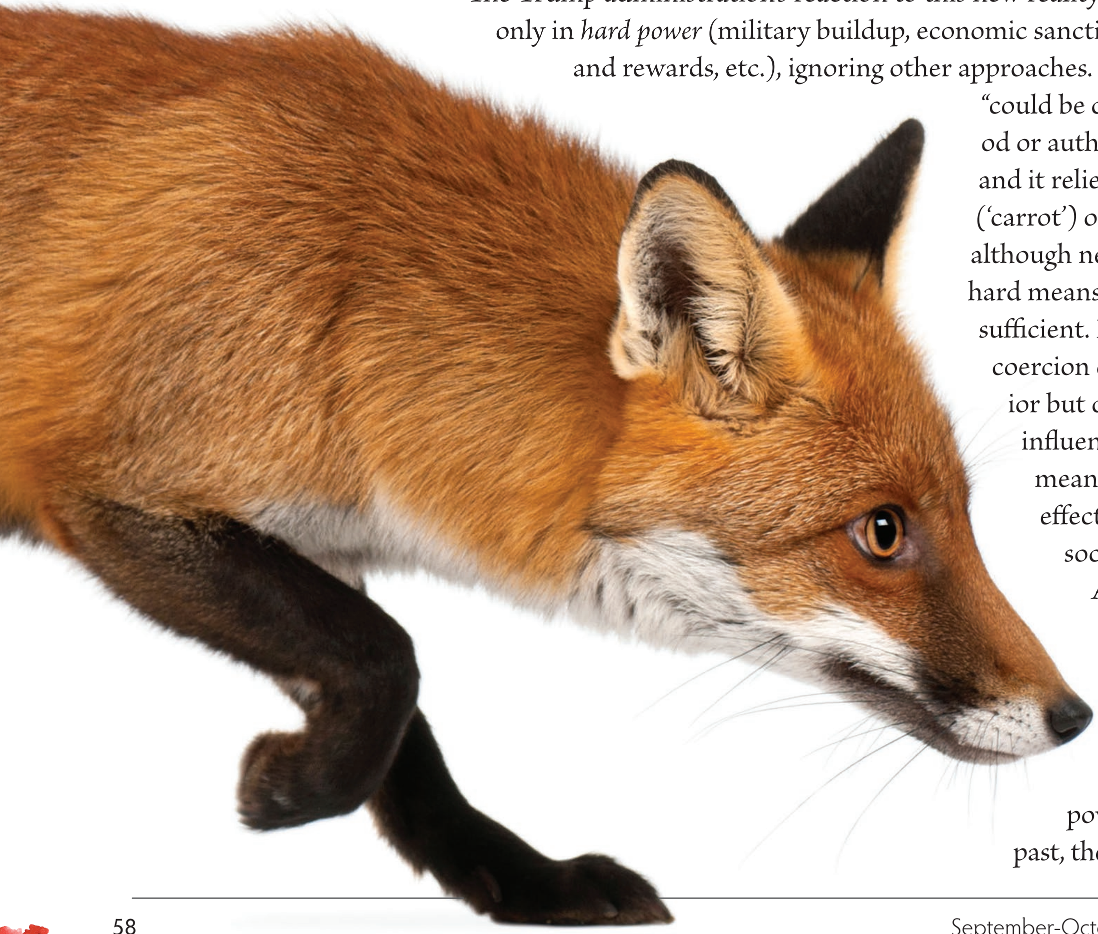
A Chinese Fox against an American Hedgehog in Cyberspace?

Kimberly Orinx

Tanguy Struye de Swielande, PhD

CHINA'S NEW STYLE WARFARE SUBMISSION

While the end of the Cold War was described as a "unipolar moment"—as defined by Charles Krauthammer in 1991—this period is now over.[1] For several years, we have experienced the return of a power competition in which America's influence is fading and challenged by other countries. The *National Security Strategy of the United States of America* identifies China and Russia as "revisionist powers" competing against the United States.[2] This state competition naturally takes place on the classical chessboard (economic and military) but also on the discursive and ideational one.



The Trump administration's reaction to this new reality has been to invest almost only in *hard power* (military buildup, economic sanctions, coercion, punishments, and rewards, etc.), ignoring other approaches. This hard-power logic "could be called [a] directive method or authority of exercising power," and it relies "on the use of incentives ('carrot') or threats ('stick')."[3] However, although necessary for great powers, hard means by themselves are far from sufficient. Indeed, influence through coercion can impact states' behavior but only in the short term. To influence on the long term, other means of power are needed; effective influence also rests on socialization and persuasion. As Eric Delbecque stresses,

> Throughout history, we have witnessed a shift in the representation and implementation of power strategies. In the past, the canons established

> the ranking of nations. Influence strategies only accompanied peripherally the essential movements traversing the military chessboard. In our times, the situation has totally reversed: strategies of influence express and structure the clashes of actors in all spheres of competition between human communities, cultural models and private organizations. It is not about aggressively defeating your rival; rather, it is about slowly depriving him of freedom of movement (through concealed or hypocritical action), constraining his choices, limiting his possibilities and prospects. In shaping your rival's global environment, you guarantee his slow decline and your own supremacy.[4]

