combination with automated harvest vulnerabilities[61]

Cyber capabilities offer a strategic opportunity that will grow in coming decades. Cyber effects will be limited if subordinated to enabler status, and by doing so provide democracies reduced military options. In order to craft a cyber theory that encompasses the characteristics Chinese cyber activities, we must look to classical theories regarding political warfare and how to update them to account for 21st century cyber capabilities. In the next section, we will be exploring how modern state actors have utilized modern political warfare capabilities that incorporate elements of cyber warfare to carry out their goals.

## Political Warfare Re-Contextualized

### *Cyber Espionage and Political Warfare*

In the wake of the 2016 United States Presidential election, two areas within the cyber domain have attracted a large amount of media attention: cyber-enabled espionage and political warfare.[62] While espionage and political warfare are not entirely new concepts, recent cyber capabilities and technological advancements have made political warfare campaigns more pervasive and successful due to the advantages that cyber can provide.[63] Cyber has allowed agents of political warfare direct access to their targets, as well as the ability to disguise their identity and intent. As a result, this has had a damaging effect on democracies who require

[61] Ibid.
[62] Thomas Paterson & Lauren Hanley. (2020). Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'. Australian Journal of International Affairs. 1-16. 10.1080/10357718.2020.1734772.
[63] Ibid.



DOI:10.6814/NCCU202000853

legitimacy and a certain level of transparency in order to function properly.[64] A study published by the Australian Journal of International Affairs outlines how the proliferation of the internet means that states are increasingly able and willing to use political warfare tactics against one another in order to achieve strategic goals.[65] Additionally, democratic states are more vulnerable to cyber-enabled political warfare tactics than their autocratic counterparts, in part because of their personal freedoms and civil liberties given to their citizens.[66] According to the study, cyber-enabled espionage and information theft is extremely damaging because it can be used to assist and augment existing political warfare campaigns.[67]

The act of engaging in espionage to obtain state secrets has been around for thousands of years, gradually evolving over time, and being further enhanced in the age of cyber. Cyber-enabled espionage has been occurring for decades and has now become the favored method for both state and non-state actors to gather information.[68] The CCP has a history of engaging in cyber-enabled espionage because it favors the low risk-high reward factor associated with cyber-attacks.[69] China feels the need to invest in cyber espionage because of the economic returns it can gain from activities such as intellectual property theft. The resulting reward is advancements in technology to help contribute to economic success, to support the CCP's legitimacy at home, and influence policy aboard. While cyber espionage results in informational, technological and financial loss, it is important to note that it does not damage democratic legitimacy in the same way that political subversion does.[70]

Subversion is a sub-category of political warfare and seeks to undermine institutional legitimacy and authority as part of a broader political warfare campaign.[71] Political subversion

[64] Ibid.; note that the extent of which political subversion causes damage to democratic legitimacy requires further study.
[65] Ibid.
[66] Ibid.
[67] Ibid, pp. 3-4
[68] Ibid.
[69] Jan Kallberg, "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review* 1, no. 1 (2016): 113-28. www.jstor.org/stable/26267302.
[70] Thomas Paterson & Lauren Hanley, "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes,'" *Australian Journal of International Affairs*. 1-16. 10.1080/10357718.2020.1734772.
[71] Ibid.



DOI:10.6814/NCCU202000853

poses a greater threat compared to cyber-enabled espionage because it serves to undermine the sovereignty and democratic principles of the target state and represents an existential threat to that state's government.[72] It challenges the values, beliefs, and societal stability of states, something that Kallberg emphasizes is at risk to cyber-attacks.[73] Political subversion campaigns have the potential to undermine the democratic process, causing voters to lose trust in their government and constitution.[74] Damage to a democracy's legitimacy is an even greater loss than economic and monetary loss because it is an immeasurable factor. Additionally, a subversive political warfare campaign may never be fully uncovered; and even if it is, the damage to a state's democracy cannot easily be undone.[75]

### *Political Warfare*

In 1942, during the Second World War, the Political Warfare Executive of the British Government compiled a brief but wide-ranging manual titled, *The Meaning, Techniques and Methods of Political Warfare.*[76] The manual understood political warfare as the "indispensable component of Total War" and a "systemic process" that employs both publicity and propaganda in order to "influence the will and so direct the *actions* of peoples in enemy and enemy-occupied territories, according to the needs of higher strategy."[77] In 1948, at the outset of the Cold War, U.S. diplomat George Kennan defined political warfare as, "the logical application of Clausewitz's doctrine in time of peace.[78] According to the RAND Corporation:



[72] Ibid.
[73] Jan Kallberg, "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review* 1, no. 1 (2016): 113-28. www.jstor.org/stable/26267302.
[74] Thomas Paterson & Lauren Hanley, "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes,'" *Australian Journal of International Affairs*. 1-16. 10.1080/10357718.2020.1734772.
[75] Ibid.
[76] Antonios Nestoras. "Political Warfare: Competition in the Cyber Era." Martens Centre For European Studies, April 2019. https://www.martenscentre.eu/sites/default/files/publication-files/cyber-warfare-politics-era.pdf.
[77] Ibid.
[78] Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, *The Growing Need to Focus on Modern Political Warfare.*



DOI:10.6814/NCCU202000853

> Political warfare is the employment of all means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (such as the Marshall Plan), and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states.[79]

By this definition, the key point is *short of war*, referring to the current state of competition, which is just short of the state of armed conflict. The term "warfare" should be limited to the "physical conduct of war or the fighting and violent aspects of war" but fails to encompass the current conditions at the given time.[80] During a state of competition or open hostility, states can employ tactics through non-violent means, utilizing overt and covert operations such as public diplomacy, propaganda, terror, and psychological warfare.[81]

According to a research brief by the RAND corporation, political warfare consists of the intentional use of one or more of the implements of power to affect the political compositions or decision-making in a state.[82] Those implements of power are shown below in a chart illustrated on the research brief. Based on research focused on three case studies – two state actors (Russia and Iran) and one non-state actor (the Islamic State of Iraq and the Levant aka. ISIL) – the study attempted to derive common characteristics of modern political warfare from each of these cases.[83] In Estonia, Russia has capitalized on the sentiments of Russian minorities and mobilized them to carry out protests, a sustained cyber-attack, and later sanctions.[84] The Russian government has maintained a hostile stance in order to destabilize Estonia and other Baltic

(Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_briefs/RB10071.html.

[79] Ibid.

[80] Antonios Nestoras, "Political Warfare: Competition in the Cyber Era." *Martens Centre For European Studies*, (April 2019). https://www.martenscentre.eu/sites/default/files/publication-files/cyber-warfare-politics-era.pdf.

[81] Ibid.

[82] Ibid.

[83] Ibid.

[84] Ibid.



DOI:10.6814/NCCU202000853

states.[85] Iran has engaged in political warfare in Syria as part of its efforts to extend its influence in the region and to ensure a pro-Iranian government in Damascus.[86] To achieve this goal, Iran has attempted to indoctrinate the National Defense Force militias with Islamic revolutionary ideology, appealed to foreign Shi'a fighters' desire to protect Syria's holy shrines, taken advantage of Syria's economic dependency to increase Tehran's influence over the Damascus government, and engaged in public diplomacy to draw Syrians to the Islamic Republic.[87] When researching these three case studies, the study was able to list key attributes that broadly describe how political warfare is carried out in these modern-day case studies. What was found is that political warfare:

- Employs diverse elements of power, including a preponderance of nonmilitary means;
- Relies heavily on unattributed forces and means;
- Is increasingly waged in the information arena, where success can be determined by the perception rather than outright victory;
- Uses information warfare, which works by amplifying, obfuscating, and, at times, persuading;
- Is employed with cyber tools to accelerate and compound effects;
- Increasingly relies on economic leverage as the preferred tool of the strong;
- Often exploits shared ethnic or religious bonds, as well as social divisions or other internal seams;
- Extends, rather than replaces, traditional conflict and can achieve effects at lower cost;
- Is also conducted by empowered non-state or quasi-state actors; and
- Requires heavy investment in intelligence resources to detect it in its early stages

From these characteristics, one can see that the importance of information stands out among others. The RAND Corporation calls this the information space and emphasizes that this area can profoundly affect all other lines of effort, and that it must be considered at the highest levels of government.[88] The transformation of technology has completely revolutionized the way we

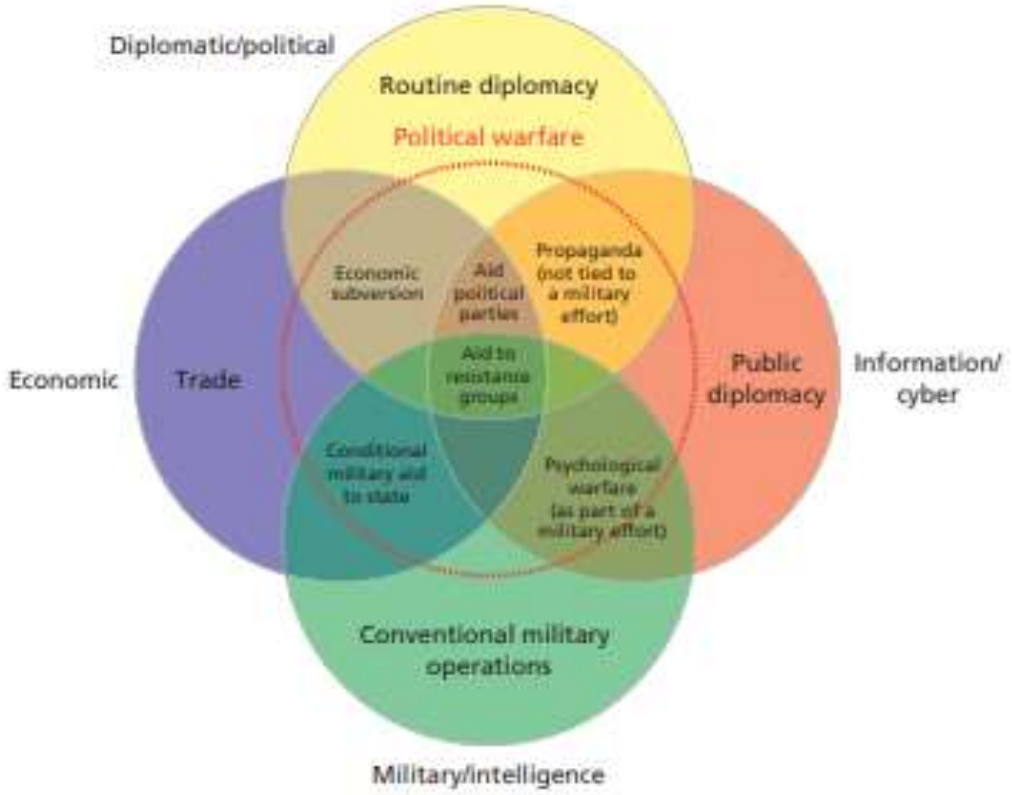
[85] Ibid.
[86] Ibid.
[87] Ibid.
[88] Ibid.



DOI:10.6814/NCCU202000853

obtain and consume information, therefore new models and theories encompassing political warfare, cyber warfare, and the ever changing landscape must be developed. China is keenly aware of the power information can have when controlling narratives and influencing public opinion abroad, making their political warfare tactics all the more threatening. The next section explores "Hybrid Warfare," which is a similar concept to political warfare but is described as using a belligerent use of irregular tactics used to describe a new generation of warfare that could be utilized to describe China's strategy against Taiwan.

**Figure 1. Where Political Warfare Fits Within the Implements of Power**




NOTE: All activities are illustrative, rather than an exhaustive list of possible actions.

- Fig. 1: Implements of Power (Listed in order clockwise): diplomatic/political, information/cyber, military/intelligence, and economic.[89]

[89] Ibid.



