Journal of Strategic Security

Volume 9
Number 2 *Summer 2016*

Article 4

# China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities

Emilio Iasiello
*Private Sector*, iasiello@aol.com

# China’s Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities

## Author Biography

Emilio Iasiello has more than 12 years' experience as a strategic cyber intelligence analyst, supporting U.S. government civilian and military intelligence organizations, as well as the private sector. He has delivered cyber threat presentations to domestic and international audiences and has published extensively in peer-reviewed journals.

## Abstract

China is engaged in longstanding cyber espionage against the U.S., as well as other nations, to collect sensitive public and private information in support of national objectives laid out in its 12$^{th}$ Five Year Plan. Foreign governments citing China’s malfeasance have rebuked these activities, a claim vehemently denied by Beijing. In response, China is leveraging the “Three Warfares” an integrated three-prong information warfare strategy to combat these accusations by leveraging Media, Legal, and Psychological components designed to influence the international community. While the United States has threatened the imposition of economic sanctions, Beijing has successfully parried consequential actions by arresting U.S.-identified hackers, thereby demonstrating its commitment toward preserving a stable and peaceful cyberspace. These interrelated “Three Warfares” disciplines have targeted the cognitive processes of the U.S. leadership, as well as the international public’s perception of China as a global threat, thereby having successfully forestalled the implementation of any effective punitive or economic deterrence strategy to include the imposition of cyber sanctions.

# Introduction

China has been allegedly engaged in a longstanding cyber espionage campaign against the United States, as well as other nations, soliciting negative reactions citing China's malfeasance. The negative press received from these activities is feeding into the perception that China's global 'rise' is predicated on surreptitious intellectual property theft to project it into great power status, and perhaps as a way to seek regional and global military balance with the United States. In order 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 designed to influence the international community, and the United States in particular, in order to forestall the development and implementation of any effective counter strategy. The result has been largely successful to date, enabling China to reach specific milestones set forth in its national development plans while escaping any serious punitive or economic repercussions from the international community, to include recent circumvention of U.S.-imposed cyber sanctions. This article will review Chinese cyber activity, international perceptions of the Chinese cyber threat, how "Three Warfares" apply to Chinese cyber operations, and then provide final conclusions.

## Chinese Cyber Activity

Former National Security Agency (NSA) Director and Commander of U.S. Cyber Command General Keith Alexander estimates the losses incurred by cyber espionage activities at approximately $338 billion, although admittedly not all the result of Chinese efforts.[1] Nevertheless, the intimation of this assessment is that China, identified as the most persistent cyber espionage actor,[2] is suspected of a good portion of this activity. Indeed, the breadth and scope of suspected Chinese sponsored and/or directed cyber espionage begs the question: Despite the tactical success of stealing a diverse spectrum of sensitive and proprietary information in the face of public protest, what is Beijing's strategic game plan?

---

[1] Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'," *Foreign Policy: The Cable*, July 9, 2012, available at: *http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/*.

[2] "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," Office of the National Counterintelligence Executive, October 2011, available at: *http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf*.

China has three primary national security objectives: Sustaining regime survival, defending national sovereignty and territorial integrity, and establishing China as both a regional and national power.[3] China views the United States with a cautious mix of skepticism, partnership, and competition. The Chinese believe that the United States is a revisionist power seeking to curtail China's political influence and harm China's interests.[4] One way to counter U.S. supremacy is for China to engage in cyber operations in an effort to extract information from "diplomatic, economic and defense industrial base sectors that support U.S. national defense programs."[5] In this context, cyber operations can be viewed as being more about trying to strengthen China's core and less about diminishing U.S. power. Focusing solely on the United States, suspected Chinese cyber espionage actors have targeted the following industries, among others, during the past two years:

[3] Colonel Jayson M. Spade, "Information as Power: China's Cyber Power and America's National Security," *U.S. Army War College*, May 2012, available at: *http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf;* *"Military and Security Developments Involving the People's Republic of China 2014," Office of the Secretary of Defense Annual Report to Congress, 2014, available at: http://www.defense.gov/pubs/2014_DoD_China_Report.pdf.*
U.S. Department of Defense, Quadrennial Defense Review 2014 (Washington, D.C.: OSD, 2014): V, available at:
http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.
[4] Andrew J. Nathan and Andrew Scobell, "How China Sees America," *Foreign Affairs,* September/October 2012, available at:
*http://www.foreignaffairs.com/articles/138009/andrew-j-nathan-and-andrew-scobell/how-china-sees-america*.
[5] "Military and Security Developments Involving the People's Republic of China 2014."



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

Space[6], Infrastructure[7], Energy[8], Nuclear Power[9], Technology Firms[10], Clean Energy[11], Biotechnology[12], and Healthcare.[13]

China's 12th Five Year Plan reflects overall goals and objectives of the government to promote economic industry growth. It is a critically important tool that maps out in five-year cycles the country's future progress via guidelines, policy frameworks, and targets for policy makers at all levels of government.[14] In the current Five Year Plan, which covers 2011-15, China identified seven priority industries to develop, areas in which the United States has typically been an innovator and leader. These "strategic emerging industries" are intended to become the backbone of China's economy in the decades ahead.[15] These industries are:

- New Energy (nuclear, wind, solar sower)
- Energy Conservation and Environmental Protection (energy reduction targets)
- Biotechnology (drugs and medical devices)

---

[6] John Walcott, "Chinese Espionage Campaign Targets U.S. Space Technology," *Bloomberg*, April 18, 2012, available at: *http://www.bloomberg.com/news/2012-04-18/chinese-espionage-campaign-targets-u-s-space-technology.html*.
[7] Tom Simmonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant," *Technology Review,* August 2, 2013, available at: *http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/*.
[8] Tom Simmonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant," *Technology Review,* August 2, 2013, available at: *http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/*.
[9] Jennifer Liberto, "New Chinese Hacker Group Targets Governments, Nuclear Facilities," *CNN Money,* June 4, 2013, available at: *http://money.cnn.com/2013/06/04/technology/security/cyber-hacker-group/index.html*.
[10] Stew Magnuson, "Stopping the Chinese Hacking Onslaught," *NDIA*, July 2012, available at: *http://www.nationaldefensemagazine.org/archive/2012/July/Pages/StoppingtheChineseHackingOnslaught.aspx*.
[11] Susan D. Hall, "Chinese Hackers Targeting the Healthcare Industry," FierceHealthIT, March 20, 2013, available at: *http://www.fiercehealthit.com/story/chinese-hackers-targeting-healthcare-industry/2013-03-20*.
[12] Nick Paul Taylor, "Chinese Trial Data Hackers Reportedly Active Again," *Fierce BioTechIT,* May 27, 2013, available at: *http://www.fiercebiotechit.com/story/chinese-trial-data-hackers-reportedly-active-again/2013-05-27*.
[13] Susan D. Hall, "Chinese Hackers Targeting the Healthcare Industry," FierceHealthIT, March 20, 2013, available at: *http://www.fiercehealthit.com/story/chinese-hackers-targeting-healthcare-industry/2013-03-20*.
[14] "China's 12th Five Year Plan," *APCO*, December 10, 2010, available at: *http://www.export.gov.il/UploadFiles/03_2012/Chinas12thFive-YearPlan.pdf*.
[15] Ibid.