China has well understood this dynamic and is attempting to master it with the development of cyber power. Unlike the United States, China grasps the importance of "soft" means. Although, as pointed out by Washington, the People's Republic of China (PRC) has the capacity to disrupt, at least temporarily, American critical infrastructure such as gas pipelines or power networks through cyberattacks, this is only a piece of how China uses cyber warfare. In 2017, China defended the idea of becoming a cyber superpower, presenting the Chinese model as the one to follow, calling it "a new option for other countries and nations that want to speed up their development while preserving their independence."[5] Thus, as the 2017 Munich Security Conference stressed, cyberconflicts today do not only target infrastructure but also the Western political system and its core values.[6] This article explains how China is developing as a cyber superpower and is forming a threat to American and Western values and interests.

A Chinese Integrative Cyber Policy

The first events that come to mind when considering cyberattacks are the Estonian cyberattacks (2007), the Stuxnet virus (2010), and the WannaCry software (2017), which were all attacks on infrastructure. Furthermore, cyberwar is often understood as "the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state."[7] Nonetheless, cyber power is also "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain."[8] Daniel Coats, former U.S. director of national intelligence, declared in January 2019 that cyber operations not only threaten infrastructure but also exercise mental pressure on American citizens.[9] As stressed by the Russians, the main battlefield is human consciousness, perceptions, and strategic calculations.[10]

Chinese scholars Qiao Liang and Wang Xiangsui maintained that "the expansion of the domain of warfare is a necessary consequence of the ever-expanding scope of human activity, and that the two are intertwined," and we are witnessing this in what is called *cyberization* of international relations.[11] Cyberization is defined as "the ongoing penetration of all different fields of activity of international relations by different mediums of the cyberspace on the one hand, and the growing dependence of actors in international relations on infrastructure, instruments, and means offered by the cyberspace on the other hand."[12] In addition, with the growing number of people connected to the internet (more than 4.3 billion people or 56 percent of world's population), cyberspace is today considered as the fifth domain of warfare.[13] Despite this observation, no consensus has been reached on a definition for cyberspace. For the purpose of this article, the authors chose Daniel T. Kuehl's definition of cyberspace, which is "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify,

(Photo [*left*] by Life on white, Alamy Stock Photo. Photo [*right*] by Robert Eastman, Alamy Stock Photo) exchange, and exploit information via interdependent and interconnected networks using information-communication technologies"; and the cyberspace description based on Martin Libicki's model of three layers: the physical layer (the hardware—tangible objects like computers, servers, routers, etc.), the syntactic or logical layer (software, protocols, etc.), and the semantic or cognitive layer (information and ideas).[14]

> A nation should be judged not simply by its military, economic, or diplomatic power but by a combination of all of three, as well as its scientific and technological base and its cultural influence.

The definition conundrum also exists for the term "cyberattacks." For instance, the *Tallinn Manual* (a study on international law's application in cyber conflict and cyber warfare) defines cyberattacks as attacks that are reasonably expected "to cause injury or death to persons or damage or destruction to objects," and the United States defines it as "actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires."[15] However, as the authors mentioned, cyber operations do not only threaten infrastructure but also perceptions. Therefore, in this article the authors adopt the following definition, which includes low-end attacks that do not reach the threshold of the use of force or armed attacks, considering a cyberattack as "[a]n act or action initiated in cyberspace to cause harm by compromising communications, information or other electronic systems, or the information that is stored, processed, or transmitted in these systems."[16]

As the authors mentioned earlier, the PRC has a global approach when it comes to cyber power, but it is also true when it comes to security. Indeed, when the Chinese write about their conception of security, it is often couched in terms of *zongheguojialiliang* (comprehensive national power). As explained by Cheng, "this concept argues that a nation should be judged not simply by its military, economic, or diplomatic power but by a combination of all of three, as well as its scientific and technological base and its cultural influence."[17] The 2015 Ministry of National Defence of the People's Republic of China's paper "China's Military Strategy" stresses the importance of national security and social stability and adopts a similar tone to its 2013 *Science of Military Strategy*, the first document in which the Chinese military publicly addressed cyber warfare from a holistic point of view.[18] These two documents emphasized that cyberspace has become a new and essential domain of military struggle in today's world. The People's Liberation Army (PLA) acknowledges that *informationization* (becoming information based) means more than just adding a layer of information technology but rather reevaluating the nature of the conflict. Since informationization has affected the global economy and society, it has also influenced the nature of war. Hence, from the Chinese perspective, war is a function of not just military forces and politics but also larger social, economic, and technological trends.[19]

In 2011, the PLA's glossary of military terms outlined "informationized warfare" as warfare where there are "networked information systems and widespread use of informationized weapons and equipment, all employed together in joint operations in the land, sea, air, outer space, and electromagnetic domains, as well as the cognitive arena."[20] This, once again, stresses the awareness that China has had for many years regarding the importance of linguistic, human, and psychological factors, whereas the United States has been mainly focused on infrastructure in modern time.[21]