DOI:10.6814/NCCU202000853

In the wake of the COVID-19 global pandemic, China is active in its political warfare campaign not only against Taiwan but in the international area too. China is currently trying to shape the world's perception of COVID-19; and the narrative surrounding its role in it by denying any responsibility for the rise of the global pandemic and shifting blame towards the United States.[90] When China is trying to influence public opinion, it utilizes its "three warfares" principles, a political warfare strategy. According to Dean Chang of the Heritage Foundation, in the context of their activities during COVID-19, "it's essential to recognize that when the Chinese Communist Party talks about 'public opinion warfare,' wages the 'three warfares,' or thinks about political warfare, in each instance it's doing so as warfare, period."[91]

## China's "Three Warfares"

The CCP introduced the concepts of public opinion warfare, psychological warfare, and legal warfare when it revised its *Political Work and Guidelines of the People's Liberation Army* doctrine in 2003.[92] The main goal of the "Three Warfares" is to essentially generate political power on all fronts; Public Opinion Warfare influences domestic and international public opinion to build support of China's military actions and dissuade an adversary from pursuing actions contrary to China's interests; Psychological Warfare undermines an enemy's ability to conduct combat operations by deterring, shocking, and demoralizing the enemy's military personnel and supporting their civilian populations; and Legal Warfare seeks to build legal justification and context for Beijing's actions.[93] Additionally, Legal Warfare is intended to build international support and manage possible political repercussions for China's military actions.[94]Media warfare incorporates mechanisms for messages that are delivered, while legal warfare provides the

[90] Dean Cheng, "For the Chinese, Political Warfare Is War by Other Means," The Heritage Foundation, *Report* April 2, 2020. https://www.heritage.org/asia/commentary/the-chinese-political-warfare-war-other-means.
[91] Ibid.
[92] Peter Mattis, "China's 'Three Warfares' in Perspective," *War on the Rocks*, January 30, 2018. https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.
[93] Emilio Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," *Journal of Strategic Security* 9, no. 2 (2016): 45-69. www.jstor.org/stable/26466776.
[94] Ibid.



DOI:10.6814/NCCU202000853

justification for why actions are permissible. Psychological warfare provides the necessary nuance in leveraging the dissemination capability of the media and the more formalized legal mechanisms to substantiate its activities to domestic and international audiences. When the three are utilized to optimal capacity, China able to influence an international narrative while facing little to no consequences.[95]

Emilio Iasiello, a strategic cyber intelligence analyst, in his article *China's Three Warfares and Strategy Mitigates Fallout From Cyber Espionage*, theorizes and analyzes why China has faced few consequences over cyber espionage activities, and offers insight into Chinese Cyber Warfare tactics and strategy.[96] Iasiello believes that the negative press received from these activities are feeding into the perception that China's global "rise" is predicated on intellectual property theft and cyber espionage in order to overtake the United States' place in the international order.[97] To combat this perception, this article suggests that China has leveraged its "Three Warfares," a three-prong information warfare approach composed of Media, Legal, and Psychological components to influence the international community; and forestall the development and implementation of any effective counter strategy.[98] Iasiello states:

> The key takeaway here is that cyber warfare is directly related to 'information advantage' and not military advantage, suggesting that peacetime cyber activities are more about bolstering China's development in strategic areas and less about establishing military superiority vis-a-vie reconnoitering a future battle space.[99]

This research will be focusing on China's public opinion/media warfare campaign against Taiwan. The CCP is constantly trying to undermine Taiwan's democratic legitimacy in order to weaken its institutional stability by influencing the public opinion of its citizens through the dissemination of misinformation.[100] The case of the COVID-19 global pandemic is no different. As previously stated by Dean Chang, China is attempting to shape the world's view of COVID-

[95] Ibid.
[96] Ibid.
[97] Ibid.
[98] Ibid.
[99] Ibid.
[100] Anonymous source from an Associate Research fellow on Taiwan's National Security Council. Interview conducted on May 2, 2020.



DOI:10.6814/NCCU202000853

19, deflecting accusations associated with the virus and shifting blame towards the United States.[101] Earlier evidence of China trying to influence public opinion abroad includes Taiwan's 2018 local elections and 2020 Presidential election, where fake news articles were frequently cited and are suspected to have originated from mainland China.

## Waldo's Five Pillars for Societal Stability

In his article, *Strategic Cyberwar Theory - A Foundation For Designing Decisive Strategic Cyber Operations*, Dr. Jan Kallberg argues that there is a need for cyber theory in order to deal with the uncertainty of the future. Traditional military theory cannot account for modern advantages and capabilities cyber technology provides, such as anonymity, object permanence, measurable results, and rapid digital execution.[102]

By following the logic and principles of political science and international relations theory, societies are upheld by their institutions, and institutional resilience varies from state to state and in different contexts. If institutions fail, then society will destabilize, and a destabilized society is vulnerable to be subdued by a foreign power. These challenges could be said to be relevant for Taiwan and the United States, as both states are currently the targets of cyber-attacks by the mainland. China is currently engaged in a political warfare campaign against Taiwan, attempting to undermine Taiwan's democratic process, attacking its institutions to destabilize its society and subjugate the state to Beijing's will.[103] Kallberg states:

> Following the stated known, strategic cyberwar theory seeks to explain how an adversarial society can be destabilized and subdued by a major cyber campaign. Cyber War has to be quickly executed, shocking the targeted society, and at the

[101] Dean Cheng, "For the Chinese, Political Warfare Is War by Other Means," *The Heritage Foundation*, (April 2, 2020). https://www.heritage.org/asia/commentary/the-chinese-political-warfare-war-other-means.
[102] Jan Kallberg, "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review* 1, no. 1 (2016): 113-28. www.jstor.org/stable/26267302.
[103] Thomas Paterson & Lauren Hanley, "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes,'" *Australian Journal of International Affairs*. 1-16. 10.1080/10357718.2020.1734772.



DOI:10.6814/NCCU202000853

same time avoid adaptive behavior that mitigates the damages from the attacks. The rapid execution denies the targeted nation the opportunity to create defensive measures and eliminate any possibility to strategically lead a coherent cyber defense.[104]

If a nation state seeks to conduct a decisive cyberwar, it will be through launching systematic destabilization attacks on the targeted society; in the case of Taiwan, cyber-attacks and the spread of misinformation attempting to undermine its democracy.[105] Kallberg introduces Dwight Waldo's Five Pillars for Society Stability to support the claim that, if any major cyber-attack undermines these pillars, then the targeted state is weakened and risks implosion.

***Legitimacy*** – Waldo believed in the Lockesian theory that citizens must have faith in their government; that in order for a government to have legitimacy, it must promise and deliver a better life for its citizens. A cyberattack seeking to damage state legitimacy could attempt to create an assumption that state leadership is unable to govern its country.

***Authority*** – Authority is accountability for any persons in leadership or organization. If there is no accountability, then any organization or politician could fall into entropy and anarchy.

***Institutional Knowledge*** – Knowledge management poses one of the major challenges for a state when governing its citizens. If public administrations are unable to organize knowledge and information, citizens are left with the impression that the government is incompetent. In this information age, the sheer overwhelming amount of data can create massive difficulties in data management. According to Kallberg, if a lack of knowledge and coordination directly affects citizens, it undermines their perception of how well the government is working.

[104] Jan Kallberg. "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations." *The Cyber Defense Review* 1, no. 1 (2016): 113-28. www.jstor.org/stable/26267302.
[105] Anonymous source from an Associate research fellow on Taiwan's National Security Council. Interview conducted on May 2, 2020.



DOI:10.6814/NCCU202000853

Cyber-attacks on institutional knowledge management could cripple the bureaucracy, creating or emphasizing inefficiencies and angering the population.

***Bureaucratic Control*** – A large bureaucracy requires an extensive degree of coordination by a state's government. As bureaucracy expands, so do issues of control and regulation. And if control is lost, then corruption, favoritism, and public theft could ensue, leading to popular discontent.

***Confidence*** – According to Waldo, when people feel secure, they have confidence and are optimistic about the future; therefore, they trust their government will provide necessary support. In this scenario, confidence is trust in the government to deliver to the society what was promised. The difference between confidence and authority is that authority is defined in the present while confidence is forward-looking. Signs of systematic failure will harm the citizenry's ability to maintain confidence in government.[106]

If China is able to exploit these five pillars, Taiwan risks societal collapse at the hands of Beijing's cyber campaign. Societies are constantly engaged in conflicts and the cornerstone of any society is its institutions. The institutional resilience varies from state to state, from stable democracies to totalitarian states on the brink of entropy. If institutions fail, society will be destabilized and weakened. A destabilized society collapses or is subjugated to foreign powers, and strategic cyberwar theory seeks to explain how an adversarial society can be destabilized and subdued by a major cyber campaign.[107] Cyberwar must be capable of shocking the target society, which then causes disarray and denies the development of an effective counter-strategy.[108] A cyber-attack that undermines institutional legitimacy has the potential to destabilize a society and greatly harm democratic states who rely on that legitimacy. In the next chapter, I will be exploring Chinese strategic cyber objectives and tactics.

[106] Jan Kallberg, "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review* 1, no. 1 (2016): 113-28. www.jstor.org/stable/26267302.
[107] Ibid.
[108] Ibid.



DOI:10.6814/NCCU202000853

## Chapter 3 – China's Objectives and Tactics

As previously stated, China is at ideological odds with the West when it comes to how a state should govern its citizens online. In this section I will be covering how China's ideological odds with the West is significant in its cyber warfare campaign, as it ties into the Public Opinion Warfare aspect of the "Three Warfares" principle.[109] Beijing has been able to leverage international influence to campaign for a "states-rights" approach to internet governance while the United States has support a multi-stakeholder model.[110] The Atlantic Council's Jason Healey describes this divergence in ideology as "a bifurcation between east and west" that allows little room for compromise.[111] Beijing rejects the model of an open Internet which the United States and its allies are in support of. On December 16, 2015, Xi Jinping called upon the international community to "respect the right of individual countries to independently choose their own path of cyber development and model of cyber regulation and participate in international cyberspace governance on an equal footing."[112] Additionally, in a critique of the U.S., Xi said, "Existing rules governing cyberspace hardly reflect the desires and interests of the majority of countries."[113]

Chinese foreign policy has shifted in recent years to adopt two key stances: defending China's *core interests* (核心利 益), and *the great rejuvenation of the Chinese nation* (中华民族伟大复兴), or often referred to as the "China Dream *(zhongguomeng)*."[114] According to the RAND corporation, the adoption by China of the "core interests" framework focused on three basic goals: preserving China's basic state system and national security; protecting China' sovereignty and territorial integrity; and continuing the stable development of China's economy

[109] Emilio Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," *Journal of Strategic Security* 9, no. 2 (2016): 45-69. www.jstor.org/stable/26466776.
[110] Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017): 119-54. Accessed May 22, 2020. www.jstor.org/stable/26267405.
[111] Ibid.
[112] Huaxia, ed., "Highlights of Xi's Internet speech," *Xinhua*, December 16, 2015, http://news.xinhuanet.com/english/2015-12/16/c_134923855.htm.
[113] Ibid.
[114] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*. (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html. Also available in print form.



DOI:10.6814/NCCU202000853

and society.[115] From those core interests, we can begin to understand where the utilization of political warfare, and cyber warfare come into play; and why China feels that carrying out a political warfare campaign against Taiwan is necessary and aligns with its core interests. Both stances have overlapping goals, and interpretations on how to achieve those goals by Chinese scholars and observers. To support this statement, the RAND Corporation states:

> In practice, the first core interest is largely consonant with the preservation of the ruling status of the CCP while the second and third interests serve as means to this end through the retention of control over Xinjiang and Tibet; the defense of China's claims in the South and East China seas; and the prevention of Taiwan independence, leading to the island's ultimate absorption. By contrast, the "China dream," while necessarily entailing the retention and/or integration of territories that Chinese leaders regard as theirs, looks further afield to a more ambitious set of goals. These include domestic economic goals such as achieving the "two 100s" which are linked to the centenaries of the founding of the CCP, in 2021, and of the PRC itself, in 2049; reducing social inequality; cleaning up the environment; developing national morals; and achieving the "strong nation dream" (强国梦) of returning the country to a position of region and global preeminence.[116]

The "Chinese Dream" helps guide all facets of the Chinese government towards a single overarching goal.[117] In 2012, Xi Jinping described the Chinese dream as the collective rejuvenation-a revival of prosperity, unity and strength; and in a 2015 interview with the *Wall Street Journal*, Xi explained that in order to understand the Chinese Dream "one needs to fully appreciate the Chinese nation's deep suffering since modern times and the profound impact of such suffering on the Chinese minds."[118] Within these two frameworks, it stands to reason that the CCP would be engaged in a political warfare campaign aimed at Taiwan. If the eventual strategic goal is the reunification of Taiwan with the mainland, then Beijing will employ whatever means it has at its disposal, in order to undermine Taiwan's democracy and prevent the

[115] Ibid.
[116] Ibid.
[117] Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017): 119-54. www.jstor.org/stable/26267405.
[118] Ibid.