- New Materials (rare earths and high-end semiconductors)
- New IT (broadband networks, Internet security infrastructure, network convergence)
- High-End Equipment Manufacturing (aerospace and telecom equipment)
- Clean Energy Vehicles[16]

It is easy to see that a correlation can be made between the types of industries that have been targeted in the United States in the last two years and the strategic emerging industries that China has highlighted for development. Moreover, China views cyber as an ideal tool to accomplish these objectives being an inexpensive facile technique to engage several potential intelligence targets at once. In February 2007, *China National Defense News* defined cyber warfare as the "use of network technology and methods to struggle for an information advantage in the fields of politics, economics, military affairs, and technology."[17] 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-vis reconnoitering a future battle space.

## The Perceived Chinese Cyber Threat

While some experts believe that the United States, along with China and Russia, are engaged in a cyber arms race,[18] China has yet to be suspected or implicated in an incident involving the destruction of information systems or the information resident on them. Many Chinese strategic military writings advocate the use of information warfare as a pre-emptive weapon prior to the onset of military engagements;[19] however, if China is behind the volume of cyber espionage activity attributed to it, during peacetime China prefers to leverage the benefit of computer intrusions as a means of information collection and commercial advantage, rather than one of deterrence.

---

[16] "China's 12th Five-Year Plan: Overview," *KPMG China*, March 2011, available at: *http://www.kpmg.com/cn/en/IssuesAndInsights/ArticlesPublications/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf*.
[17] Robyn E. Ferguson, "Information Warfare with Chinese Characteristics: China's Future View of Information Warfare and Strategic Culture," (Dissertation), 15.
[18] Robert Windrem, "Expert: U.S. In Cyber Arms Race With China, Russia," *NBC News Investigations*, February 20, 2013, available at: *http://investigations.nbcnews.com/_news/2013/02/20/17022378-expert-us-in-cyberwar-arms-race-with-china-russia*.
[19] James Mulvenon, "The People's Liberation Army in the Information Age," (Santa Monica: RAND, 1999), 183.



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

Currently, several countries including Australia, Canada, Germany, India, Taiwan, and the United Kingdom, among others, have publicly accused China of intruding into their public and private sector networks.[20] In particular, the United States has been the prime target of suspected Chinese orchestrated or directed cyber operations for approximately a dozen years. While the U.S. government maintained a reserved stance for most of this time, in 2012 it became more outspoken with regard to the volume of cyber espionage activity targeting its public and private sectors. In October 2011, U.S. Congressman Mike Rogers of the House Permanent Select Committee on Intelligence publicly accused China of stealing sensitive information:

> "China's economic espionage has reached an intolerable level and I believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy."[21]

In 2013, the security company Mandiant published a detailed report identifying a Chinese military unit involved in cyber espionage.[22] Never before had technical evidence and analysis linking activities to a government entity been made public. The Mandiant report proved to be a watershed moment for senior U.S. government officials with several of them, including President Obama, publicly addressing the issue of Chinese cyber espionage. Shortly after publication of the Mandiant report, in March 2013, U.S National Security Advisor Thomas Donilon stated:

> "…businesses are speaking out about their serious concerns about sophisticated targeted theft of confidential business information and proprietary information through cyber intrusions emanating from China."[23]

---

[20] Timothy L. Thomas, "Google Confronts China's Three Warfares," *Parameters* 40:2 (Summer 2010), available at: *http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2010summer/Thomas.pdf*.

[21] "Lawmaker: China Engaging in Cyber Spying," *Fox News,* October 4, 2011, available at: *http://www.foxbusiness.com/technology/2011/10/04/lawmaker-china-engaging-in-cyber-spying/*.

[22] "APT 1: Exposing one of China's Espionage Units," *Mandiant*, available at: *http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf*.

[23] Tom Donilon, "The United States and the Asia-Pacific in 2013," *The Asia Society*, March 11, 2013, available at: *http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a*.

In that same month, President Obama engaged directly with Chinese President Xi Jinping about cyber security and future engagement possibilities,[24] which was followed by a summit in June, where the two leaders more fully discussed cyber security, with Obama opting not to directly accuse the Chinese leader of espionage activity.[25] However, any headway was derailed in May 2014 when the U.S. Department of Justice indicted five Chinese military officers with committing cyber espionage, the first time ever the U.S. government publicly accused members of a foreign government with crimes against U.S. companies.[26] Further reports of another suspected Chinese espionage group like 'Axiom',[27] reputed to be more sophisticated than the one profiled in the Mandiant report, further paints a condemning picture of China as a relentless cyber thief of sensitive information. Given the voluminous cyber incidents pointing toward some level of Chinese government affiliation, Beijing finds itself trying to sustain its 'peaceful rise' image in the midst of growing global public dissent, led at the spear tip by the United States and its threat of imposing cyber sanctions against those entities that benefited from commercial espionage activities.

## Three Warfares – A Primer

It seems counterproductive for a country so concerned with 'face' to engage in such blatant and aggressive activities that threaten to harm its global image. Two important concepts in Chinese culture are *guanxi* and *mianzi*. The first, *guanxi*, has been defined as sharing favors between individuals, connections, relationships, and the ability to exert influence. The second, *mianzi*, means 'face,' as in saving face, losing face, and giving face.[28] So why would a country steeped in this mindset willingly risk its image, especially at a time when the country is seen as a peacefully rising world economic power?

---

[24] Steve Howard, "Obama, China's Xi Discuss Cybersecurity Dispute on Phone Call," *Reuters*, March 14, 2013, available at: *http://www.reuters.com/article/2013/03/14/us-usa-china-obama-call-idUSBRE92D11G20130314*.
[25] M. Alex Johnson and Matthew DeLuca, "Obama Takes Diplomatic Tack on Chinese Cyberespionage Charges," *NBC News*, June 7, 2013, available at: *http://usnews.nbcnews.com/_news/2013/06/07/18804533-obama-takes-diplomatic-tack-on-chinese-cyberespionage-charges*.
[26] Devlin Barrett and Siobhan Gorman, "U.S. Charges Five in Chinese Military of Hacking," *The Wall Street Journal,* May 19, 2014, available at: *http://www.wsj.com/articles/SB10001424052702304422704579571604060696532*.
[27] Adam Segal, "Axiom and the Deepening Divide in U.S.-China Relations," *Council on Foreign Relations Blog,* October 29, 2014, available at: *http://blogs.cfr.org/cyber/2014/10/29/axiom-and-the-deepening-divide-in-u-s-china-cyber-relations/*.
[28] "China," Cultural Savvy, available at: *http://www.culturalsavvy.com/china.htm*.