Accordingly, the importance that China places on the cognitive domain is reflected in its concept of *san zhongzhanzheng* (three warfares), introduced in 2003: *xinlizhanzheng* (psychological warfare), *yulunzhanzheng* (public opinion warfare), and *faluzhanzheng* (legal warfare).[22] The aim of this concept, used in times of peace and war, is to "try to influence the public's understanding of conflict by retaining support from one's own population, degrading it in the opponent's population, and influencing third parties."[23]

Public opinion warfare is applied in various channels such as the media to disseminate information to a targeted audience, that is, enemy forces. It complements psychological and legal warfare by including the goal to dominate the venues jointly used in the three types of warfare.[24]

Legal warfare, at its most basic level, involves "arguing that one's own side is obeying the law, criticizing the other side for violating the law, and making arguments for one's own side in cases where there are also violations of the law."[25]

Finally, psychological warfare aims at influencing the opponent's way of thinking or behavior and consolidating friendly psychology. Like opinion warfare, it uses information and media to achieve political and military objectives.[26] Moreover, despite using nonmilitary means, it is considered as part of the broader concept of information warfare and has always been under the responsibility of the PLA.[27] Consequently for Chinese leaders, on the one hand, psychological warfare is about protecting the country from external influence to avoid a collapse of the Chinese Communist Party, while on the other hand, it is used to weaken open societies by disrupting their messages and proposing alternative narratives.

Protection of the Chinese Regime

Beijing well understands the importance of preventing states from trying to influence its population. The perfect example of how China is attempting to achieve this goal is its espousal of the concept of cyber sovereignty. The 2010 Information Office of the State Council's "White Paper on the Internet in China" states, "Within Chinese territory, the internet is under the sovereignty of China."[28] The concept of cyber sovereignty is based on two main principles: (1) banning unwanted influence in a country's "information space," and (2) shifting the internet governance from current bodies that include academics and the private sector to an international forum such as the United Nations that would imply a transfer of power to states alone. According to President of the People's Republic of China Xi Jinping, "respecting cyber sovereignty" implies

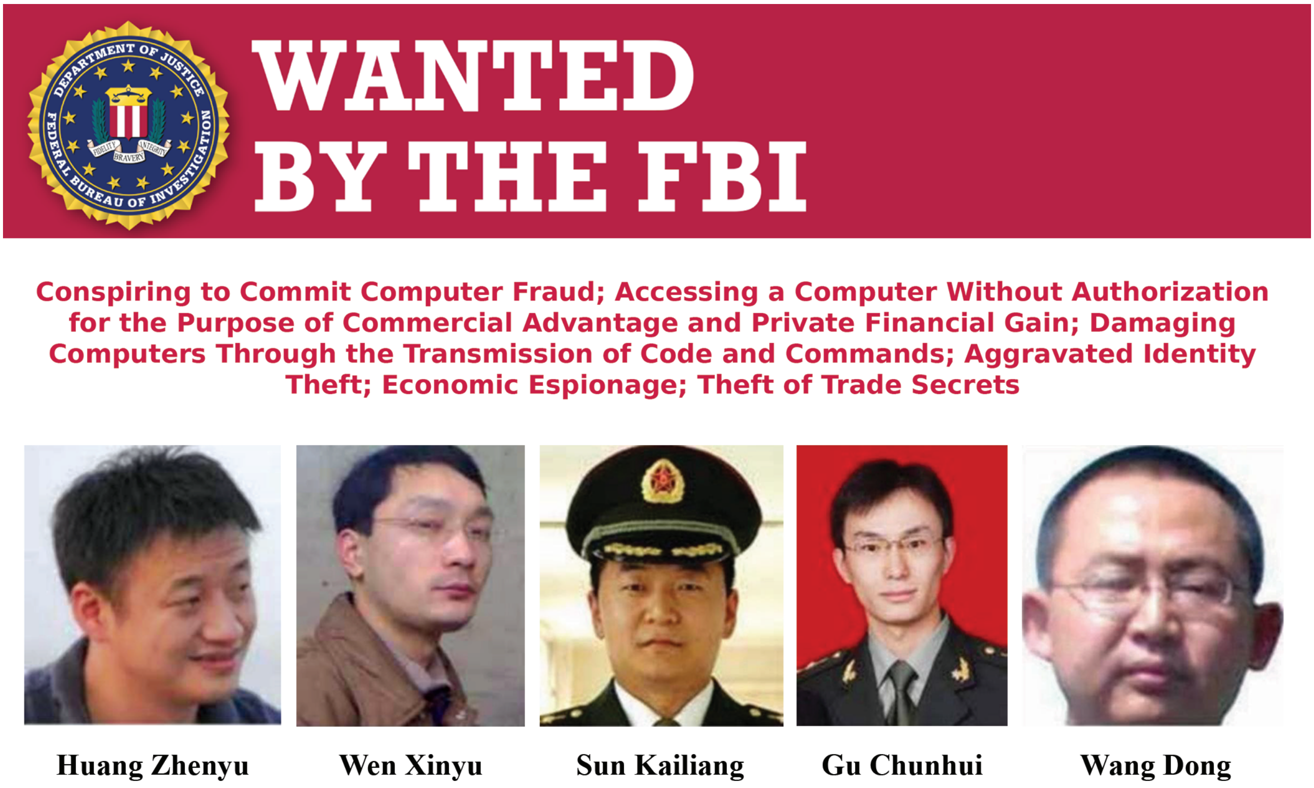
> respecting each country's right to choose its own internet development path, its own internet management model, its own public policies on the internet, and to participate on an equal basis in the governance of international cyberspace—avoiding cyber-hegemony, and avoiding interference in the internal affairs of other countries. … [We must] build a multilateral, democratic, and transparent governance system for the global internet.[29]