DOI:10.6814/NCCU202000853

Taiwan independence movement from gaining momentum.[119] Additionally, this means preventing any third party intervention in that effort, most notably by causing rifts in foreign relations with states like the U.S., Australia, Japan, and South Korea. As previously emphasized by President Xi, China seeks to "democratize" international society, by advocating for a "state-rights" approach where individual states can choose their social, political, and economic systems, free from criticism.[120] China is determined to achieve its ultimate goal of rejuvenating the state from its "Century of Humiliation" and will incorporate strategic political warfare tactics to spread its influence and hold in territories like Hong Kong and Taiwan. Chinese citizens believe that under the guidance of the CCP, the state can pursue the "Chinese Dream" through its growing international strength free from foreign interference.

**Importance of the People's Liberation Army to the Chinese Dream**

As the armed wing of the Chinese Communist Party, the People's Liberation Army (PLA), is tasked with safeguarding the national strategic goal of the "Chinese Dream." From this perspective, the PLA must fulfill its mandate *(luxing shiming)* as the Party's army, and the armed forces must always obey the Party.[121] According to Kolton, the CCP expects the PLA to guarantee "a stable external environment for continued economic development," and ties its success to the political success of the state. As the armed wing of the party, and because the PLA is tasked with carrying out the ideology of the party, military strategy must coincide with the CCP's strategic goals.

In May 2015, China's Ministry of National Defense (MND) published a white paper articulating the country's military strategy. According to Kolton, this document reimagined military power and called for the PLA to abandon its traditional emphasis of land warfare.

[119] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends.* (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html. Also available in print form.
[120] Ibid.
[121] Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017): 119-54. www.jstor.org/stable/26267405.



DOI:10.6814/NCCU202000853

Several authoritative Chinese sources described the white paper as an accurate indicator of the PLA's strategy and a call for it to adapt to new political warfare strategies to adapt to the modern military landscape.[122] Anthony Cordesman and Steven Colley of the Center for Strategic and International Studies (CSIS) also accept what this white paper means for understanding PLA strategic thinking.[123] It is important to note, however, that publications that reveal this amount of information usually fail to confirm which concepts the PLA operationalize and which ones they reject.[124] As such, it is difficult to determine which particular areas the PLA places a strategic importance on, oftentimes referring to these concepts in vague or abstract terms. Additionally, PLA texts do not necessarily reflect the views of the CCP, nor the entire Chinese government. Nevertheless, Kolton believes that the MND white paper is helpful when it comes to understanding PLA thinking.[125] The 2015 Military Strategy explains, "China's armed forces take their dream of making the military strong as part of the Chinese Dream. Without a strong military, a country can be neither safe nor strong."[126] Using this logic, China identifies the need for an advanced military in order to achieve its strategic goals. According to Kolton:

> As the country aims for the "Chinese Dream," the strategic end-state for the PLA can be expressed in three sub-objectives: sovereignty, modernity, and stability. These goals translate into enduring themes for the military: (1) Protect the Party and Safeguard Stability, (2) Defend Sovereignty and Defeat Aggression, (3) Modernize the Military and Build the Nation. To accomplish these end, the MND assigns its armed forces strategic tasks *(zhanlu renwu)*, which guide the employment of resources to accomplish objectives.[127]

[122] Ibid.
[123] Anthony H. Cordesman and Steven Colley, "Chinese Strategy and Military Modernization in 2015: A Comparative Analysis," *Center for Strategic and International* Studies (October 10, 2015), 121.
[124] Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017): 119-54. www.jstor.org/stable/26267405.
[125] Ibid.
[126] Ibid.; David M. Finkelstein, "China's National Military Strategy," in James C. Mulvenon and Richard H. Yang, eds., *The People's Liberation Army in the Information Age*, (Santa Monica, CA: RAND Corporation, 1999), 103.
[127] Ibid.



DOI:10.6814/NCCU202000853

In meeting these objectives, China has set two decisive milestones called the "two centenaries" *(liang ge yibai nian)* that Western scholars frequently cite as deadlines for Chinese overseas activities in the South China Sea, Hong Kong, and Taiwan.[128] The first centenary is set in 2021, one hundred years after the founding of the CCP and the second in 2049, making the one-hundred-year anniversary of the founding of the People's Republic. At this point, the CCP hopes and plans to achieve its goal of returning China to a "prosperous, strong, democratic, culturally advanced and harmonious" society.[129] In October 2015, the Fifth Plenary Session of the 18th CCP Central Committee reaffirmed the two centenaries in its 13th Five-Year Plan.[130] Additionally, Xi identified international stability as one necessary condition for the Chinese Dream. President Xi evaluates the success of the CCP in terms of achieving the Chinese Dream with the centenaries set as deadlines to meet certain accomplishments. Thus, the Chinese Dream and the two centenaries orient and pace the PLA as it operationalizes the national military strategy.[131]

In the case of cyber, members of the CCP have unique ways and means of interpreting and pursuing the use of cyber and how to implement cyber warfare strategies to achieve their goals. In the case of Taiwan, one retired PLA lieutenant general believes cyber operations enable China to pursue reunification with Taiwan and to realize the Chinese Dream without lethal military conflict.[132] In the 12th National Committee of the Chinese People's Political Consultative Conference (CPPCC), this general argued that the PLA must develop sophisticated cyber capabilities in order to "defeat its adversaries without fighting," emphasizing the low risk-

[128] Michael D. Swaine, "Xi Jinping's Address to the Central Conference on Work Relating to Foreign Affairs: Assessing and Advancing Major- Power Diplomacy with Chinese Characteristics," *China Leadership Monitor* 46 (March 19, 2015); David M. Finkelstein, "China's National Military Strategy," in James C. Mulvenon and Richard H. Yang, eds., *The People's Liberation Army in the Information Age*, (Santa Monica, CA: RAND Corporation, 1999), 103.
[128] Ibid.
[129] Michael Kolton. "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence." *The Cyber Defense Review* 2, no. 1 (2017): 119-54. www.jstor.org/stable/26267405.
[130] Ibid.; Yin Pumin, "Mapping Out Success: New five-year blueprint lays down specific objectives for a prosperous China," *Beijing Review* 45 (November 5, 2015), http://www.bjreview.com.cn/Current_Issue/Editor_ Choice/201511/t20151102_800041696.html.
[131] Ibid.
[132] Ibid.



DOI:10.6814/NCCU202000853

high reward factor associated with cyber.[133] From this logic we can deduce that China favors cyber tactics in order to avoid armed military conflict, and to minimize risk and condemnation from the international community. As previously mentioned, the ability of cyber warfare to enhance an existing political warfare campaign, such as undermining democratic legitimacy, coincide with the CCP's larger strategic goals of reuniting Taiwan with the mainland.

## Why is Taiwan Important to China?

The CCP has long placed strict restrictions on the information related to their plans on Taiwan in order to ensure that any publications released serve as propaganda and psychological warfare. As a result, it has been nearly impossible for American scholars to use open source to understand Chinese military thinking regarding Taiwan. To make the issue more frustrating, the most readily available Chinese sources regarding Taiwan are intended to spread misinformation. The CCP goes to great lengths to assure its audience that victory is inevitable no matter what. Its intent is for Taiwan and the U.S. to believe that every effort to defend the island is futile.[134]

Ian Easton, in his book *The Chinese Invasion Threat*, argues that the CCP is funneling massive amounts of resources into creating a powerful military machine in order to acquire the capabilities needed to annex or conquer Taiwan[135]. As previously mentioned, this goal is part of its greater objective of "achieving national unification." Though, it is important to note that the rapid expansion of China's military power does not necessarily mean war is imminent or even likely.[136] According to Easton:

> The PRC has long sought the annexation of Taiwan under its "one China" principle. In Beijing's view, Taiwan's de facto independence and democratic system of government pose existential threats to the CCP's right to rule China. Taiwan is thus portrayed in Chinese propaganda as a "splittist regime." Legitimacy across the

[133] Ibid.
[134] David Shambaugh appears to be the first American "China Hands" to recognize and record this phenomenon. See his book, *Modernizing China's Military: Progress, Problems, and Prospects* (Los Angeles, CA: University of California Press, 2002), pp. 307-311.
[135] Ian Easton. *The Chinese Invasion Threat: Taiwan's Defense and American Strategy in Asia*. (Manchester: Eastbridge Books, 2019).
[136] Ibid.



DOI:10.6814/NCCU202000853

> Taiwan Strait is viewed as something political scientists typically refer to as a "zero-sum game" because only one side can win, and that will necessarily mean that the other side must be vanquished. China's stated goal is Cross-Strait unification under a formula called "One Country, Two Systems." This approach envisions the ROC government in Taiwan surrendering sovereignty to the PRC authorities, allowing them to transform the island nation in to an occupied, authoritarian administrative territory like Hong Kong.[137]

Under the long-term objective of achieving the "Chinese Dream," under the "one China" principle, the PLA under the CCP has been driven to bolster its military for future war in the Taiwan strait. Invading Taiwan is something that is at the heart of the PLA's desire to "liberate" Taiwan; it is something that has been indoctrinated and instilled into the minds of all high-ranking officers.[138] Easton emphasizes that, to the PLA, the interests of the regime (the CCP) are paramount over the interests of the people of China, and its "main strategic direction" is to annex Taiwan.[139] Chinese leadership understands and recognizes the roadblocks ahead and will continue to invest heavily in "strategic deception, intelligence collection, psychological warfare, joint training and advanced weaponry."

## Chinese Tactics and Strategies: Public Opinion Warfare

When talking about Chinese political warfare strategies, it is impossible to ignore the CCP's weaponization of Public Opinion Warfare and in the cyber age. According to a study by the RAND Corporation, "thought work" or the information operations of the Party, the state, and the PLA are often collectively referred to as "public opinion management" when undertaken inside China and "overseas propaganda work" when conducted outside of the PRC.[140] The overall goal of these public opinion operations is to defend the ruling status and interests of the

[137] Ibid.
[138] Ibid.
[139] Ibid.
[140] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*. (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.



DOI:10.6814/NCCU202000853

CCP while expanding its ability to shape the international context regarding China. Reshaping context and narrative allows more room for the CCP to pursue its objectives of the "Chinese Dream." Domestic efforts to control public opinion primarily seek to distract and disperse discussions that carry the potential to undermine regime legitimacy.[141] As previously mentioned, the CCP and Chinese scholars are highly aware of the impact cyber and social media can have on the mobilization of anti-regime sentiment. Public opinion warfare at home means influencing society so that it remains stable and does not question the ruling status of the CCP. External operations are often aimed at specific targets such as ethnic minorities (Tibetans, Uighurs, Mongols, and others), democracy advocates in Hong Kong, and Taiwan independence activists. Additionally, at both the regional and global levels, Chinese academics, think-tank analysts, and even top leaders have highlighted the roughly 60 to 65 million overseas ethnic Chinese who could be potentially utilized to spread economic, diplomatic and political influence.[142] For this reason, Beijing places an extremely high priority on controlling as many international Chinese-language media outlets as possible, from Hong Kong, Taiwan, Singapore, all the way to the United States and Australia, where millions of ethnic Chinese reside. This is not something entirely new to China as author and prominent Chinese social critic Murong Xuecun has noted.[143] Since its establishment in 1949, the PRC has been utilizing tactics such as propaganda to influence public opinion with some activities even dating to the CCP's founding in 1921.[144] For China, foreign policy begins at home, and the majority of the PRC's efforts over recent decades to use information for political goals and to shape public opinion through propaganda has been focused first on defending the regime and secondarily on swaying foreign audiences."[145]

[141] Ibid.
[142] Ibid.
[143] Murong Xuecun, "The New Face of Chinese Propaganda," *New York Times*, December 20, 2013.
[144] Ibid.
[145] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*. (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.