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

The implementation of non-kinetic, non-violent, but still offensive operations is best suited for Chinese peacetime strategy of influencing the cognitive processes of a country's leadership and population, or what Sun Tzu describes as 'subduing the enemy without fighting.'[29] In 2003, the Communist Chinese Party Central Committee and the Central Military Commission approved the concept of 'Three Warfares,' a People's Liberation Army non-military information warfare tool to be used in the run up to and during hostilities.[30] Collectively, the 'Three Warfares' allow China to enter any fray, whether in peace or war, with a political advantage that can be used to alter public or international opinion.[31] They are:

- *Psychological Warfare*–Undermines an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralizing the enemy military personnel and supporting civilian populations. [32]

- *Public Opinion/Media Warfare*–Influences domestic and international public opinion to build support for China's military actions and dissuade an adversary from pursuing actions contrary to China's interests. [33]

- *Legal Warfare*–Uses international and domestic law to claim the legal high ground or assert Chinese interests. It can be employed to hamstring an adversary's operational freedom and shape the operational space. Legal warfare is also intended to build international support and manage possible political repercussions of China's military actions. [34]

Media warfare incorporates the mechanism for messages to be delivered, while legal warfare provides the justification of why actions are permissible. Psychological warfare provides the necessary nuance leveraging the dissemination capability of the media and the more formalized legal mechanisms to substantiate its activities to domestic and international

[29] Sun Tzu, *The Art of War,* available at: *http://www.theartofwar.ws/The_Art_of_War.pdf*.
[30] "Military and Security Developments Involving the People's Republic of China 2011," Office of the Secretary of Defense Annual Report to Congress, 2011: 26, available at: *http://www.defense.gov/pubs/pdfs/2011_CMPR_Final.pdf*.
[31] Timothy L. Thomas, "Google Confronts China's Three Warfares."
[32] "Military and Security Developments Involving the People's Republic of China 2011," 26.
[33] Ibid.
[34] Ibid.

audiences. Given that each of these types of warfare rely on the targeting and influencing of a specific target audience, it is easy to see why Chinese analyses almost always link these three types of 'combat' together.[35]

## Public Opinion/Media Warfare

Public opinion warfare refers to the use of various information channels, including the Internet, television, radio, newspapers, movies, and other forms of media in accordance with an overall plan and defined objectives to transmit selected news and other materials to an intended audience.[36] The goals are to preserve friendly morale, generate public support at home and abroad, weaken the enemy's will to fight, and alter the enemy's situational assessment. Defensive public opinion warfare is leveraged against adversarial public opinion warfare to neutralize possible effects on the Chinese populace.[37] Given the voluminous hacking allegations levied against China, defensive public opinion warfare is a natural counterbalance.

According to Cheng, four themes are inherent in Chinese writings on public opinion[38]:

- *Follow Top-Down Guidance*–The senior leadership will dictate courses of action based on strategic objectives.

- *Emphasize Preemption*–Chinese analyses of public opinion warfare emphasize that "the first to sound grabs people, the first to enter establishes dominance (*xian sheng duoren, 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.,

[35] Dean Cheng, "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response," *The Heritage Foundation*, No. 2745, November 26, 2012, available at: *http://www.heritage.org/research/reports/2012/11/winning-without-fighting-chinese-public-opinion-warfare-and-the-need-for-a-robust-american-response*.
[36] Ibid.
[37] Ibid.
[38] Ibid.



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

are seen as an invaluable resource in getting China's message before domestic and global audiences.

Public criticism over Beijing-sponsored intrusions surfaced as early as 2005 when it was revealed that suspected Chinese government intrusions dubbed 'Titan Rain' had been targeting U.S. public and private sectors entities since 2003.[39] Since that time, numerous foreign governments have gradually come out publicly to identify the Chinese government, or its operatives, as perpetrators of intrusion activity against their networks.[40] Furthermore, U.S. government entities have long suspected Chinese telecommunications companies Huawei and ZTE as being instruments of the state, and possible mediums that can be leveraged by the Chinese government for intelligence collection.[41] Such debate has risen to the highest levels as seen in 2013 meetings between Chinese president Xi Jinping and U.S. President Barack Obama.[42] In 2014, Secretary of Defense Charles Hagel disclosed U.S. cyber force structure and capabilities to China in an effort to demonstrate military transparency.[43]

### *Chinese Public Opinion / Media Warfare Applications to Cyberspace*

Chinese response has evolved during this period in which it has been framed as an antagonistic cyber presence. Typically, China has met such accusations with a defensive posture, denying allegations and asking for more information in an attempt to help track down the perpetrators. Indeed, senior official

---

[39] Nathan Thornburg, "The Invasion of the Chinese Cyberspies," *Time*, August 29, 2005, available at: *http://content.time.com/time/magazine/article/0,9171,1098961-1,00.html*.
[40] Jason Koutsoukis, "Chinese Waging Online Spy War;" *The Age*, February 10, 2008, available at: *http://www.theage.com.au/news/national/chinese-waging-online-spy-war/2008/02/09/1202234232007.html*; Roger Boyes, "China Accused of Hacking into Heart of Merkel Administration," *The Times*, August 27, 2007, available at: *http://www.thetimes.co.uk/tto/news/world/europe/article2595759.ece*; Donna Buenaventura, "China Tried to Hack Our Computers, Says India Security Chief M.K. Narayanan," *The Times Online*, January 18, 2010, available at: *http://blogs.msmvps.com/donna/2010/01/18/china-tried-to-hack-our-computers-says-india-s-security-chief-m-k-narayanan/*.
[41] Nathan Ingraham, "US Government Claims Huawei and ZTE Pose a Risk to National Security: the Accusations, Responses, and Fallout," *The Verge,* October 11, 2012, available at: *http://www.theverge.com/2012/10/11/3488584/huawei-zte-us-government-security-investigation*.
[42] "Admit Nothing and Deny Everything," *The Economist*, June 6, 2013, available at: *http://www.economist.com/news/china/21579044-barack-obama-says-he-ready-talk-xi-jinping-about-chinese-cyber-attacks-makes-one*.
[43] Joe McReynolds, "Cyber Transparency for Thee, But Not for Me," *The Jamestown Foundation China Brief*, 14: 8, available at: *http://www.jamestown.org/single/?tx_ttnews[tt_news]=42246&no_cache=1#.VTfXNBdSxdY* .

statements issued from China's Ministry of Defense,[44] Ministry of Foreign Affairs,[45] and its Prime Minister[46] have towed the same party line, asserting that China is not behind the attacks, that China is a victim not a perpetrator of cyber-crime activity, and that China's laws strictly identify hacking as illegal.[47]

However, China shifted to a more assertive stance once former NSA contractor Edward Snowden released alleged highly classified documents exposing U.S. global surveillance efforts. Instead of trying to deflect accusations, China now points its own finger at the U.S. government. In particular, Beijing has demanded an explanation from the United States over reports of NSA spying on the Chinese company Huawei.[48] The irony is not lost on China, given earlier U.S. government concerns over Huawei's suspected spying on behalf of the Chinese government, which was ultimately not proven after a study was conducted on behalf of the U.S. Congressman and Chairman of the House Permanent Select Committee on Intelligence, Mike Rogers.[49] Although skeptics persisted, in October 2012, the White House conducted its own security review of Huawei and found no clear evidence that Huawei spied on behalf of the Chinese government.[50] Further pushing U.S. cyber malfeasance into the spotlight, in March 2014, China's National Computer Emergency Response Team identified the United States as the top source of intrusion activity against its computers.[51]

---

[44] Charles Riley, "China's Military Denies Hacking Allegations," *CNNMoney,* February 20, 2013, available at: *http://money.cnn.com/2013/02/20/technology/china-cyber-hacking-denial/*.