In Xi's statement, the key term is "multilateral." Contrary to the current multistakeholder approach to cyberspace, which is the "involvement on an equal footing of all actors with a vested interest in the internet including businesses and civil society," China vigorously defends the opposite idea, promoting the multilateral or intergovernmental internet governance that considers states as the principal decision-makers.[30] Moreover, cyber sovereignty was described in 2015 by Xu Lin, the head of the Cyberspace Administration of China at the time, as the difference between the multistakeholder approach and the multilateral approach.[31]

According to the principle of sovereignty defined in the 1928 Island of Palmas international law: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[32] On this basis, the sovereignty related to cyberspace is expressed as referent to the information infrastructure in a state's territory, airspace, and territorial waters and sea (including the seabed and subsoil); the direct consequence is that information infrastructure, regardless of their specific owners or users, are under the sovereignty of a country's judicial and administrative jurisdiction, which is protected by sovereignty.[33] Being one

Kimberly Orinx is a PhD candidate and teaching assistant at Université Catholique de Louvain, Belgium. Her research focuses on cyberspace and the China-Russia-United States triangle. She holds an LLM in international law from the Free University of Brussels and two master's degrees in international relations from Tongji University (Shanghai, China) and the Free University of Brussels.

Tanguy Struye de Swielande, PhD, is a professor of international relations at Université Catholique de Louvain, Belgium. He is the founder of the Genesys Network and the director of the Center for the Study of Crisis and International Conflicts. He is also a research fellow at the Egmont Institute and guest lecturer at the Belgian Royal Military Academy.



WANTED BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Huang Zhenyu | Wen Xinyu | Sun Kailiang | Gu Chunhui | Wang Dong

In May 2014, five Chinese military hackers were indicted by the United States on charges of computer hacking, economic espionage, and other offenses directed at six American victims in the U.S. nuclear power, metals, and solar products industries. This marked the first time criminal charges had been filed against known state actors for hacking.

of the "Five Principles of Peaceful Coexistence" developed in the 1950s, the sovereignty principle is at the bedrock of Chinese foreign policy.[34]

This cyber sovereignty concept is part of the larger term "information security," which in turn is critical for China to maintain its core values. Contrary to Western countries, which use the term "cybersecurity," China and Russia favor "information security," thus, highlighting fears concerning both the technical and cognitive dimensions of cyberattacks.[35] The concept developed by Beijing is, therefore, pertaining to its need to control the narrative. According to Mikk Raud, author of *China and Cyber: Attitudes, Strategies, Organisation*, "Ever since the internet became a publicly available communication platform in China, the question was not whether to control it, but rather how to control it."[36] Moreover, in a 2013 report commonly called "Document No. 9" (officially titled "Communique on the Current State of the Ideological Sphere"), the PRC claimed that "Western constitutional democracy is an attempt to undermine the current leadership and the socialism with Chinese characteristics system of governance" and asserted that Western universal values are "an attempt to weaken the theoretical foundation of the Party's leadership."[37] The last paragraph of the document also states, "We must reinforce our management of all types and levels of propaganda on the cultural front, perfect and carry out related administrative systems, and allow absolutely no opportunity or outlets for incorrect thinking or viewpoints to spread."[38]

In the 2015 *National Security Law of the People's Republic of China*, the Chinese government clearly shows its desire to control the political landscape and protect the Chinese Communist Party. In defining security in broad terms, the notion of security goes beyond the physical threats to the territory and encompasses the ideological sphere:

> National security refers to the relative absence of international or domestic threats to the state's power to govern, sovereignty, unity and territorial integrity, the welfare of the people, sustainable economic and social development,

> and other major national interests, and the ability to ensure a continued state of security. National security efforts shall adhere to comprehensive understanding of national security, make the security of the People their goal, political security their basis and economic security their foundation; make military, cultural, and social security their safeguard.[39]

Consequently, China protects itself from foreign influence by putting in place different regulatory mechanisms such as the so-called "Great Firewall," which was coined for the first time in a 1997 *Recorded Future* article in which a Communist Party official stated that the firewall was "designed to keep Chinese cyberspace free of pollutants of all sorts, by the simple means of requiring internet service providers to block access to 'problem' sites abroad."[40] This echoes the first principle of cyber sovereignty about the importance of banning "unwanted" influence in a country's information space.