DOI:10.6814/NCCU202000853

***Public Opinion/Media Warfare***

Public Opinion Warfare is utilized to influence domestic and international public opinion in order to build support of China's actions and to dissuade adversaries from pursuing actions contrary to China's interest; something that China has been able to leverage strategically in recent years. Through the use of various mediums such as the internet, television, news publications, movies, etc., the CCP's goal is to preserve a positive morale and generate public support at home and abroad.[146] China has, to a large extent, successfully utilized its media warfare by promoting a narrative of being a cyber-ally while tempering bad press when it is accused of conducting cyber espionage.[147] Dean Cheng, in another article, identifies four themes that are inherent in Chinese writings on public opinion:

> ***Follow Top- Down Guidance*** – Senior leadership will dictate courses of action based on strategic objectives.
>
> ***Emphasize Preemption*** – Chinese analyses of public opinion warfare emphasize that "the first sound grabs people, the first to enter establishes dominance (*xian sheng douren, xianru weizhu*)."
>
> ***Be Flexible and Responsive to Changing Conditions*** – Use of different propaganda activities depending on the audience. "One must make distinctions between the more stubborn elements and the general populace."
>
> ***Exploit All Available Resources*** – Civilian and commercial news assets such as news organizations, broadcasting facilities, internet users, etc., are seen as an invaluable resource in getting China' message before domestic and global audiences. [148]

[146] Emilio Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," *Journal of Strategic Security* 9, no. 2 (2016): 45-69. Accessed May 26, 2020. www.jstor.org/stable/26466776.
[147] Ibid.
[148] Dean Cheng, "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response," *Report,* The Heritage Foundation, No. 2745, November 26, 2012, http://www.heritage.org/research/reports/2012/11/winningwithout-fighting-chinese-public-opinion-warfare-and-the-need-for-a-robust-americanresponse.



DOI:10.6814/NCCU202000853

These themes provide insight into the logic behind Chinese media warfare. By generating public support domestically and abroad, China can weather most negative pressed aimed towards their activities. The CCP focuses on a mix of defensive and offensive information goals and walks a tightrope in balancing and controlling international narratives surrounding China. The RAND Corporations coins this strategy, "China's offensive approach to defense."

> It seeks to delegitimize opposition to CCP rule and paint those who would criticize the Party's leadership and its ruling status as an "extremely tiny handful" (**小数的小数**) of "anti-China" (**反**华) people with "ulterior motives" (别有用心) organized by "black hands" (**黑手**), often in the service of "hostile foreign forces" (敌对的外国实力). At the same time, in seeking to extend China's influence, the Party's propaganda embraces a dualistic image of the PRC's growing power as simultaneously entirely benign – characterized by a path of "peaceful development" (**和平**发展) and the embrace of the Five Principals of Peaceful Coexistence (**和平共**处五项原则) – but also inevitable and irresistible (and consequential if crossed).[149]

By utilizing this framework of public opinion warfare and "defensive and offensive" information goals, the CCP has engaged in political warfare campaigns that seek to spread various narratives domestically and internationally which, when joined in tandem, have consequential effects on their targets. The Chinese state has utilized an effective public opinion campaign to paint this narrative of China's rising being peaceful and necessary for the state's rejuvenation, and that anyone who opposes it, is simply against the progress and the changing of times. President Xi reportedly sees the combination of propaganda and public opinion manipulation in tandem with United Front activities as so important to the perpetuation of the CCP's power and the achievement of the regime's foreign policy goals that he made himself the head of a new

[149] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*. (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.



DOI:10.6814/NCCU202000853

bureaucratic agency, the United Front Leading Small Group (统一战线领导小组), in 2015.[150]

Public Opinion Warfare has the additional benefit of being extremely damaging when leveraged against democratic systems like Taiwan. Unlike China where state legitimacy is maintained through the centralized power of the CCP and its control on the public opinion and support of its domestic citizens, a democratic system like Taiwan, which thrives on the transparency and accuracy of information in order to maintain regime legitimacy, risks societal instability at the hands of Beijing's political warfare efforts through subversive and overt tactics such as military exercises, propaganda, cyber-attacks, and the spread of fake news and misinformation.

## Chinese Social Media Activities

This section will explore how China applies its cyber warfare strategy to its social media activities. China has been able to greatly leverage social media to re-contextualize narratives surrounding itself, and building a favorable public image of the state. According to the RAND Corporation, China's use of social media encompasses a range of activities that are categorized by their targets, and type of approach.[151] Promoting government narratives, enforcing the party line abroad, military strategic messaging, and spreading fake news will be the categorized activities that will be the focus of this section as these tactics can be seen in play in Taiwan. According to Easton:

> "Taiwan's rise as one of Asia's most vibrant democracies and an alternative to China's repressive authoritarian model is viewed with extreme concern in Beijing's halls of power. From China's perspective, the existence of Taiwan as a democracy is a grave challenge to its political legitimacy. The CCP views Taiwan as its most dangerous external national security threat, and the PLA, as the armed wing of the party and guarantor of the regime's fragile legitimacy, has been tasked with the mission of preparing for an assault on the island as its principal war planning scenario. The overarching plan is referred to in restricted-access Chinese military

[150] Ibid.; Gerry Groot, "The Long Reach of China's United Front Work," *Lowy Interpreter*, November 6, 2017.
[151] Ibid.



DOI:10.6814/NCCU202000853

writings as the "Joint Island Attack Campaign." The campaign includes operations that span the entire spectrum of the modern battlefield, including air, land, sea, space, and cyber space domains. Even media outlets area a target.[152]"

Because the Taiwan issue is "fundamentally political [by] nature," it means that the Chinese government will continue to conduct an all-out campaign, utilizing diplomatic, economic, and psychological warfare tactics.[153] This includes plans to utilize fake news and misinformation to spin international narratives surrounding Taiwan and to influence international law to delegitimize and demoralize Taiwan. This is what the PLA refers to this as "political warfare."[154]

***Promoting Government Narratives***

According to the RAND Corporation, press releases of official Chinese government and institutional positions represent the most common form of social media engagement by China. Most of these are government social media webpages or blogs where basic information and pre-approved data about an organization and its activities are presented. "For example, the SCIO has a Twitter page where it presents the latest approved releases from the Chinese central government, while the *People's Daily* maintains a Facebook account where it posts photos of foreign leaders visiting China, photos of panda, and stories about China's latest high-speed rail connections."[155] The activities are usually intended to present a favorable image of a China that is "well-led, respected, perceived as nonthreatening by the outside world," and advance Chinese interests.[156] One of the applications of this social media tactic is astroturfing where state-run or

[152] Ian Easton, *The Chinese Invasion Threat: Taiwan's Defense and American Strategy in Asia*. (Manchester: Eastbridge Books, 2019); *Informatized Army Operations*, pp. 109-119.
[153] Ibid.
[154] Ibid, pp. 119-121.
[155] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends.* (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.
[156] Ibid.



DOI:10.6814/NCCU202000853

state-orchestrated propaganda is present as if it were coming from the grassroots. In Taiwan, when President Tsai Ing-Wen was elected in January of 2016, there was a "coordinated grassroots messaging campaign" in which "attackers posted pro-mainland comments to show the reaction of Chinese citizens to Taiwan's election of Tsai and expressed a desire to reunify China and Taiwan."[157] This is just one example of Chinese government's ability to conduct propaganda campaigns utilizing foreign social media which could cause detrimental harm to Taiwan's democracy. Under President Xi, the Chinese government has tried to produce less forced, and formalistic propaganda products and now is regularly producing short videos that are intended for foreign audiences and distributed on Western social media platforms such as Twitter, YouTube, and Facebook; many of which are used by Taiwanese citizens as well. These videos have improved in quality and appeal over time and demonstrate that the CPP has the ability to adapt and appeal to foreign audiences on social media.

***Enforcing the Party Line Abroad***

Part of China's social media activities involve the theme of enforcing their Party Line abroad where they scrutinize and criticize statements and actions by foreign entities that do not necessarily comply with the CCP's doctrine. One example is its collection of information about foreigners from postings by Chinese citizens when they travel overseas.

> Such an approach effectively transforms any Chinese citizen using social media into an extension of the PRC state intelligence apparatus. This use of social media leverages reporting by Chinese citizens on overseas events that might "offend" Chinese sensibilities, potentially leading to costly consequences for foreigners, even in their own home countries. For example, in Australia, Chinese students in that country have posted on their WeChat accounts the personal information of professors who referred to Taiwan as a separate country or described border

[157] Ibid.



DOI:10.6814/NCCU202000853

> territories to which China lays claims as Indian territory, leading to a flood of online complaints against the schools where the faculty were employed.[158]

This effort has extended to foreign companies too as in January 2018, Marriott International, Delta Airlines, and Zara, among others, were forced to apologize for listing Tibet and Taiwan as separate countries.[159] In another incident, a Marriott employee accidentally "liked" a Twitter post by a Tibetan independence group that supported Marriott for listing Tibet as a separate country, leading to further Chinese criticism and the employee's eventual firing. This suggests a coordinated campaign of pressure against Western companies in service of upholding China's party line.[160]

***Military Strategic Messaging***

In terms of the military, the PLA and selected Chinese central government organs have posted several offensive messages on social media platforms when it served their interests. Some of these posts have been used for "signaling resolve, deterrence, or coercion to key domestic and overseas audiences by posting messages or imagery of PLA capabilities, exercises, or operations."[161] Much of this information could be signaled at Taiwan intelligence operations, intended to either to intimidate by showing-off their expanding capabilities, or deter by providing misinformation. This theory is further supported by the widespread "phenomenon of military enthusiast bulletin boards and websites that have frequently been the first to report the initial operations or roll-outs of Chinese capabilities, some of which are likely not even close to being ready for operation deployment."[162] According to the RAND Corporation:

> The fact that photos or information about such capabilities are not sanitized after their initial postings strongly suggests that either the information is deliberately leaked or Chinese military authorities believe that, once out in the public domain, such information can be leveraged to their advantage. One way that authorities may

[158] Ibid.
[159] Ibid.
[160] Ibid.
[161] Ibid.
[162] Ibid.



DOI:10.6814/NCCU202000853

> see such value is if the information circulating on the bulletin boards or fan websites convinces foreign powers that China has a capability that it has not yet fully perfected months or years in advance of its operational deployment, thereby shaping foreign behavior in ways that China prefers. For example, when information about China's first advanced stealth fighter, the J-20, first began circulating, it did so via images on military fan websites such as *Tiexue.net*. Most updates on China's aircraft carrier program and images of various other Chinese military hardware have been delivered in the same way.

In February of 2020, the Peoples Liberation Army forces participated in a joint air and maritime drill over two days involving back-to-back circumnavigating flights around Taiwan, while a Chinese aircraft carrier and attached group of warships sailed near the island in April.[163]

***Spreading Fake News***

The spread of fake news has become an international buzz topic after the 2016 U.S. Presidential Election, in which then-Republican Candidate Trump criticized American media outlets for disseminating fake "news." Russia and China both have histories of influencing foreign media through the distribution of misinformation and fake news. The RAND Corporation states that, "Chinese officials have attempted to distribute false, incorrect, exaggerated, or fabricated information through official, unofficial, covert, or clandestine social media accounts created or operated by human propagandists (五毛党) or artificial intelligence bots (机器五毛党)."[164] All known cases of China disseminating and fabricating false information have been exclusively found in Taiwan. China is reported to have manufactured disinformation against the Tsai administration about religion, retirement, and infrastructure.[165]As J. Michael Cole argues:

---

[163] "US Says Taiwan's Exclusion from WHO Caused Loss of Lives." Al Jazeera. *Al Jazeera News*, May 13, 2020. https://www.aljazeera.com/news/2020/05/taiwan-exclusion-caused-loss-lives-200513025007789.html.