[45] David Barboza, "China Says Army Is Not Behind Attacks in Report," *The New York Times,* February 21, 2013, available at: *http://www.nytimes.com/2013/02/21/business/global/china-says-army-not-behind-attacks-in-report.html?_r=0*.

[46] "Espionage Report: Merkel's China Visit Marred by Hacking Allegations," *Spiegel Online*, August 27, 2007, available at: *http://www.spiegel.de/international/world/espionage-report-merkel-s-china-visit-marred-by-hacking-allegations-a-502169.html*.

[47] "M Trends 2014: Beyond the Breach," *Mandiant*, available at: *https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf*.

[48] Liz Peek, "U.S. and China in a Lethal Game of Cyber Chess," *The Fiscal Times*, April 9, 2014, available at: *http://www.thefiscaltimes.com/Blogs/Peek-POV/2014/04/09/US-and-China-Lethal-Game-Cyber-Chess*.

[49] Mike Rogers and Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei Technologies and ZTE," *U.S. House of Representatives*, October 8, 2012, available at: *https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf*.

[50] "Huawei: Leaked Report Shows No Evidence of Spying," *BBC News*, October 18, 2012, available at: *http://www.bbc.com/news/technology-19988919*.

[51] Ben Blanchard, Li Hui, and Paul Carsten, "China Blames U.S. for Rise in Hacking Attacks," *The Fiscal Times*, March 28, 2014, available at:



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

U.S. efforts to manage its public image have fallen short after allies and adversaries alike expressed outrage from the Snowden scandal.[52] The subtle nuance from which the U.S. government bases its defense, namely that it conducts such activities to support national security interests and not to provide competitive advantage to U.S. corporations, seems trite, particularly after being caught with its hand in the proverbial cyber cookie jar. Several accusations have surfaced because of leaked documents pointing to the NSA spying on non-national security entities such as Brazil's biggest oil company,[53] the European Union commissioner investigating Google, Microsoft, and Intel,[54] and the International Monetary Fund and World Bank.[55] Even on its home front, the U.S. public and special interest groups seeking to preserve civil liberties have condemned NSA activities.[56]

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 willing cyber security partner. In 2014, China expressed its desire for mutual cyber cooperation with the United States,[57] and as of April 2014, the Pentagon has engaged in military exchanges with China in the spirit of military transparency.[58]

---

*http://www.thefiscaltimes.com/Articles/2014/03/28/China-Blames-US-Rise-Hacking-Attacks*.

[52] Charly Wilder, "Out of Hand: Europe Furious over U.S. Spying Scandal," *Spiegel Online*, October 24, 2013, available at: *http://www.spiegel.de/international/world/angry-european-and-german-reactions-to-merkel-us-phone-spying-scandal-a-929725.html*.

[53] Jonathan Watts, "NSA Accused of Spying on Brazilian Oil Company Petrobas," *The Guardian*, September 9, 2013, available at: *http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras*.

[54] Edward Moyer, "NSA Spied on EU Antitrust Official Who Sparred With U.S. Tech Giants," *Cnet*, December 20, 2013, available at: *http://www.cnet.com/news/nsa-spied-on-eu-antitrust-official-who-sparred-with-us-tech-giants/*.

[55] Mark Hosenball, "Obama Halted NSA Spying on IMF and World Bank Headquarters," *Reuters*, October 31, 2013, available at: *http://www.reuters.com/article/us-usa-security-imf-idUSBRE99U1EQ20131031*.

[56] Charlie Savage, "Watchdog Report Says NSA Is Illegal and Should End," *The New York Times*, January 23, 2014, available at: *http://www.nytimes.com/2014/01/23/us/politics/watchdog-report-says-nsa-program-is-illegal-and-should-end.html?partner=rss&emc=rss&smid=tw-nytimes&_r=1*.

[57] "U.S., China Agree to Work Together on Cyber Issues," *Reuters*, April 13, 2013, available at: *http://www.reuters.com/article/2013/04/13/us-china-us-cyber-idUSBRE93C05T20130413*.

[58] Peek, "U.S. and China in a Lethal Game of Cyber Chess."

Despite ongoing allegations of Chinese cyber misconduct, China has made strides in somewhat polishing its tarnished image at the timely expense of U.S. secret cyber activities. Perhaps in light of this, in May 2014, the U.S. Justice Department indicted five Chinese military hackers for cyber espionage.[59] While this landmark decision attempted to directly implicate China's government with cyber espionage, it failed to incriminate China any more in the public's eye. After all, many public and private organizations generally believe that the Chinese government steals intellectual properties and sensitive information. Rather, the onslaught of exposed highly sensitive documents revealing the U.S. government's role in similar activity (against allied and adversary governments alike) proved to be a bigger injustice and a black mark against a government advocating human rights and individual freedoms.

## Legal warfare

Legal warfare is one of the key instruments of psychological and public opinion warfare.[60] Legal warfare is typically used in conjunction with one or both of the other two types of warfare as maximum effectiveness is achieved when they build upon each other. In this way, legal warfare provides the basis that strengthens public opinion warfare and psychological warfare.[61] By definition, legal warfare is designed to provide justification for a course of action.

There are two influences that help form Chinese legal warfare:

- *Chinese Views of the Role and Rule of Law*–Historical and cultural considerations inform the Chinese government's understanding of legal warfare. Confucianism and Legalist influences were integral to imperialist China but as the government evolved during Mao's tenure, Marxist perspectives advocated that the "law should serve as an

[59] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, May 19, 2014, available at: *http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor*.
[60] Dean Cheng, "Winning Without Fighting: Chinese Legal Warfare," The *Heritage Foundation,* No. 2692, May 21, 2012, available at: *http://www.heritage.org/research/reports/2012/05/winning-without-fighting-chinese-legal-warfare*.
[61] Kexin, L., *Study Volume on Legal Warfare,* (Beijing, PRC: National Defense University Press, 2006): 18, 34-37.