From Disruption of the Western Narrative to an Alternative One

Since the Chinese know they are not yet competitive in the traditional domains, they advance their pawns on other chessboards. As Kenneth Geers wrote in his paper "Sun Tzu and Cyberwar": "Because cyber warfare is unconventional and asymmetric warfare, nations weak in conventional military power are also likely to invest in it as a way to off-set conventional disadvantages."[41] Therefore, in particular, Beijing invests in the "discursive chessboard" by developing alternative narratives and discourses to manipulate the interests and identities of Western societies.

With the growing importance of social media, the PRC government seized a strategic opportunity. According to studies, Americans "spend more than eleven hours per day on average 'listening to, watching, reading, or generally interacting with media,' and express varying levels of trust in the reliability of the information on social media."[42] With that in mind, Beijing is rumored to have hired people called *wumao dang* (50 Cent Party members) in order to conduct what might be called "reverse censorship."[43] They are supposed to post large numbers of fabricated social media comments as if they were the genuine opinions of ordinary Chinese people.[44]

This is an example of what is usually called "influence operations," which the RAND Corporation defines as "the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent."[45] More precisely, "influence cyber operations" encompass activities undertaken in cyberspace affecting the cognitive layer of cyberspace with the intention of influencing attitudes, behaviors, or decisions of target audiences.[46] These types of operations are about trust, not the truth.[47] However, the Chinese government has no scruples using this strategy. As Col. Qiao Liang of the PLA declared, "The first rule of unrestricted warfare is that there are no rules, with nothing forbidden."[48] In this context, the application of "overwhelming force" on the "decisive point" as determined by Antoine-Henri de Jomini is disruption of society: the civil population and the elites.[49] This concurs with Sun Tzu's thinking that "you can be sure of succeeding in your attacks if you only attack places which are undefended."[50]

Yet, democracies are little armed when facing "weaponized narrative," namely the "use of disinformation, fake news, social media, and other information and communication technologies to create stories intended to subvert and undermine an adversary's institutions, identity, civilization and will by creating and exacerbating complexity, confusion, and political and social schisms."[51] Furthermore, decreasing American and Western leadership, loss of trust in politicians, and increasing challenges to Western democracies have worsened the situation. Indeed, the Western narrative, with the return of populism in Western societies, is in a profound crisis; many citizens are consequently abandoning the narrative, finding refuge in alternative narratives, and being easily manipulated by foreign actors to change their schemata or mental maps, pushing people to extremes and making compromise almost impossible.

But for Beijing, it is not only about disrupting the Western narrative but also promoting a narrative of its authoritarian model. According to American political scientist Joseph S. Nye Jr., "The countries that are likely to be more attractive and gain soft power in the information age are those with multiple channels of communications that help to frame issues, whose dominant culture and ideas are closer to prevailing global norms, and whose credibility is enhanced by their domestic and international values and policies."[52] Thus, China strives to be more influential by developing new narratives. Since 2014, Beijing has hosted the World Internet Conference, also known as the Wuzhen Summit, in Wuzhen, China. This conference gathers officials and CEOs from all around the world and aims at legitimizing the Chinese vision of cyberspace and promoting international norms in China's view.[53] As noted by Adrian Shahbaz's article "The Rise of Digital Authoritarianism," China has "hosted media officials from dozens of countries for two- and three-week seminars on its sprawling system of censorship and surveillance."[54] "Digital authoritarianism" is being encouraged "as a way for governments to control their citizens through technology, inverting the concept of the internet as an engine of human liberation."[55] Thus, China is increasingly defending and promoting its authoritarian model and is willing to export "socialism with Chinese characteristics," therefore, proposing an alternative to the liberal model. To this end, it strengthens its discursive power by proposing new ideas, concepts, and institutions in order to strengthen the control of the regional and the international agenda-setting at the political, economic, and security levels. This is how Beijing persuades other states to adopt its vision of the world order (with some success already in regions of Africa, Central Asia, and the Middle East).

Building on what has been developed, China has become an "entrepreneur of identity" who recruits followers "by encouraging some identities and marginalizing others" and consequently fashioning identities to manage and manipulate the consent: power successfully employed without the sanction of the reason or the conscience of the obedient.[56] It is what Pierre Bourdieu called the power of suggestion.[57] This is characterized by subjectification:

> If structuration practices are internalized through constant repetition, social actors are constituted who feel compelled to respond in a particular way to certain stimulus … A highly disciplined socialization has the potential to deliver highly predictable social subjects who respond like automatons based upon socialization through repetition and rote learning.[58]

By encouraging reproduction and routine, standards, and predictability, states are socialized into compliance.[59] The more China is able to have followers sharing a common social identity, the more the balance of power in Chinese favor will become a reality. Of course, these are long-term policies and require strategic patience because people's minds change only over time, and they are complementary to the other determinants of power. Nonetheless, through (but not only through) cyber technology, the Chinese have been able to enforce "coordinated actions, messages, images, and other forms of signaling or engagement intended to inform, influence, or persuade selected audiences in support of national objectives," whereas the American narrative under the Trump administration has been characterized by "information fratricide."[60] The United States could lose the battle for hearts and minds if it does not change its course. As American environmental scientist Braden Allenby notes:

> No great power stays great without its exceptionalism narrative, and the U.S. narrative needs rebooting. Persistent problems such as lack of economic mobility, smoldering racial tensions, and intolerance of immigrants cannot be ignored. A new U.S. exceptionalism, one that fits a far more complex world and prepares citizens for living and working in periods of unprecedented technological and concomitant social and economic change, is required. In short, if the Shining City on the Hill is to remain a beacon, its unifying narrative must be revived.[61]

Applying ancient strategists' principles such as Sun Tzu's idea of "mastering the enemy without fighting," China has well understood the potential of influencing the cognitive processes through cyber power. This art of influence, the interconnected nature of information, and the characteristics of cyberspace blurred the lines between war and peace with actions beyond normal peacetime competition but short of all-out war and made the clear distinctions between military and civilian almost impossible.[62] This gray zone, where the tools employed will remain short of high intensity, creates an interval in which strategic narratives and other influence tactics play a key role.[63]

These Chinese policies undermine the values, norms, and standards defended by the West and, consequently, the status and reputation of the United States.[64] If the United States and its allies do not develop a counternarrative, they could lose their dominant position because strategic narratives shape how order is conceived and play a role in the production of order and how it is maintained.[65] Being powerful without a convincing narrative will not be very helpful in the long term, and social networks are thus powerful instruments of influence. To build its counternarrative, the United States needs to formulate clear objectives, to know the ecosystem or environment (be it local, regional, or systemic),

> “The United States, with its allies, will have to guarantee an open internet and fight the tendency of cyber sovereignty in China, Russia, and developing countries: ‘The internet is the place where the great ideological battles will be won and lost.’”

to identify and target key actors, to determine communication relays to diffuse the message/arguments. Furthermore, the United States, with its allies, will have to guarantee an open internet and fight the tendency of cyber sovereignty in China, Russia, and developing countries: “The internet is the place where the great ideological battles will be won and lost.”[66]

Conclusion

To influence through propaganda, or in other words fake news, is not new, but the digitalization has accelerated and facilitated the process. Furthermore, China has raised barriers to external political and cultural influence in its country, while foreign open democratic systems have represented an opportunity for Beijing to take advantage of. By weakening democracies, China has made the Western model more fragile and less attractive, presenting its authoritarian model as a possible, if not more attractive, alternative.

The United States has seemed to realize, with delay, the influence strategy that China has been putting into place for many years. For example, in March 2018, the Asia and Pacific Subcommittee of the Foreign Affairs Committee dedicated a hearing titled “Responses to China’s Foreign Influence Operations,” in which they addressed several points including cyber sovereignty and the fact that Chinese operations are covert and coercive as “they seek to distract, manipulate, suppress, and interfere.”[67] Accordingly, it is time for the United States to adopt a more holistic approach toward cyber power. In a 1953 essay, philosopher Isaiah Berlin differentiated hedgehogs from foxes.[68] The hedgehogs see the world through only one lens, exactly how the U.S. military until recently perceived “information operations as wartime activities which are led at the operational level.”[69] By contrast, foxes have a more complex view of matters, like China. In that respect, the Chinese developed a more inclusive or integrative strategy toward cyber power and “consider information counter-struggle as something conducted during peacetime and a strategic-level activity executed by the whole society.”[70]

In conclusion, while the expression of power includes coercion and threats, it is not limited to them. Empowering followers is necessary to gain and maintain power and influence. In that sense, the lasting power is also reliant on storytelling. And here lies the problem: the United States has lost its narrative leadership and its discursive power, even in the cyber and social network domains. Countering the Chinese threat to American hegemony requires a massive mobilization of societal resources and their connectivity to support and defend an inclusive grand strategy. Such effort, lacking today, is essential to influence others’ behavior. As explained above, the United States’ traditional view of military and economic capacities as the Nation’s main strengths has been expanded to other components. The lack of discursive and narrative power impacts status recognition and, ultimately, American leadership, and influence on the world stage. ■

Notes

[1] Charles Krauthammer, “The Unipolar Moment,” *Foreign Affairs* 70, no. 1 (1990/1991).

[2] The White House, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 25.

[3] Joseph S. Nye Jr., *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books, 1990), 27–28.

[4] Eric Delbecque, *L’influence ou les guerres secrètes* (Paris: Vuibert, 2011), 17.

[5] Adrian Shahbaz, “The Rise of Digital Authoritarianism,” in *The Rise of Digital Authoritarianism* (New York: Freedom House, October 2018), 7.

[6] “Munich Security Report 2017: Post-Truth, Post-West, Post-Order?” (Munich: Munich Security Conference, 2017).

7. Craig B. Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?," in *Cyberspace and International Relations: Theories, Prospects, and Challenges*, ed. Jan-Frederik Kremer and Benedikt Müller (New York: Springer, 2014), 23.

8. Joseph S. Nye Jr., *Cyber Power* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010), 3–4.

9. *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Before the Senate Select Committee on Intelligence*, 116th Cong. (29 January 2019) (statement of Daniel R. Coats, Director of National Intelligence), 5.

10. Dmitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," Proliferation Papers No. 54 (Paris: Institut Français des Relations Internationales, November 2015), 26, accessed 10 June 2019, https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

11. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Beijing: People's Liberation Army Literature and Arts Publishing House, 1999), 189.