[164] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends.* (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.

[165] Ibid.



DOI:10.6814/NCCU202000853

> Beijing also knows it can rely on traditional media in Taiwan to amplify the [disinformation] message through their own coverage, which – due to the competitive nature of Taiwan's media environment – often entails poor fact-checking and attribution. Thus a piece of (dis)information (or "fake news") originating in China will often go through a process of circular corroboration by replicators – traditional and online media – in Taiwan. As a result, this (dis)information is normalized and becomes part of the narrative. Subsequently, the (dis)information becomes the subject of heated debates on evening TV talk shows, compelling the embattled (and distracted) government to respond with denials or corrections.[166]

One example of this is a China-originated rumor from mid-2017 which claimed that the Tsai administration had banned the burning of incense and "ghost money" at Taoist temples.[167] This rumor was spread through Taiwanese social media, and ultimately led to a mass protest in Taipei where nearly 10,000 people turned out, demanding the government lift a ban which didn't exist.[168] Further examination by RAND researchers show that the original version of the document was in simplified Chinese rather classical Chinese and originated on COCO01.net, an online content farm with a track record of publishing false information about Taiwan.[169] "Taiwan's National Security Bureau (NSB) further asserted that China also used Weibo, WeChat, LINE, and other online media platforms to spread rumors that President Tsai would reform Taiwan's pension system and was threatening to cut off payments for those who left the

[166] For an overview of recent Chinese disinformation campaigns against Taiwan, see J. Michael Cole, "Will China's Disinformation War Destabilize Taiwan?" *National Interest*, (July 30, 2017); J. Michael Cole, "China Intensifies Disinformation Campaign Against Taiwan," *Taiwan Sentinel*, January 19, 2017a; Ying Yu Lin, "China's Hybrid Warfare and Taiwan," *The Diplomat*, (January 13, 2018).

[167] Lu Hsin-hui, Hsieh Chia-chen, Yeh Tzu-kang and Elizabeth Hsu, "Authorities Deny Rumor of Ban on Incense, Ghost Money Burning," *Central News Agency (Taiwan)*, July 21, 2017. https://focustaiwan.tw/politics/201707210016.

[168] "Taiwan's Taoists Protest Against Curbs on Incense and Firecrackers," *BBC News*, July 23, 2017. https://www.bbc.com/news/world-asia-40699113.

[169] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends.* (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.



DOI:10.6814/NCCU202000853

country."[170] This claim was confirmed by a National Security Council official, who stated that China utilizes Chinese-language social media such as WeChat, and LINE in Taiwan to disseminate fake news and misinformation.

## Chinese Military Activities

### *PLA Strategic Support Force*

The PLA Strategic Support Force (PLASSF) is a service branch of the People's Liberation Army and was established on December 31, 2015. This new branch was designed to facilitate the integration of capabilities for cyber, space, and the electromagnetic spectrum and would be integral in any future PLA plan to fight and win an "informationized" war.[171] Much of the information regarding this branch is limited and has been shrouded in mystery. Additionally, as previously mentioned, it is difficult to tell whether Chinese sources are accurate or merely contributing to the PLA's public opinion warfare, intending to influence foreign audiences and researchers with carefully planted information. As of now the PLASSF comprises of two departments: Space Systems, and Network Systems. Network Systems will be the focus as it is believed to be the source of China's growing cyber capabilities. One Taiwanese source claims that there may even be a third department called the "PLA Cyberspace Operation United of the Strategic Support Corps," which previously was a unit under the Headquarters of the General Staff.[172] This claim is further supported by a report by the Project 2049 Institute which states that:

> Recent references to a PLASSF "Third Department" may suggest either a third systems department or, more likely, the dominance of the former 3PLA within the

[170] "National Security Unit: Anti–Pension Reform Protests Had Intervention from Chinese Forces" ["國安單位：反年改陳抗 有中國勢力介入"], *Liberty Times*, July 18, 2017; "Taiwan Cuts 18 Pct Interest in Civil Service Pension Reform Bill," *Reuters*, June 27, 2017; "Taking on Taiwan's Ruinous and Partisan Pension System," *Economist*, May 18, 2017.
[171] Elsa B. Kania. "China's Strategic Support Force At 3." *The Diplomat*, (December 29, 2018). https://thediplomat.com/2018/12/chinas-strategic-support-force-at-3/.
[172] Shen Ming-shih, "China's Cyber Warfare Strategy and Approaches toward Taiwan," *Taiwan Strategists*, no. 2 (June 2019): 1–18. https://www.pf.org.tw/article-pfch-2122-6510.



DOI:10.6814/NCCU202000853

Network Systems Department.[173] Li Tiantian (李天天) is cited as deputy commander of a PLASFF "Third department." Li previously served as deputy director of the GSD Intelligence Department, and was dual hatted as director of the Ministry of National Defense Peacekeeping Office.

In that same report by the Project 2049 Institute, based on the limited information available, the PLASSF "appears intended to integrate the launch, tracking, and control of satellites with the operational units that apply the service that the satellites provide, such as command, control, communications, computers, intelligence, surveillance, and reconnaissance."[174] The PLASSF may also integrate national-level technical reconnaissance assets including the use of cyber with leaders and support administrative staff in order to facilitate "cross-domain fusion" of space and network operations.[175] An example of "cross-domain fusion," is the enhancing China's ability to monitor North Korean missile activites through the combination of technical reconnaissance, space tracking, and space-based reconnaissance.[176] To reiterate, the development of the PLASSF is an example of the PLA horizontally and vertically developing its capabilities in every domain. The PLASSF will be a significant component and indicator of the broader PLA reform and progress towards fulfilling its objective of becoming a "world-class military."[177]

The Network Systems Department also oversees the PLASSF Information Engineering University, a corps leader-grade organization. The following is a list of 2nd level departments provided by the Project 2049 Institute that they may oversee. This list helps paint a picture of

[173] The 3PLA was coined as "China's Version of the NSA" in a headline by the Wall Street Journal, See James T. Areddy. "Meet 3PLA, China's Version of the NSA." *The Wall Street Journal*, (July 9, 2014). https://blogs.wsj.com/chinarealtime/2014/07/08/meet-3pla-chinas-version-of-the-nsa/.; Rachael Burton, "Project 2049 Institute," Project 2049 Institute, September 25, 2018. https://project2049.net/2018/09/25/the-peoples-liberation-army-strategic-support-force-leadership-and-structure/.

[174] Rachael Burton, "Project 2049 Institute," *Project 2049 Institute*, (September 25, 2018). https://project2049.net/2018/09/25/the-peoples-liberation-army-strategic-support-force-leadership-and-structure/.

[175] Ibid.

[176] Ibid.

[177] Ibid.; Elsa B. Kania. "China's Strategic Support Force At 3." *The Diplomat*, (December 29, 2018). https://thediplomat.com/2018/12/chinas-strategic-support-force-at-3/.



DOI:10.6814/NCCU202000853

what skills and education the Network Systems Department are emphasizing in order to build a successful force.

- Political Department (**政治部**)
- S&T Research Department (**科研部**)
- Training Department (训练部)
- Command Information Systems Academy (**指**挥信息系统学院)
- Electronic Technology Academy (电子技术学院)
- Encryption Engineering Academy (**密**码工程学院)
- Luoyang Foreign Language Academy (**洛阳外国**语学院)
- Geospatial Information Academy (**地理空**间信息学院)
- Cyberspace Security Academy (**网**络空间安全学院)
- Navigation and Aerospace Target Engineering Academy (导航与空天目标工程学院)
- Command Officer Basic Education Academy (**指**挥军官基础教育学院)
- Blockchain Academy (**区**块链研究院; located in Shenzhen)
- National Digital Switching Engineering Research Center (**国家数字交**换系统工程研究 **中心** / **国家数字交**换系统工程技术研究中心)
- National Key Laboratory of Mathematical Engineering and Advanced Computing (**数学 工程与先**进计算国家重点实验室)
- Information Technology Research Institute (**信息技**术研究所)
- Fuzhou Sub-Academy (**福州分院**)
- Changshu Sub-Academy (**常熟分院**)
- Songshan Training Base (**嵩山**训练基地).



DOI:10.6814/NCCU202000853

Again much of the information regarding the PLASSF and its organization, structure, and capabilities is very limited. Majority of information is dated to 2018, meaning that more sophisticated cyber capabilities have been or are already being developed. This is a section of the PLA that requires much further research and study.

***PLA Unit 61398***

According to multiple news sources, PLA Unit 61398, otherwise known as APT-1, based out of Shanghai, is thought to be the source of many alleged Chinese computer hacking attacks. Mandiant report asserts that; APT-1 might be the 2nd Bureau of the PLA General Staff Department's 3rd Department ((总参三部二局), otherwise known as Unit 61398.[178] The group is believed to recruit young university students, with one Zhejiang University site reading: "The graduate school has received notice that Unit 61398 of China's People's Liberation Army seeks to recruit 2003-class computer science graduate students. Students who sign the service contract will receive a 5,000 yuan per year national defence scholarship. After graduation, the students will work in the same field within the PLA."[179] The following are key findings from the report that describe the capabilities of PLA Unit 61398:[180]

- The nature of "Unit 61398's" work is considered by China to be a state secret; however, we believe it engages in harmful "Computer Network Operations."
- Unit 61398 requires its personnel to be trained in computer security and computer network operations and also requires its personnel to be proficient in the English language.

[178] Mandiant, "APT1 - Exposing One of China's Cyber Espionage Units," *Fireeye*, February 18, 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.
[179] Stephen Thompson, "Spotlight on China's Hackers after Accusation against PLA Unit 61398," *South China Morning Post*. Accessed April 21, 2013. https://www.scmp.com/lifestyle/technology/article/1219328/spotlight-chinas-hackers-after-accusations-against-pla-unit.
[180] Mandiant, "APT1 - Exposing One of China's Cyber Espionage Units." *Fireeye*, (February 18, 2013). https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.



DOI:10.6814/NCCU202000853

- APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously
- APT1 focuses on compromising organizations across a broad range of industries in English-speaking countries
- APT1 maintains an extensive infrastructure of computer systems around the world
- The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators

In November of 2014, the United States charged five Chinese military officers with hacking into American nuclear, metal, and solar companies to steal trade secrets, and increasing tensions between the two states over the issue of cyber espionage.[181] Beijing was quick to deny these accusations, with its Foreign Ministry arguing that the U.S. grand jury indictment was "made up." According to the indictment, Chinese state-owned companies "hired" PLA Unit 61398 to provide information technology services, "including assembling a database of corporate intelligence."[182] Since 2006, cyber-attacks on Western defense contractors have been found to be the result of another cyber warfare unit: PLA Unit 61486.[183] Both units are suggested to share information and cooperate closely with the School of Information Security Engineering, Shanghai Jiao Tong University even providing technological support to PLA Unit 61486.[184]

**China's Strategic Objective: Taiwan's Pillars of Societal Stability**

As previously stated by Kallberg, "If nation states seek to conduct decisive cyberwar, it will not be achieved by anecdotal exploits, but instead by launching a systematic destabilizing

[181] Jim Finkle, Joseph Menn, and Aruna Viswanatha, "U.S. Accuses China of Cyber Spying on American Companies," *Reuters*, (November 21, 2014). https://www.reuters.com/article/us-cybercrime-usa-china-idUSKCN0J42M520141120.
[182] Ibid.
[183] Shen Ming-shih, "China's Cyber Warfare Strategy and Approaches toward Taiwan." *Taiwan Strategists*, no. 2 (June 2019): 1–18. https://www.pf.org.tw/article-pfch-2122-6510.
[184] Ibid.