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

ideological instrument of politics."[62] Today, there is a focus on commercial and contract law, while criminal law remains weak.[63]

- *Chinese Perception of Legal Warfare in the West*–China perceives that importance of Western interests to use law as justification for its actions. In the first Gulf War, the United States obtained U.N. authorization for sanctions as well as use of force in Iraq, while in Kosovo, it argued that its actions were "consistent with the law" because they were taken under NATO auspices.[64] Being able to use rule of law or its legal perceptions to justify actions is a powerful tool in Chinese thinking.

### *Chinese legal warfare applications to cyberspace*

As a mode of influence, legal warfare is typically used prior to the outbreak of physical conflict, and occurs only in context of actual warfare. However, since the international spotlight has shifted to cyber espionage activities and China has been called out as a perpetrator of intellectual property theft, evidence suggests that the Chinese may be using tenets of legal warfare to push strategic interests. The following events occurred after several governments publicly blamed China for hacking into their networks and stealing data:

- *2014 U.S. Plans to Relinquish Internet Control*–In December 2012, China along with Russia gained international support to have all states have equal rights to the governance of the Internet. The agreement updated 24-year-old U.N. telecommunications rules.[65] While non-binding, eighty-nine countries signed it with 55 reserving the right to sign it at a later date,[66] showing the widespread support. This initiative continued the necessary steps for the International Telecommunications Union (ITU) to play an active role in the multi-stakeholder model of the Internet.[67] Such efforts, coupled with the leaking of sensitive documents pertaining to the National Security

[62] Eric W. Orts, "The Rule of Law in China," *Vanderbilt Journal of Transnational Law*, January 1, 2001, available at: *http://www.highbeam.com/doc/1G1-72733959.html*.
[63] Cheng, "Winning Without Fighting: Chinese Legal Warfare."
[64] Ibid.
[65] Amy Thomson, "UN Telecom Treaty Approved Amid U.S. Web-Censorship Concerns," *Bloomberg*, December 14, 2012, available at: *http://www.bloomberg.com/news/articles/2012-12-13/u-s-and-u-k-refuse-to-sign-un-agreement-on-telecommunications*.
[66] "U.S. and UK Refuse to Sign UN's Communications Treaty," *BBC News,* December 14, 2012, available at: *http://www.bbc.co.uk/news/technology-20717774*.
[67] Ibid.

Agency's alleged global surveillance, applied considerable pressure on the United States to back away from supporting the Internet Corporation for Assigned Names and Numbers' (ICANN) influence on Internet controls.[68] Gaining international support and using the ITU as an authorized body gave these efforts the auspice of legitimacy. As of January 2016, U.S. officials remained committed to relinquishing federal government control over the administration of the Internet by September.[69]

- *2011/2015 China-Russia Letters to the United Nations*–Since there are no official international laws or even common definitions governing cyber activity, China has been a prominent voice in advocating for norms of behavior for nation states. In 2011, China teamed up with Russia, Tajikistan, and Uzbekistan to submit an international code of conduct for information security to the U.N.,[70] and updated it in January 2015.[71] Essentially, the core of both proposals highlighted identifying the rights and responsibilities of states in the information space, as well as promoting their constructive and responsible behaviors to enhance their cooperation in addressing common threats and challenges. Although as of this writing, the proposal is still being reviewed by member states, China did assume a leading international role in trying to establish behavior norms for nation states using an international body as a validating entity of its efforts.

[68] Craig Timberg, "U.S. to Relinquish Last Control Over the Internet," *The New York Times*, March 14, 2014, available at: *http://www.washingtonpost.com/business/technology/us-to-relinquish-remaining-control-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.html*.
[69] RRN Prasad, "Towards Freedom of the Internet," *The Financial Express*, January 4, 2016, available at: *http://www.financialexpress.com/article/fe-columnist/towards-freedom-of-the-internet/187447/*.
[70] "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-Genera," UN General Assembly, A/66/359, available at: *https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf*.
[71] "Letter Dated 09 January 2015 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary General," UN General Assembly, A/69/723, *https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf*.



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

- *2009 Updating of Chinese Cybercrime Legislation*–China has maintained publicly that hacking is against Chinese laws.[72] In 2009, China extended penalties for those convicted of cybercriminal activities.[73] When accused of sponsoring hacking, China is quick to cite its laws as a legal justification of why it does not engage in that activity.[74]

China uses international organizations like the UN, whose authorization is backed by legal considerations, in order to give its efforts legitimacy. This ultimately serves two important strategic objectives: 1) It tempers the negative image of China as a hacking state by showing that it is seeking to work collectively and within the defined rules of established international organizations, and 2) It helps China implement non-kinetic asymmetric means to pursue its political and economic objectives, avoiding the need to use military force or influence, thereby reducing the risk of potential escalation over a given issue.

## Chinese psychological warfare

Psychological Warfare is deeply rooted in Chinese strategy; for example, "Chinese writings posit that during peacetime, psychological operations seek to reveal and exploit divisions in the enemy's domestic political establishment or alliance system and cast doubt on the enemy's value concepts."[75] It aims for a high degree of precision in targeting critical nodes in order to achieve nonlinear effects.

[72] "China Says Cyber Hacking is Against the Law," *Voice of America*, January 13, 2010, available at: *http://www.voanews.com/content/china-says-cyber-hacking-is-against-law-81473967/111452.html*.
[73] Gu Jian, **"**Strengthening international cooperation and joining hands in fighting against transnational cybercrime," *China.org,* November 9, 2010, available at: *http://www.china.org.cn/business/2010internetforum/2010-11/09/content_21306503.htm*.
[74] Jim Finkle, Joseph Menn, and Aruna Viswanatha, "US Accuses China of Cyber Spying on American Companies," *Reuters*, November 20, 2014, available at: *http://www.reuters.com/article/2014/11/20/us-cybercrime-usa-china-idUSKCN0J42M520141120*.
[75] Mark Stokes, "The Chinese Joint Aerospace Campaign: Strategy, Doctrine, and Force Modernization in China's Revolution in Doctrinal Affairs," James Mulvenon and David Finklestein (eds.), (Alexandria, VA: CNA Corporation, 2005), 272.