12. Kremer and Müller, *Cyberspace and International Relations*, xi.

13. "Internet Users in the World by Regions – March 2019 – Updated," Internet World Stats, 31 March 2019, accessed 1 May 2019, https://internetworldstats.com/stats.htm; Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009).

14. Kuehl, "From Cyberspace to Cyberpower"; Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, 1st ed. (Cambridge, UK: Cambridge University Press, 2007), 236–37.

15. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press, 2013), 106; Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: U.S. Government Publishing Office, 8 June 2018), GL-4.

16. "Report on Cyber Defence Taxonomy and Definitions," 6200 TSC FCX 0010/TT-10589 (Brussels: North Atlantic Treaty Organization, n.d.).

17. Dean Cheng, *Winning without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response* (Washington, DC: The Heritage Foundation, 26 November 2012), 1.

18. *China's Military Strategy* (Beijing: The State Council Information Office, 26 May 2015), accessed 14 February 2019, eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm; *The Science of Military Strategy 2013* (Beijing: The Academy of Military Science of the People's Liberation Army, 2013), accessed 2 March 2019, https://fas.org/nuke/guide/china/sms-2013.pdf.

19. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, CA: Praeger, 2017), 37.

20. Ibid., 39.

21. *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), accessed 2 March 2019, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

22. Cheng, *Winning without Fighting*, 3.

23. Ibid.

24. Ibid., 2.

25. Han Yanrong, "Legal Warfare: Military Legal Work's High Ground: An Interview with Chinese Politics and Law University Military Legal Research Center Special Researcher Xun Dandong," *Legal Daily (PRC)*, 12 February 2006.

26. Cheng, *Cyber Dragon*, 45.

27. Guo Yanhua, *Psychological Warfare Knowledge* (Washington, DC: National Defense University Press, 2005), 10.

28. "White Paper on the Internet in China" (Beijing: The Information Office of the State Council, June 2010), accessed 18 March 2019, http://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm.

29. "Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference" (China: Wuzhen, 16 December 2015), accessed 18 March 2019, https://fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml.

30. Mikk Raud, *China and Cyber: Attitudes, Strategies, Organisation* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016), 15; Franz-Stefan Gady, "The Wuzhen Summit and the Battle over Internet Governance," *The Diplomat* (website), 14 January 2016, accessed 4 April 2019, https://thediplomat.com/2016/01/the-wuzhen-summit-and-the-battle-over-internet-governance/.

31. Gady, "The Wuzhen Summit and the Battle over Internet Governance."

32. "Reports of International Arbitral Awards: Island of Palmas Case (Netherlands, USA)," vol. II (New York: United Nations, 4 April 1928), accessed 18 March 2019, http://legal.un.org/riaa/cases/vol_II/829-871.pdf.

33. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 25.

34. Jean-Pierre Cabestan, *La Politique Internationale de la Chine: Entre Intégration et Volonté de Puissance* (Paris: Presses de Sciences Po, 2015), 75.

35. Julien Nocetti, "Géopolitique de la Cyber-Conflictualité" [Geopolitics of the Cyber-Conflict], *Politique Étrangère* [Foreign Policy] 2 (2018): 24.

36. Raud, *China and Cyber*, 6.

37. "Document 9: A ChinaFile Translation—How Much is a Hardline Party Directive Shaping China's Current Political Climate?," ChinaFile, 8 November 2013.

38. Ibid.

39. *National Security Law of the People's Republic of China* (Beijing: Ministry of National Defence of the People's Republic of China, 2015), accessed 20 March 2019, http://eng.mod.gov.cn/publications/2017-03/03/content_4774229.htm.

40. Insikt Group, *Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion* (Washington, DC: Recorded Future, 6 March 2019), accessed 15 April 2019, http://go.recordedfuture.com/hubfs/reports/cta-2019-0306.pdf.

41. Kenneth Geers, *Sun Tzu and Cyberwar* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 9 February 2011), 5.

42. Insikt Group, *Beyond Hybrid War*, 14. The report cites the *The Nielsen Total Audience Report: Q1 2018* as the source for media usage information.

43. Ibid., 12.

44. Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review* 111, no. 3 (2017): 497.

45. "Information Operations," RAND Corporation, accessed 18 April 2019, https://www.rand.org/topics/information-operations.html.

46. Pascal Brangetto and Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," in *8th International Conference on Cyber Conflict*, ed. Nikolaos Pissanidis, Henry Roigas, and Matthijs A. Veenendaal (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016), 113.

47. Žiga Turk, "Disinformation as a Political Weapon" (paper presentation, New Horizons Symposium - 2018, Brussels, 22 October 2018).

48. Liang and Xiangsui, *Unrestricted Warfare*, 2.

49. Craig B. Greathouse, "Cyber War and Strategic Thought," 28.

50. Sun Tzu, *The Art of War*, trans. Lionel Giles (London: Quarto, 2017), 18.

51. Braden R. Allenby, "White Paper on Weaponized Narrative" (Tempe, AZ: Arizona State University, June 2017), 1, accessed 7 June 2019, https://weaponizednarrative.asu.edu/publications/weaponized-narrative-white-paper-0.