DOI:10.6814/NCCU202000853

attack on the targeted society."[185] There is clear evidence in Taiwan that China is currently conducting cyber activities in order to destabilize Taiwan's society. Of Waldo's pillars for societal stability mentioned by Kallberg, legitimacy and confidence, are the most vulnerable to Chinese cyber warfare. Chinese efforts to spread disinformation and fake news are aimed at undermining the states legitimacy. To restate, Waldo believed in the Lockesian theory that citizens must have faith in their government and that it should promise to deliver a better life for its citizens. The spread of disinformation harms the credibility and legitimacy of elected officials and the offices they occupy. Public opinion matters significantly in a robust democracy like that of Taiwan, which boasted a 74.9% turnout during 2020 Presidential Elections.[186] A cyberattack seeking to damage state legitimacy could attempt to create an assumption that state leadership is incompetent and unable to govern its country. Regarding Confidence, Waldo believed that when people feel secure, they have confidence and are optimistic about the future; therefore, they trust their government and will provide the necessary support. In this scenario, confidence is trust in the government to deliver to the society what was promised. Chinese social media activity is just one dimension of its political warfare campaign to undermine the confidence of Taiwanese citizens. A large portion of Chinese propaganda is aimed at weakening Taiwanese morale and promoting the narrative that conflict is inevitable. China has also had a history of luring Taiwanese companies and investors to the mainland in the name of cross-straits economic integration. As a result, many Taiwanese scholars have researched the phenomena of the hollowing-out of Taiwan's economy. Additionally, military propaganda, and frequently military exercises at the islands doorstep creates an immense atmosphere of tension among Taiwanese citizens. It is difficult to quantitatively assess how much of an impact rumors and misinformation like this has on public opinion, legitimacy, and confidence in a state like Taiwan; further research and theoretical development is required to determine the impact of misinformation on democratic legitimacy.

[185] Jan Kallberg, "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review* 1, no. 1 (2016): 113-28. www.jstor.org/stable/26267302.

[186] Dominique Reichenbach, "Taiwan's Electoral System Puts the US to Shame," *The Diplomat*, February 13, 2020. https://thediplomat.com/2020/02/taiwans-electoral-system-puts-the-us-to-shame/.



DOI:10.6814/NCCU202000853

## Effectiveness of China's Strategy

Measuring the effectiveness of China's political warfare strategy against Taiwan is extremely difficult to measure given the lack of information of some areas and the potential inaccuracy of others. It is difficult; if not impossible to find measurable evidence of the effect of public opinion warfare on foreign audiences.[187] It is likewise difficult to assess what impact China's social media activities have influencing foreign public opinion, but it is clear the Chinese government views it as an important vector for such influence. One clear aspect of China's information operations is its penetration and presence on Western social media platforms, many of which are used in Taiwan by citizens and government officials alike.[188] Since joining Twitter and Facebook in 2011 and 2013, respectively, *People's Daily* has accumulated 4.4 million and 41 million followers, respectively.[189] In 2018, Taiwan was the biggest user of mobile data in Asia, and only second in the World with Taiwanese mobile users consuming twice as much data as South Koreans and; almost six times as much as Singaporeans.[190] Again, it is difficult to gauge accurately how much the Chinese government is spending on propaganda in foreign countries. The RAND Corporation cites one U.S. scholar who estimated China spends nearly $10 billion USD per year.[191] Additionally, individuals connected to the Chinese government have also spent millions buying foreign media, including $260 million USD for the *South China Morning Post*.[192] The RAND corporation states that:

> China's 'advertising' spending on Western social media is equally opaque, but recent *New York Times* reports confirm that the Chinese government does pay to deliver its propaganda to foreign audiences. According to one report, China "spends

[187] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*. (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.
[188] Ibid.
[189] Ibid.
[190] Scott Morgan. "Taiwan Biggest User of Mobile Data in Asia, s..." *Taiwan News*, (July 23, 2018). https://www.taiwannews.com.tw/en/news/3488375.
[191] Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*. (Santa Monica, CA: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2713.html.
[192] Ibid.



DOI:10.6814/NCCU202000853

> hundreds of thousands of dollars" on Facebook advertising alone to promote its content on the network. According to another, "an editor at China's state-run news agency, Xinhua, paid [a company] for hundreds of thousands of followers and retweets on Twitter," with the intent of helping Xinhua expand its reach on the social media platform. This lines up with earlier reporting that Xinhua's Twitter followers were growing at an unnatural rate and suggests that other Chinese propaganda organizations may also be buying followers and influence on Western social media. Clearly, the Chinese government is willing to exploit U.S. social media companies for its propaganda purposes, many of which are widely used in countries across Asia.[193]

China is clearly invested in the effort to disseminate propaganda and misinformation across foreign media platforms in order to influence public opinion. The effectiveness of these tactics on influencing public opinion and state legitimacy is worth further research. As previously mentioned, political warfare campaigns have the potential to undermine and damage the legitimacy of democracies, but to what extent requires further study. A case study on the effectiveness of China's cyber warfare strategy on Taiwan should be undertaken in the near future.

[193] Ibid.



DOI:10.6814/NCCU202000853

## Chapter 4 – Taiwan's Counter Strategies

Taiwan has much to lose at the hands of China's coordinated political warfare campaign against it. Beijing and Taipei pose an existential threat to one another, as many observers and officials on either side of this issue see it as a zero-sum game. Taiwan's democracy is a stark antithesis to China's authoritarian system and its presence right at China's doorstep makes it impossible for the CCP to ignore. China is determined to undermine the legitimacy of Taiwan's democracy in hopes of destabilizing its society so that it becomes vulnerable. In recent years, China has expanded its judicial reach beyond its borders by targeting and prosecuting Chinese citizens and foreigners in order to mute criticisms of China and the CCP. According to the RAND Corporation:

> One of the most prominent examples of this type of operation is the arrest of Taiwan national Lee Ming-che and his prosecution inside China for purportedly discussing support for China's democratization on Chinese social media platforms. His posts were seen as endangering state security. During his trial, prosecutors also referenced discussions held by others on Facebook outside of China and treated these as evidence of crimes that could be prosecuted inside China, should the individual in question come into Chinese government officers' hands.[194]

According to the Center for a New American Security, "for the last decade, Taiwanese internet security specialists have observed a recurring pattern: innovative, highly targeted data theft attacks appear in both government and industry systems in Taiwan…"[195] Taiwan is also an ideal and logical target for Beijing to target for a number of reasons. The island is in extremely close proximity to the mainland while sharing much of the same language and historical culture. Additionally, hackers can operate within the same time zone; and have nearly instantaneous

[194] Ibid.

[195] Robert E. Kahn, Mike McConnell, Joseph S. Nye, Peter Schwartz, Nova J. Daly, Nathaniel Fick, Martha Finnemore, Richard Fontaine, Daniel E. Geer, David A. Gross, Jason Healey, James A. Lewis, M. Ethan Lucarelli, Thomas G. Mahnken, Gary McGraw, Roger H. Miksad, Gregory J. Rattray, Will Rogers, and Christopher M. Schroeder. *America's Cyber Future: Security and Prosperity in the Information Age*. Report. Edited by Lord Kristin M. and Sharp Travis. Center for a New American Security, 2011. 20-31. Accessed March 26, 2020. www.jstor.org/stable/resrep06319.7.



DOI:10.6814/NCCU202000853

feedback, allowing them to hone their hacking skills and transfer it to foreign environments.[196] To provide context to the scenario that Taiwan is in, the Center for a New American Security states:

> Given the complexity of Taiwan's political status and the tense relationship between it and the mainland, the cyber threat from Beijing is a huge concern in Taipei. Officials worry that China could use cyberwarfare tactics on defense platforms or to influence political or defense decision-making. Moreover, Taipei worries that in a crisis scenario, China could attack its infrastructure or inhibit the military's communication ability. The government has stated that Taiwan is attacked more often than the United States and Hong Kong, and it believes that "Chinese hackers have infiltrated Taiwan's defense, foreign affairs, air traffic control and communication systems, saying that the scale has reached 'quasi-war level.'"[197]

## Notable Cyber-Attacks on Taiwan

### *DDP Website Hacks*

On two occasions the Democratic Progressive Party's website was hacked supposedly by Chinese-sponsored groups. In December 2015, local news organizations were hacked by APT-16 utilizing an email phishing scheme in order to infiltrate staff emails and send emails posing as other party members.[198] In June of 2016, the DDP website was hacked again and replaced with a spoof site that was used to collect user data. A study by the Center for New American Security, noted that these attacks were aimed "against Taiwanese political targets [and] suggests the actors behind the present campaign are supported by mainland Chinese sponsors."[199]

[196] Ibid.
[197] Ibid.
[198] Ibid.
[199] Ibid.



DOI:10.6814/NCCU202000853

***First Commercial Bank ATM Heist***

In July 2016, a group of cyber criminals from Europe and Russia utilized malware against the First Commercial Bank of Taiwan to hack 41 ATMs, stealing over $2 million USD in cash.[200] Nearly a week after the incident occurred, three bagmen were apprehended by the police in Taiwan and through multiple sources of information and confessions by the suspects, $2.4 million USD was recovered. This case was an example of collaboration by Taiwan with multiple outside resources, that led to the swift arrest and prosecution of these cyber-criminals.

## What is Taiwan Currently Doing?

In May 2015, DPP defense analysts proposed the creation of a cyber army as a fourth branch of its armed service, estimating that it would employ 6,000 personnel and have a budget of $30.7 million USD.[201] To follow this up, in August of 2016, the Tsai administration established a new government agency known as the Department of Cyber Security, within the Ministry of Science and Technology whose mission is to "oversee the implementation of information security policies, legal measures and operation standards."[202] On June 6, 2018, the Office of the President announced the Cybersecurity Management Act, the first piece of cybersecurity legislation in Taiwan which went into effect on January 1, 2019. According to the act, "cybersecurity" is now an issue of "national security" and that it will shape the future of Taiwan's cybersecurity landscape for years to come. The act lays the framework in order for Taiwan to better define and classify terms and incidents regarding cyber, along with providing guidelines to improve infrastructure and to allocate funding for these programs. Additionally, it promotes the research of cybersecurity by designated the government to provide resources to cultivate a task force of cybersecurity professionals and how to develop an effective cyber defense in Taiwan.

[200] Ibid.
[201] Ibid. Jason Pan, "Taiwan to Go Ahead with Cyberarmy Plan: Ministry," Taipei Times, May 27, 2016, http://www.taipeitimes.com/News/taiwan/archives/2016/05/27/2003647240.
[202] Ibid.



DOI:10.6814/NCCU202000853

***National Center for Cyber Security Technology (行政院国家資通安全会報技術服務中心)***

In order to promote a national cybersecurity policy, the Executive Yuan incorporated a plan to develop critical information and communication infrastructure security and initiated phase one of that plan back in 2001. As a result, the National Information and Communication Security Task force (NICST) along with the National Center for Cyber Security Technology (NCCST) in March 2001 in order to assisted the NICST with the cybersecurity defense of government agencies. The NCCST is currently in the fifth phase of its cybersecurity program which went into effect in 2017. The goals of this phase is to develop a "national cyber security joint-defense system, increase the cyber security self-development energy, and nurture cyber security talents."[203] The NCCST has listed the core missions of the fifth phase of its cyber program:

1. Research cyber security regulations, standards, guidance, and analyze cybersecurity threat trends in order to grasp current cyber security risks and to develop proper defense mechanisms
2. Develop a government cyber security governance model by establishing big data analysis capabilities and strengthening cybersecurity joint-defense monitoring of government agencies
3. Planning and promoting overall cyber security protection from government agencies and establishing a comprehensive cyber defense mechanism
4. Promoting a national-level joint-defense system and establishing cybersecurity information sharing mechanisms
5. Assisting government agencies in dealing with cybersecurity issues and strengthening emergency response and recovery capabilities by holding cybersecurity exercises and audits and promoting response and transparency
6. Promoting cybersecurity protection of critical infrastructure
7. Plan a government cybersecurity development blueprint; execute training assessments; and continue to develop cybersecurity professionals to increase national cybersecurity awareness

[203] "About NCCST." About NCCST - National Center for Cyber Security Technology, n.d. https://www.nccst.nat.gov.tw/About?lang=en.