*Chinese psychological warfare applications to cyberspace*

According to Chinese scholars, psychological warfare is an integral part of information warfare.[76] However, defining information warfare in a Chinese context is more challenging, as there is not a published doctrine on information warfare and there are only Chinese doctrinal writings available to provide insight into this complex discipline. Early writings on the subject were largely borrowed from translated United States, Russian, French, and German doctrines.[77] As time has passed, there have been developments in Chinese thinking with regard to information warfare, most notably with regard to the concept of 'information dominance,' which according to Chinese cyber expert Dr. James Mulvenon, is the main objective of Chinese information warfare strategy.[78] Information dominance has two primary targets: The physical information infrastructure and the data that has passed through it, and perhaps more importantly, the human agents that interact with those data, especially those making decisions.[79]

According to Chinese writings, there are five broad tasks associated with psychological warfare.[80] Taking into consideration China's involvement in global intrusion activity, these tasks may be applied to the current environment in the following manner:

1) *Presenting Your Own Side as Just*—China is very much concerned with its public image, which makes its ambivalence toward the negative publicity surrounding suspected hacking activity curious. All attempts to 'blame and shame' China have ended in a resounding failure, which can be attributed to the fact that China has established and maintained the same official position, regardless of what government is finger pointing. Beijing typically parries such claims by consistently denying hacking allegations and then immediately pointing out that they are the victims of hacking.[81] Further, as noted

[76] Dean Cheng, "Winning Without Fighting: The Chinese Psychological Warfare Challenge," *The Heritage Foundation*, No. 2821, July 11, 2011, available at: *http://www.heritage.org/research/reports/2013/07/winning-without-fighting-the-chinese-psychological-warfare-challenge*.
[77] Ferguson, "Information Warfare with Chinese Characteristics," 31.
[78] James Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, James Mulvenon and Richard H. Yang (eds.) (Washington, DC: RAND, 1999): 180.
[79] Cheng, "Winning Without Fighting: The Chinese Psychological Warfare Challenge."
[80] Guo Yanhua, *Psychological Warfare Knowledge* (Beijing: National Defense University Press, 2005), 14-16.
[81] "Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting," *The White House*, June 8, 2013, available at:



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

earlier, Beijing frequently cites that hacking is against the law in China,[82] trying to show that, as a country, it is doing its part to best address hostile activities in cyberspace through legal channels. Lastly, China in partnership with Russia, Tajikistan, and Uzbekistan, proposed before the United Nations (UN) a code of conduct in cyberspace for nation states,[83] and updated it in February 2015 after it had received input from member states.[84] This achieved two important objectives: 1.) It showed China being proactive in trying to establish an international set of responsible behavior norms for nation states in cyberspace; and 2.) It demonstrated China's willingness to collaborate with others as equals. The proposal tendered at the UN further demonstrated China's desire to gain consensus among the international community. Taken collectively, these efforts can be interpreted as China's mitigation of the negative press it receives by presenting itself as responsible and collaborative. The proactive desire to collaborate with other governments on such issues may have been the impetus to lead the United States in June 2015 to agree to negotiate with China on some kind of "code of conduct" in cyberspace.[85]

2) *Emphasizing One's Advantages*—In 2014, China became the world's largest economy. China's gross domestic product blistered from 2003-13, averaging more than 10 percent a year.[86] While the United States has kept Chinese companies at bay from penetrating U.S. markets, China has enthusiastically pursued other markets where the U.S. has typically enjoyed a trade advantage. Recently, China overtook the United States as Africa's and Brazil's largest trade partner. [87] This has

*http://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-*.

[82] "China Says Cyber Hacking is Against the Law."

[83] "Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary General."

[84] "Letter Dated 09 January 2015 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary General."

[85] Greg Austin, "China's Cyber Turn: Recognizing Change for the Better," *The Diplomat*, December 21, 2015, available at: *http://thediplomat.com/2015/12/chinas-cyber-turn-recognizing-change-for-the-better/*.

[86] Tom Orlik, "Charting China's Economy: 10 Years Under Hu," *The Wall Street Journal*, November 16, 2012, available at: *http://blogs.wsj.com/chinarealtime/2012/11/16/charting-chinas-economy-10-years-under-hu-jintao/tab/print/*.

[87] "More than Minerals," *The Economist,* May 23, 2013, available at: *http://www.economist.com/news/middle-east-and-africa/21574012-chinese-trade-*

translated into economic advantages regardless of negative press about alleged Chinese hacking. These countries simply do not care about the threat, seeing economic engagement and accelerated infrastructure development as outweighing any potential consequence. Brazil is welcoming more Chinese private customers as active players in more diversified ways of bilateral economic cooperation,[88] and in Africa, China has been the leading supplier of telecommunications equipment.[89] The stigma placed on the Chinese telecommunications company Huawei is a perfect example of China playing to its strengths. Despite the suspicions leveled largely by the U.S. government that Huawei may act as an agent of the Chinese government, the House-driven study didn't yield any conclusive proof of espionage. Furthermore, the company is "the second largest telecommunications provider in the world, with deployed products and solutions in over 140 countries, indicating that several countries in the world are not as concerned with Huawei posing an intelligence threat."[90] Even U.S. allies Australia and the UK appear not to levy the same level of concerns as the United States. The UK's Huawei Advisory Board–an entity composed of both members of the UK's intelligence service GCHQ staff, governmental employees, and members of industry, as well as Huawei personnel–concluded after an audit that Huawei's work in the UK did not pose a national security threat.[91] In 2013, Huawei supported the creation of an Australian Cyber Security Center development to test the security credentials being implemented into critical infrastructure.[92]

---

*africa-keeps-growing-fears-neocolonialism-are-overdone-more*; "China Overtakes U.S. as Brazil's Top Trade Partner," *Latin American Times*, October 17, 2013, available at: *http://www.laht.com/article.asp?ArticleId=333733&CategoryId=10718*.

[88] Du Wenjuan, "China Investment in Brazil More Diversified," *China Daily*, May 14, 2013, available at: *http://usa.chinadaily.com.cn/business/2013-05/14/content_16498645.htm*.

[89] "China's Mighty Telecom Footprint in Africa," *New Security Learning,* February 14, 2011, available at: *http://www.newsecuritylearning.com/index.php/archive/75-chinas-mighty-telecom-footprint-in-africa*.

[90] Emilio Iasiello, "Stuffing the Genie Back into the Bottle: Can Threats to the IT Supply Chain Be Mitigated?" *Foreign Policy Journal*, April 3, 2013, available at: *http://www.foreignpolicyjournal.com/2013/04/03/stuffing-the-genie-back-in-the-bottle-can-threats-to-the-it-supply-chain-be-mitigated/*.

[91] Liat Clark, "Huawei Not a Threat to UK..Says Huawei Oversight Board," *Wired*, March 27, 2015, available at: *http://www.wired.co.uk/news/archive/2015-03/27/huawei-not-a-threat-to-national-security*.

[92] Hafizah Osman, "Huawei Supports Australian Cyber Security Centre Development," *Arnnet.com*, January 23, 2013, available at: *http://www.arnnet.com.au/article/451519/huawei_supports_australian_cyber_security_centre_development_/*.



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

3) *Undermining the Opposition's Will to Resist*—There have been several writings on the China cyber threat by civilian and government regional, cultural, and functional experts, in addition to international media and print news channels covering the topic. In each instance, two resounding messages are conveyed: 1) The Chinese cyber threat is massive and pervasive representing the largest transfer of wealth in human history,[93] and 2) China seeks access to computer networks to not only steal sensitive information but also to establish "information dominance."[94] Whether described as being sophisticated, rudimentary, or somewhere in between, Chinese espionage activity has been constant and persistent. Even the term "advanced persistent threat," given to it purportedly by the U.S. Air Force in 2006 to be able to discuss it with unclassified personnel,[95] portrays the adversary as skilled and relentless, and considering its lack of covertness, fearless as well. The fact that there have been few consequences suffered by the alleged Chinese cyber operatives for their actions lends further support to the notion that they cannot be beat, or at the very least, their brazen activity cannot be stopped. As Richard Clarke said, "Every major company in the United States has already been penetrated by China."[96] Coming from a man considered the first cyber czar in the U.S. government, such platitudes further paint the adversary as a nearly unbeatable opponent.