DOI:10.6814/NCCU202000853

8. Promote cybersecurity academic research and cooperation along with international cyber cooperation and information sharing

***Ministry of Justice Investigation Bureau (法務部調)***

The Investigation Bureau of the Ministry of Justice is a criminal-investigation and counter-intelligence agency which reports directly to the Ministry of Justice. The MJIB's Cyber Crime Prevention Division covers a wide portfolio of cyber related responsibilities relating to national security. This office's responsibilities include detecting and preventing cyber-crimes, establishing information systems support and education, devising strategies in order to prevent cyber-crimes, collecting information on threats related to cyber security (providing support to government agencies and private companies), and enhancing cybercrime investigation capabilities.[204] At the time of writing, the MJIB appears to be the only Taiwanese government organization that publically specializes in combating cyber-attacks and the spread of fake news in the country. The existence of other efforts and organizations are likely classified or not widely known through public knowledge and research as the widespread dissemination of this type of information would harm Taiwan's cyber defense capabilities and expose points of vulnerability to foreign adversaries.

According to one briefing by the MJIB, Taiwan has detected a growing number of cases of disinformation related to COVID-19 since late February 2020, more than 70% of which originated from China.[205] MJIB official Chang Yu-Jen stated that the rise in disinformation is likely because of Chinese netizens who are unhappy with Taiwanese criticism of how China has managed their COVID-19 outbreak.[206] According to Chang, one method of spreading misinformation is the use of a template in which key-words can be swapped out and reposted

[204] "Cyber Crime Prevention." *法務部調查局*, Ministry of Justice Investigation Bureau, 11 July 2016, www.mjib.gov.tw/EditPage/?PageID=cccf1206-a941-466d-84c0-5b505a3c4acb.
[205] Zhong-han, Miao, Yen-hsi Lai, and Yi-ching Chiang. "70 Percent of Fake COVID-19 News from China: Investigation Bureau." Focus Taiwan. Focus Taiwan - CNA English News, April 8, 2020. https://focustaiwan.tw/cross-strait/202004080010.
[206] Ibid.



DOI:10.6814/NCCU202000853

over and over again across multiple accounts.[207] Other forms of fake news and misinformation include photo shopped images of Taiwanese new channels as well as fake government announcements and statements.[208]

### *Information Security Workstation of the Bureau of Investigation of the Ministry of Justice*

On April 24, 2020, the Ministry of Justice unveiled the new Information Security Workstation of the MIJB. President Tsai attended the unveiling ceremony, first expressing that the inauguration of the office was an important part of the implementation of China's ICT (Information and communications technology) security strategy and to strengthen Taiwan's democratic defense mechanisms.[209] The inauguration of this office came at time during the COVID19 global pandemic when a reportedly large number of fake messages have been circulating online.[210] The accompanying press release expressed that the spread of misinformation has caused a great amount of interference in national defense epidemic operations and that in order to defend against information warfare, the government must go all out.[211] In 2019, the Bureau of Investigation established a fake information prevention center, cracking down on the source of misinformation and fake news. President Tsai highly praised the Bureau's integration of "professional and dedicated" security investigation teams who are tasked with the investigation of cybercrimes in accordance with the law.[212] She also encouraged all government colleagues in security and national security agencies to invest in security, hoping to maintain administrative neutrality in the future, and improve democratic defense mechanisms in order to safeguard [Taiwan's] democracy.[213]

[207] Ibid.
[208] Ibid.
[209] Ministry of Justice Investigation Bureau "The Information Security Workstation of the Bureau of Investigation of the Ministry of Justice Was Officially Unveiled." *法務部調查局*, Ministry of Justice Investigation Bureau, 24 Apr. 2020, www.mjib.gov.tw/news/Details/1/600.
[210] Ibid.
[211] Ibid.
[212] Ibid.
[213] Ibid.



DOI:10.6814/NCCU202000853

## What Can Taiwan Do?

Taiwan is already fully aware of the challenges ahead when facing a cyber threat as daunting as this one. Currently, various government officers support the idea that the Taiwanese government is already doing what it can with the resources that are currently provided.[214] A research report by the RAND Corporation provides some insight into how a state can develop effective measures to confront political warfare; in order to develop and sustain an effective strategy and approach to the threats that China possess, there is (1) a need for strategy, (2) the need for a whole-of-government approach to statecraft led by an appropriately [DoS] enabled head of government, and (3) the formulation and coordination of response with and through other sovereign governments, allies and partners. The following objectives are further explained below:

> **Need for Strategy** – The general requirement for a cost-effective approach to national defense suggests that early and effective nonmilitary responses – and nonlethal uses of the military element of national power – may provide the [Taiwan] with valuable tools to deter adversaries, prevent conflicts from escalating, or mitigate their effects.[215] In some cases, these approaches may effectively reduce or remove the incipient threats. Taiwan is already facing an ongoing cyber threat, but is seeing limited results as issues still persist. Revising current strategy may be required in order to further prevent conflicts from escalating.
>
> **Need for a Whole-of-Government Approach –** Taiwan greatest challenge in developing an effective defense against China's political warfare strategy and thus its coordinated cyber-attacks is its lack of a "Whole-of-Government Approach." As of writing, many key Taiwanese ministries lack the resources to defend against

[214] Anonymous source from Taiwan's National Security Council, Associate research fellow. Interview conducted on May 2, 2020.
[215] Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, The Growing Need to Focus on Modern Political Warfare. Santa Monica, CA: *RAND Corporation*, 2019. https://www.rand.org/pubs/research_briefs/RB10071.html.



DOI:10.6814/NCCU202000853

sophisticated network security attacks.[216] The NSB and MJIB appear to be sufficiently equipped to handle cyber and intelligence issues within their jurisdiction and are the organizations most likely to be equipped to lead a "Whole-of-Government Approach" given their experience and expertise in the field. Coordinated cyber-teams need to be integrated at all state-level organizations in order to develop and effective political warfare defense. The Ministry of Justice should advise the office of the President to administer a more comprehensive cybersecurity agenda.

**Coordinated with the Governments –** There must be coordination between the governments of those countries where the aggression, subversion, coercion, or destabilization is occurring, along with other partners or allies who are willing and able to contribute their resources and efforts in a common effort.[217] At this point in time, it would be difficult to recommend that Taiwan rely on its allies. As of writing, the United States and China are currently locked in an information war with one another on the narrative surrounding COVID-19. Additionally, the United States is dealing with pressing domestic issues as well as a national presidential election, while the CCP is moving forward with legislation to clamp down on protests in Hong Kong as well as strategic territorial moves. Sino-U.S. relations are at an all-time low since Kissinger's first visit to China and the U.S. is preoccupied with domestic turmoil, therefore it would be difficult for Taiwan to rely on its most powerful ally at this time.

Due to these concerns, Taiwan should focus on developing its cyber-defensive capabilities even further in order to combat the potential threat of future cyber-attacks from China's ongoing political warfare campaign. To that end, the Taiwanese government should strengthen reconnaissance capabilities and reinforce countermeasures to protect military facilities and key infrastructures (nuclear reactors, power grids), as well as command and control functions. New

[216] Anonymous source from Taiwan's National Security Council, Associate research fellow. Interview conducted on May 2, 2020.
[217] Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, The Growing Need to Focus on Modern Political Warfare. Santa Monica, CA: *RAND Corporation*, 2019.



DOI:10.6814/NCCU202000853

system installations must be equipped with capabilities to survive against electro-magnetic pulse attacks (EMPs) and secure an environment to prevent network security attacks like DDoS attacks. Building resilient systems with trained experts in the field of cyber security so that Taiwan can be more responsive and recover quicker in the event coordinated cyber-attacks do occur.[218]




[218] Shen, Ming-shih. "China's Cyber Warfare Strategy and Approaches toward Taiwan." *Taiwan Strategists*, no. 2 (June 2019): 1–18. https://www.pf.org.tw/article-pfch-2122-6510.



DOI:10.6814/NCCU202000853

## Conclusion

Cyber warfare remains a dynamic landscape in which many researchers and academics are still struggling to grasp the fundamental ideology behind it. Because of such quick advancements in technology in the last few decades, cyber warfare has developed at a rate in which the academic community has yet to come to a consensus regarding the definition of it. Traditional political warfare theory struggles to encompass all of the capabilities cyber possess and cyber is advantageous in ways that were not previously imaginable. In order to better understand cyber and cyber warfare, a consensus as to what are the norms that which govern cyber needs to be reached within the academic and international community in order to further the discussion. Only from there can we begin to understand the nature of cyber-attacks and the strategies surrounding coordinated cyber warfare campaigns. There is currently a large gap in the education of information technology in government organizations both in Taiwan and the United States. The rapidly advancing technological capabilities in the private sector leaves government agencies even further behind and ill-equipped to handle large-scale issues and attacks such as a coordinated cyber/political warfare campaign. Relying on dedicated government intuitions and task forces is a very narrow minded approach to dealing with cyber issues. Governments need to be able to quickly assess the information and identify the threat presented to them in a timely matter in order to combat the efficiency and quickness associated with cyber.

The CCP and PLA are currently capable of carrying out coordinated cyber-attacks in addition to dispersing widespread misinformation regarding their military and economic capabilities in order to sway the public opinion and morale of targets abroad. We can understand that reunification with Taiwan is inherently a political goal of the CCP in order to achieve the "Chinese Dream." The "Chinese Dream" and the protection of state sovereignty is allowing the CCP and PLA to opening interpret which methods are feasible to carry out this foreign policy mandate. To the Chinese, cyber warfare is simply an extension of political warfare, and helps facilitate the undermining of Taiwan's democratic regime. Taiwan has been facing a coordinated political warfare campaign at the hands of the CCP for decades and cyber-attacks are just another dimension to their overall plan. Because of the low risk-high reward factor associated with a coordinated cyber campaign, the CCP is funneling its resources into bolstering its offensive cyber capabilities with conducting research and development of more advance technologies that could potentially enhance their capabilities in the future (facial recognition, AI, 5G).



DOI:10.6814/NCCU202000853

There is substantial evidence that the CCP is engaged in coordinated political warfare campaign against Taiwan with the intent purpose of undermining its democratic legitimacy. The purpose of this political warfare campaign is the eventual objective of fulfilling the "Chinese Dream" by uniting Taiwan with the mainland. As it stands now, Taiwan is on the receiving end of overt and subvert tactics by Beijing ranging from military exercises, threats of war, diplomatic pressure to cyber-attacks, espionage, and economic tactics. The PLA have incorporated tactics of disseminating military propaganda in order to demoralize Taiwanese citizens and its government in order to create the atmosphere that conflict is inevitable and that Taiwan stands no chance against Beijing's military. As a result, Taiwan has been put in a precarious situation where it is fighting for breathing room to maintain international autonomy without having to rely on its strategic allies. The Taiwanese government has demonstrated an awareness of the coordinated cyber campaign against its social infrastructure and institutions. What it lacks is a coordinated effort from all bodies of government to combat the potential threat of cyber-attacks and the spread of misinformation and fake news in its social media networks. While there are currently efforts to bolster Taiwan's cyber defense capabilities, it is likely not enough at the current moment. Taiwanese government offices often times lack dedicated information technology teams working on their network security, let alone are those offices likely educated on the matter of cyber security. Additionally, due to the nature of the Taiwanese new cycle and the use of online social media, the spread of misinformation and fake news is still an ongoing issue. Though there have been successful attempts and operations to combat and identify the source of is misinformation, the effects it has on government institutions and democratic legitimacy needs to be further studied.