4) *Encouraging Dissension in the Enemy's Camp*—This task focuses on disrupting the cognitive processes of policymakers and decision makers, inhibiting their ability to develop a plan of action. The theory suggests that the best strategy is to attack the enemy's mind, leaving him unable to plan,[97] which given U.S. policymakers' history of not

---

[93] Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History.'"
[94] Marcel A. Green, "China's Growing Cyberwar Capabilities," *The Diplomat*, April 13, 2015, available at: *http://thediplomat.com/2015/04/chinas-growing-cyberwar-capabilities/*.
[95] Richard Bejtlich, "Testimony before the U.S. China Economic and Security Review Commission Hearing on "Developments in China's Cyber and Nuclear Capabilities," March 26, 2012, available at: *http://www.uscc.gov/sites/default/files/3.26.12bejtlich.pdf*.
[96] Jonathan Fisher, "China Has Hacked Every Major U.S. Company, Claims Richard Clarke," *Web Pro News*, March 28, 2012, available at: *http://www.webpronews.com/china-has-hacked-every-u-s-major-company-claims-richard-clarke-2012-03*.
[97] Timothy L. Thomas, "New Developments in Chinese Strategic Psychological Warfare," *Special Warfare* 1:9 (2003), available at: *http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA434978*.

being in accordance on cyber issues, makes them a prime exploitable target. One thing is clear: Since suspected Chinese cyber espionage was first discovered in 2003,[98] there has been no concrete course of action as to how to handle Chinese cyber espionage until the United States' creation of cyber sanctions, an effort to deter all grave cyber activities, but in particular, those believed to be conducted or endorsed by China.[99] Previously, agencies supported various courses of action. There were proponents of "active cyber defense" such as U.S. Cyber Command[100] and the Defense Advanced Research Projects Agency[101] as a means to deter adversaries in cyberspace. However, there were some like U.S. Representative Mike Rogers who believed there needed to be a viable strong defense in place before engaging in any offensive cyber operations.[102] Still others, such as the Government Accountability Office (GAO) cited lack of clearly defined roles and responsibilities of federal agencies as a serious impediment to productive cyber security.[103] Continued failure to establish a strong national level cyber security strategy prohibits the U.S. government from going down a unified path with all stakeholders understanding their part in the process. Even a February 2013 Executive Order on Improving Critical Infrastructure Cyber Security has not generated significant support. While a positive step, it failed to clearly mandate changes, relying on companies' willingness to comply with the measures stated in the order. Although it did not reference the February Order, the GAO in a March report still cited the need of an integrated national cyber security strategy complete with milestones, performance measures, and Congressional oversight.[104] Whether

[98] Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time*, August 25, 2005, available at: *http://content.time.com/time/nation/article/0,8599,1098371,00.html*.
[99] Tal Kopan, "White House Readies Cyber Sanctions Against China Ahead of State Visit," *CNN*, September 24, 2015, available at: *http://www.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-president-obama/*.
[100] "Strategy for Operating in Cyberspace," U.S. Department of Defense, July 2011, available at: *http://www.defense.gov/news/d20110714cyber.pdf*.
[101] Angelos Keromytis, "Active Cyber Defense," *DARPA*, available at: *http://www.darpa.mil/program/active-cyber-defense*.
[102] John Reed, "Mike Rogers: Cool It with Offensive Cyber Ops," *ForeignPolicy.com*, December 14, 2012, available at: *http://foreignpolicy.com/2012/12/14/mike-rogers-cool-it-with-offensive-cyber-ops/*.
[103] "National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented," *Government Accountability Office,* February 2013, available at: *http://www.gao.gov/assets/660/652170.pdf*.
[104] "A Better Defined and Implemented National Strategy is Needed to Address Persistent Challenges," *Government Accountability Office,* March 7, 2013, available at: *http://www.gao.gov/assets/660/652817.pdf*.



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

intentionally or not, Chinese cyber espionage campaigns have taken advantage of the indecisive climate that had permeated in the U.S. government prior to the 2015 agreement between the two governments to not hack each other for commercial economic advantage.

5) *Implementing Psychological Defenses*—In the Chinese view, it is assumed that an opponent will mount psychological attacks, as well as exposing them and defeating them in order to demoralize an opponent by demonstrating the ineffectiveness of his efforts.[105] China has maintained its political stance that it does not conduct hacking. Even after approaching Chinese President Xi Jinping directly about Chinese espionage, Xi deflected blame onto poor network security, and not the government hacking U.S. targets. Indeed, when the NSA's secret surveillance program was exposed, China immediately jumped on the opportunity of making the U.S. government the bad guy.[106] Even the much-maligned Chinese telecommunications giant Huawei seized the moment to condemn NSA spying and promote a global cyber security dialogue.[107]

When these five psychological warfare tasks are taken collectively, the message being promoted is that China is a dominant cyber force. By denying the accusations, China further builds on this image without having to say it publicly, or leak into the press its involvement in a significant cyber event.. After all, unlike the U.S., China has not found the desire or need to bolster its image as a dominant player in cyberspace via public announcements or national strategies; instead, Beijing has relied upon others to speculate on its capabilities and strength, allowing it to concentrate its energies on trying to temper negative press while concurrently maintaining its covert espionage efforts to support its national objectives.

## Dodging U.S. Cyber Sanctions

While the Chinese cyber espionage activity has enjoyed relative freedom for a substantial amount of time, the 2015 state visit put China on notice that cyber

[105] Cheng, "Winning Without Fighting: The Chinese Psychological Warfare Challenge."
[106] "China Accuses U.S. of Hypocrisy Over Internet Spying," *Sydney Morning Herald*, June 28, 2013, available at: *http://www.smh.com.au/world/china-accuses-us-of-hypocrisy-over-internet-spying-20130628-2pouk.html.*
[107] Ellen Messmer, "Don't Trust the NSA? China-based Huawei Says, 'Trust Us,'" *Network World,* October 18, 2013, available at: *http://www.networkworld.com/news/2013/101813-nsa-huawei-274959.html?page=1.*

espionage for commercial advantage would not be tolerated by the United States. In an effort to avoid these penalties, Beijing reached accord days before President Xi's official state visit to the United States in which both agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[108]

As a result of the agreement, China arrested hackers identified by the United States,[109] thereby demonstrating its commitment to arresting criminal elements in cyberspace, even if they are China's own citizens. While opinions differ on Beijing's motives for arresting Chinese hackers, it is not without precedent. In 2010, after a lengthy international coordinated effort, Chinese authorities detained a Chinese national for hacking seven National Aeronautics and Space Administration (NASA) systems, according to a testimony from a NASA official to Congress.[110]

While Washington waits to see if Beijing will prosecute these hackers, the more important takeaway is China's demonstration of its willingness to work with the United States–and perhaps by extension other governments as well–on similar cyber issues, something that had not been done previously. Sanctions still loom large on the table if perceived Beijing-sponsored hacking against commercial interests does not abate; however, if handled correctly, the threat of sanctions may ultimately serve China's interests by addressing head-on the biggest black mark against China. Holding fast to the principles of legal and media warfare, China's assurance of "opposing cyber attacks and espionage and combating all forms of hacking activities in accordance with the law,"[111] coupled with public examples of collaborating with stakeholders toward this end, may gradually assuage opponents' concern of the "China threat," and in turn, depict China as a willing partner instead of an antagonist.

---

[108] "FACT SHEET: President Xi Jinping's State Visit to the United States," The White House, September 25, 2015, available at: *https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states*.
[109] "Chinese Hackers Arrested After U.S. Request," *BBC News*, October 12, 2015, available at: *http://www.bbc.com/news/technology-34504317*.
[110] Paul K. Martin, Inspector General, National Aeronautics and Space Administration, "NASA Cybersecurity: An Examination of the Agency's Information Security," Statement before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, February 29, 2012, available at: *https://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf*.
[111] "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on October 13, 2014," Ministry of Foreign Affairs, October 13, 2015, available at: *http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1165638.shtml*.



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

Additionally, initiating additional cyber security cooperation with regional governments will further bolster China's message of seeking a stable Internet, safe from criminal and terrorist activities. China has been active in this regard, engaging in cyber security discussions with Japan,[112] Malaysia,[113] and South Korea,[114] as well as a series of no-hack pacts leading to the November 2015 G20 agreement to not conduct cyber-enabled commercial espionage.[115]

It can be expected that China will pursue more of these through independent bilateral meetings or through international organizations like the Shanghai Cooperation Organization.

## Conclusion

Despite being accused of perpetrating long running and substantial cyber espionage campaigns against the United States as well as several other countries, China has escaped any significant punitive or economic repercussions. China's "Three Warfares," a three-pronged information warfare strategy designed to influence the international community, has played an important role in forestalling any significant deterrence response, while allowing China to promote itself as a viable partner in cyberspace. China has sought to dull public perception of its rising threat by denying accusations, while capitalizing on the Snowden leaks of U.S. global surveillance activities to tarnish the U.S. image. Concurrently, China has used legal mechanisms to help promote itself as a viable cybersecurity partner. The act of championing the right of every state to be included on Internet governance gained enough traction to encourage the U.S. to step down from its governing role. Providing the UN with an updated "code of conduct" for nation state behavior in cyberspace demonstrated its interest to the global community that it was leading efforts toward achieving stability in cyber space. Updating its cyber-crime legislation exhibited Beijing's commitment

---

[112] "S.Korea, Japan, China to Hold Cyber Policy Talks," *Yonhap News Agency*, October 13, 2015, available at: *http://english.yonhapnews.co.kr/news/2015/10/13/0200000000AEN20151013004800315.html.*

[113] "Malaysia, China to Work Together on Cyber Crimes," *The Malay Mail Online*, August 22, 2014, available at: *http://www.themalaymailonline.com/malaysia/article/malaysia-china-to-work-together-to-combat-cyber-crimes.*

[114] "S.Korea, Japan, China to Hold Cyber Policy Talks."

[115] Ellen Nakashima, "World's Richest Nations Agree Hacking for Commercial Benefits Is Off-Limits," *The Washington Post*, November 16, 2015, available at: *https://www.washingtonpost.com/world/national-security/worlds-richest-nations-agree-hacking-for-commercial-benefit-is-off-limits/2015/11/16/40bd0800-8ca9-11e5-acff-673ae92ddd2b_story.html.*

toward penalizing those engaged in hacking, quickly followed by arresting suspected hackers at the U.S. behest in 2015.[116] Finally, China's use of psychological operations (PSYOPS) has presented itself as a law abiding stakeholder in cyberspace while quietly basking in the writings that have identified it as a significant cyber power. The more experts warn of China's powerful cyber capabilities, the more of a cyber equal China is perceived to be without Beijing ever having to intimate it.

As a result, the confluence of these three strategies has kept the West from deterring suspected Chinese espionage for a substantial period of time. In fact, the more time that has been allowed to elapse, the more China has been able to take advantage of it. In the time that the U.S. has mulled over finally levying cyber sanctions against China, Beijing has capitalized on meeting with countries like Japan and South Korea on cyber security issues,[117] as well as engaging in a series of "no hack pacts" between China and Russia,[118] the United Kingdom, [119] and the United States,[120] an effort culminating in the historic November 2015 agreement by members of the G20 to not engage in cyber-enabled espionage for commercial advantage.[121]

Moreover, China has done this while becoming the world's largest economy in the process, and while promoting itself as a regional leader by spearheading efforts for a Maritime Silk Road (a system of linked ports, projects and special economic zones in Southeast Asia and the northern Indian Ocean[122]) and the Asian Infrastructure Investment Bank (which already has 20 governments on

---

[116] Ellen Nakashima, "Chinese Government Has Arrested the Hackers Breached OPM Database," *The Washington Post*, December 2, 2015, available at: *https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html*.
[117] "S. Korea, Japan, China to Hold Cyber Policy Talks."
[118] Olga Razumovskaya, "Russia and China Pledge Not to Hack Each Other," *The Wall Street Journal blog*, May 8, 2015, available at: *http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/*.
[119] Katie Bo Williams, "UK, China Mirror U.S. Anti-Hacking Pact," *The Hill*, October 21, 2015, available at: *http://thehill.com/policy/cybersecurity/257602-uk-china-mirror-us-anti-hacking-pact*.
[120] "Fact Sheet: President Xi Jinping's State Visit to the United States," *The White House*, September 25, 2015, available at: *https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states*.
[121] Nakashima, "World's Richest Nations Agree."
[122] David Brewster, "The Bay of Bengal: The Maritime Silk Route and China's Naval Ambitions," *The Diplomat,* December 14, 2014, available at: *http://thediplomat.com/2014/12/the-bay-of-bengal-the-maritime-silk-route-and-chinas-naval-ambitions/*.



https://scholarcommons.usf.edu/jss/vol9/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489

board).[123] China's plan may just be to rise through its region first before ascending to a global throne brought on by some of the fruits of its espionage efforts. In this context, China's cyber espionage can be viewed as less about reducing U.S. capability, and more about building itself to assume a larger status in the world.

[123] Thitinan Pongsudhirak, "China's Aspiring Global Leadership," *East Asia Forum,* November 25, 2014, available at: *http://www.eastasiaforum.org/2014/11/25/chinas-aspiring-global-leadership/*.