In the midst of the COVID-19 global pandemic, Taiwan has been facing a bombardment of misinformation regarding the virus and the government's handling of the pandemic. With the upcoming U.S. Presidential election, it would be extremely difficult for Taiwan to rely on its allies, and asking it to endure this harsh period at the hands of Beijing's political warfare campaign is a near death sentence. The recent climate political of Hong Kong does not reassure the international community that the CCP will not allow the same autonomy to Taiwan if it were to unite with the mainland. The COVID-19 global pandemic has thrusted Taiwan into a position of vulnerability where its forced to fend for itself, prevent outbreaks of infections, while at the same time maintaining the transparency of its democracy to reassure its citizens that it will not



DOI:10.6814/NCCU202000853

bow to the will of Beijing. What Taiwan needs to do at this point is a more holistic government approach of tackling cyber security with each government office likely having a dedicated cyber team. As it stands right now, Taiwan's current efforts to combat external cyber threats and misinformation is not enough, and its democracy faces structural harm if these issues were to persist; especially under the current COVID-19 global pandemic.





DOI:10.6814/NCCU202000853

## Bibliography


1. Areddy, James T. "Meet 3PLA, China's Version of the NSA." *The Wall Street Journal. Dow Jones & Company*, July 9, 2014. https://blogs.wsj.com/chinarealtime/2014/07/08/meet-3pla-chinas-version-of-the-nsa/
2. Burton, Rachael. "Project 2049 Institute." *Project 2049 Institute*, September 25, 2018. https://project2049.net/2018/09/25/the-peoples-liberation-army-strategic-support-force-leadership-and-structure/.
3. Cheng, Dean. "For the Chinese, Political Warfare Is War by Other Means." *The Heritage Foundation*, April 2, 2020. https://www.heritage.org/asia/commentary/the-chinese-political-warfare-war-other-means.
4. Cheng, Dean. "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response," *The Heritage Foundation*, No. 2745, November 26, 2012, http://www.heritage.org/research/reports/2012/11/winningwithout-fighting-chinese-public-opinion-warfare-and-the-need-for-a-robust-americanresponse.
5. Cordesman, Anthony H. & Steven Colley, "Chinese Strategy and Military Modernization in 2015: A Comparative Analysis," *Center for Strategic and International Studies* (October 10, 2015), 121.
6. Easton, Ian. *The Chinese Invasion Threat: Taiwan's Defense and American Strategy in Asia*. Manchester: Eastbridge Books, 2019.
7. Finkle, Jim, Joseph Menn, and Aruna Viswanatha. "U.S. Accuses China of Cyber Spying on American Companies." *Reuters*, November 21, 2014. https://www.reuters.com/article/us-cybercrime-usa-china-idUSKCN0J42M520141120.
8. Finkelstein, David M., "China's National Military Strategy," in *The People's Liberation Army in the Information Age* by James C. Mulvenon and Richard H. Yang, eds., (Santa Monica, CA: RAND Corporation, 1999), 103.
9. Glaser, Bonnie, and Matthew P. Funaiole. "China's Provocations Around Taiwan Aren't a Crisis." *Foreign Policy*, May 15, 2020. https://foreignpolicy.com/2020/05/15/chinas-provocations-around-taiwan-arent-a-crisis/.




DOI:10.6814/NCCU202000853

10. Iasiello, Emilio. "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities." *Journal of Strategic Security* 9, no. 2 (2016): 45-69. Accessed May 23, 2020. www.jstor.org/stable/26466776.

11. Jing Nanxiang, "Cyber Freedom and Cyber Self-Discipline," *Liberation Army Daily*, December 20, 2011, from "*Summary: JFJB on Cyber Freedom and Cyber Self-Discipline for PRC Netizens*," translated by OSC, CPP20111221088010.

12. Kahn, Robert E., Mike McConnell, Joseph S. Nye, Peter Schwartz, Nova J. Daly, Nathaniel Fick, Martha Finnemore, Richard Fontaine, Daniel E. Geer, David A. Gross, Jason Healey, James A. Lewis, M. Ethan Lucarelli, Thomas G. Mahnken, Gary McGraw, Roger H. Miksad, Gregory J. Rattray, Will Rogers, and Christopher M. Schroeder. *America's Cyber Future: Security and Prosperity in the Information Age*. Report. Edited by Lord Kristin M. and Sharp Travis. *Center for a New American Security*, 2011. 20-31. Accessed March 26, 2020. www.jstor.org/stable/resrep06319.7.

13. Kallberg, Jan. "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations." *The Cyber Defense Review* 1, no. 1 (2016): 113-28. Accessed March 20, 2020. www.jstor.org/stable/26267302.

14. Kolton, Michael. "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence." *The Cyber Defense Review* 2, no. 1 (2017): 119-54. Accessed May 22, 2020. www.jstor.org/stable/26267405.

15. Kania, Elsa B. "China's Strategic Support Force At 3." *The Diplomat*. December 29, 2018. https://thediplomat.com/2018/12/chinas-strategic-support-force-at-3/.

16. Krejsa, Harry, and Hannah Suh. *Report.* Center for a New American Security, 2017. Accessed March 26, 2020. www.jstor.org/stable/resrep06143.

17. Lindsay, Jon R. "Exaggerating the Chinese Cyber Threat." *Belfer Center For Science and International Affairs*, May 2015. https://www.belfercenter.org/sites/default/files/files/publication/linsday-china-cyber-pb-final.pdf.



DOI:10.6814/NCCU202000853

18. Lü Jinghua [吕晶华], “Gongtong goujian heping anquan kaifang hezuo de wangluo kongjian,” [共同构建和平安全开放 合作的网络空间] (Jointly building a peaceful and safe cyberspace through open cooperation) *PLA Daily*, October 18, 2016, http://www.81.cn/jfjbmap/content/2015-10/18/content_126334.htm.

19. Lu Hsin-hui, Hsieh Chia-chen, Yeh Tzu-kang and Elizabeth Hsu. “Authorities Deny Rumor of Ban on Incense, Ghost Money Burning,” *Central News Agency (Taiwan)*, July 21, 2017. https://focustaiwan.tw/politics/201707210016.

20. Lyu, Jinghua. “What Are China's Cyber Capabilities and Intentions?” *IPI Global Observatory*, March 22, 2019. https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/.

21. Mattis, Peter. “China's 'Three Warfares' in Perspective.” *War on the Rocks*, January 30, 2018. https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.

22. Mazarr, Michael J., Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*. Santa Monica, CA: *RAND Corporation*, 2019. https://www.rand.org/pubs/research_reports/RR2713.html.

23. Miao, Zhong-han, Yen-hsi Lai, and Yi-ching Chiang. “70 Percent of Fake COVID-19 News from China: Investigation Bureau.” Focus Taiwan. *Focus Taiwan - CNA English News*, April 8, 2020. https://focustaiwan.tw/cross-strait/202004080010.

24. Morgan, Scott. “Taiwan Biggest User of Mobile Data in Asia, s...” *Taiwan News*, July 23, 2018. https://www.taiwannews.com.tw/en/news/3488375.

25. Murong Xuecun, “The New Face of Chinese Propaganda,” *New York Times*, December 20, 2013.

https://www.nytimes.com/2013/12/21/opinion/sunday/murong-the-new-face-of-chinese-propaganda.html.



DOI:10.6814/NCCU202000853

26. Nestoras, Antonios. "Political Warfare: Competition in the Cyber Era." *Martens Centre For European Studies*, April 2019. https://www.martenscentre.eu/sites/default/files/publication-files/cyber-warfare-politics-era.pdf.

27. Swaine, Michael D. "Chinese Views on Cybersecurity in Foreign Relations." *The Carnegie Endowment for International Peace*, September 20, 2013.

28. Shi-Kupfer, Kristin. "Governance Through Information Control," China Monitor, No. 26, *Mercator Institute for China Studies*, January 19, 2016.

29. Sardarizadeh, Shayan, and Olga Robinson. "Coronavirus: US and China Trade Conspiracy Theories." *BBC News*. BBC, April 26, 2020. https://www.bbc.com/news/world-52224331.

30. Pan, Jason. "Taiwan to Go Ahead with Cyberarmy Plan: Ministry," *Taipei Times*, May 27, 2016, http://www.taipeitimes.com/News/taiwan/archives/2016/05/27/2003647240.

31. Paterson, Thomas & Hanley, Lauren. (2020). Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'. *Australian Journal of International Affairs*. 1-16. 10.1080/10357718.2020.1734772.

32. Reichenbach, Dominique. "Taiwan's Electoral System Puts the US to Shame." *The Diplomat*, February 13, 2020. https://thediplomat.com/2020/02/taiwans-electoral-system-puts-the-us-to-shame/.

33. Robinson, Linda, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, *The Growing Need to Focus on Modern Political Warfare.* (Santa Monica, CA: *RAND Corporation*, 2019). https://www.rand.org/pubs/research_briefs/RB10071.html.

34. Swaine, Michael D., "Xi Jinping's Address to the Central Conference on Work Relating to Foreign Affairs: Assessing and Advancing Major- Power Diplomacy with Chinese Characteristics," *China Leadership Monitor* 46 (March 19, 2015); David M. Finkelstein, "China's National Military Strategy," by James C. Mulvenon and Richard H. Yang, eds., in *The People's Liberation Army in the Information Age* (Santa Monica, CA: *RAND Corporation*, 1999), 103.



DOI:10.6814/NCCU202000853

35. Shen, Ming-shih. "China's Cyber Warfare Strategy and Approaches toward Taiwan." *Taiwan Strategists*, no. 2 (June 2019): 1–18. https://www.pf.org.tw/article-pfch-2122-6510.
36. Thompson, Stephen. "Spotlight on China's Hackers after Accusation against PLA Unit 61398." *South China Morning Post*. Accessed April 21, 2013. https://www.scmp.com/lifestyle/technology/article/1219328/spotlight-chinas-hackers-after-accusations-against-pla-unit.
37. Ye Zheng, "From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond," translated by Yang Fan in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (London: Oxford Scholarship Online, April 2015), 132, doi:10.1093/acprof:oso/9780190201265.001.0001.
38. Yin Pumin, "Mapping Out Success: New five-year blueprint lays down specific objectives for a prosperous China," *Beijing Review 45* (November 5, 2015), accessed January 10, 2016, http://www.bjreview.com.cn/Current_Issue/Editor_Choice/201511/t20151102_800041696.html.
39. "US Says Taiwan's Exclusion from WHO Caused Loss of Lives." Al Jazeera. *Al Jazeera News*, May 13, 2020. https://www.aljazeera.com/news/2020/05/taiwan-exclusion-caused-loss-lives-200513025007789.html.
40. "Taiwan's Taoists Protest Against Curbs on Incense and Firecrackers," BBC, *BBC News*, July 23, 2017. https://www.bbc.com/news/world-asia-40699113.
41. "APT1 - Exposing One of China's Cyber Espionage Units." *Fireeye*, February 18, 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.



DOI:10.6814/NCCU202000853

## Chinese Sources


42. “Cyber Crime Prevention.” *法務部調查局*, Ministry of Justice Investigation Bureau, 11 July 2016, www.mjib.gov.tw/EditPage/?PageID=cccf1206-a941-466d-84c0-5b505a3c4acb.
43. “The Information Security Workstation of the Bureau of Investigation of the Ministry of Justice Was Officially Unveiled.” *法務部調查局*, Ministry of Justice Investigation Bureau, 24 Apr. 2020, www.mjib.gov.tw/news/Details/1/600.
44. Huaxia, ed., “Highlights of Xi's Internet speech,” *Xinhua*, December 16, 2015, http://news. xinhuanet.com/english/2015-12/16/c_134923855.htm.
45. “National Security Unit: Anti–Pension Reform Protests Had Intervention from Chinese Forces” [“國安單位：反年改陳抗 有中國勢力介入”], *Liberty Times*, July 18, 2017; “Taiwan Cuts 18 Pct Interest in Civil Service Pension Reform Bill,” Reuters, June 27, 2017; “Taking on Taiwan’s Ruinous and Partisan Pension System,” Economist, May 18, 2017.






DOI:10.6814/NCCU202000853