52. Joseph S. Nye Jr., *Soft Power: The Means to Success in World Politics* (New York: PublicAffairs, 2004), 31.

53. Cameron F. Kerry, "Can China have Difficult Conversations about the Internet?," Brookings, 6 December 2018, accessed 7 June 2019,

https://www.brookings.edu/blog/techtank/2018/12/06/can-china-have-difficult-conversations-about-the-internet/.

[54] Adrian Shahbaz, "The Rise of Digital Authoritarianism," in *The Rise of Digital Authoritarianism* (New York: Freedom House, October 2018), 1.

[55] Ibid., 2.

[56] Bernd Simon and Penelope Oakes, "Beyond Dependence: An Identity Approach to Social Power and Domination," *Human Relations* 59, no. 1 (2006): 119; Markus Brauer and Richard Bourhis, "Social Power," *European Journal of Social Psychology* 36, no. 4 (2006): 604; as quoted by American political scientist Elmer Eric Schattschneider in John Gaventa, *Power and Powerlessness: Quiescence and Rebellion in an Appalachian Valley* (Oxford, UK: Clarendon Press, 1980), 9.

[57] Pierre Bourdieu, *Language and Symbolic Power*, ed. John B. Thompson (Oxford, UK: Polity Press & Basic Blackwell, 1991), 52.

[58] Mark Haugaard, "Rethinking the Four Dimensions of Power: Domination and Empowerment," *Journal of Political Power* 5, no. 1 (2012): 49.

[59] As quoted by Claus Mueller in John Gaventa, *Power and Powerlessness: Quiescence and Rebellion in an Appalachian Valley* (Oxford, UK: Clarendon Press, 1980), 18.

[60] Christopher Paul, *Strategic Communication Origins, Concepts, and Current Debates* (Santa Barbara, CA: Praeger, 2011), 3–4.

[61] Braden R. Allenby, "The Age of Weaponized Narrative, or, Where Have You Gone, Walter Cronkite?," *Issues in Science and Technology* 33, no. 4 (Summer 2017): 65–70.

[62] Oliver Fitton, "Cyber Operations and Gray Zones: Challenges for NATO," *Connections: The Quarterly Journal* 15, no. 2 (2016): 111–12.

[63] "Quadrennial Defense Review Report" (Washington, DC: Department of Defense, February 2010), 73; Adam Elkus, "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense," War on the Rocks, 15 December 2015, accessed 4 March 2019, https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/; Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: United States Army War College Press, December 2015). The concept of gray zone warfare is controversial in its essence. In official U.S. military doctrine, the concept of the gray zone appeared in the "Quadrennial Defense Review Report" in 2010 for the first time. The document states that ambiguities caused by the state of war and peace will constitute the challenge for the strategic security environment.

[64] Allenby, "The Age of Weaponized Narrative," 65–70.

[65] Alister Miskimmon, Ben O'Loughlin, and Laura Roselle, *Strategic Narratives: Communication Power and the New World Order* (London: Routledge, 2013), 28.

[66] Carla Hobbs, Andrew Puddephatt, and José Ignacio Torreblanca, "The Geo-Economics of the Digital," in *Connectivity Wars: Why Immigration, Finance and Trade are the Geo-Economic Battlegrounds of the Future*, ed. Mark Leonard (London: European Council on Foreign Relations, 2016), 117.

[67] *U.S. Responses to China's Foreign Influence Operations: Hearing Before the Subcommittee on Asia and the Pacific of the Foreign Affairs House of Representatives*, 115th Cong., 2nd sess. (21 March 2018), 4.

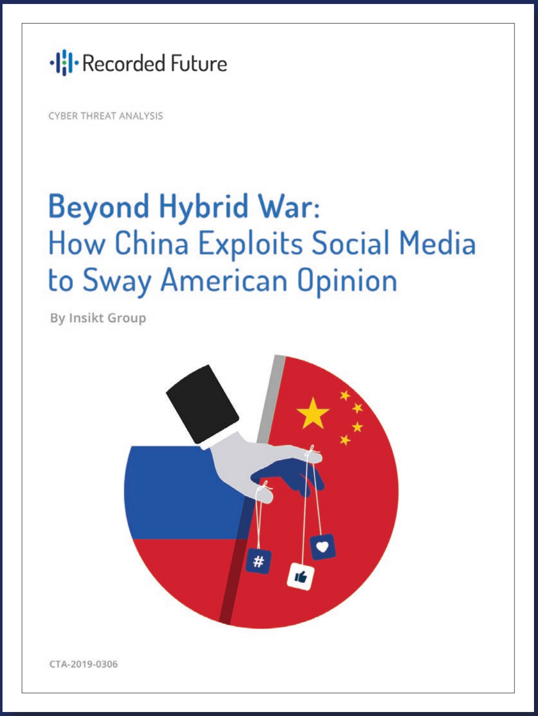
[68] Isaiah Berlin, *The Hedgehog and the Fox: An Essay on Tolstoy's View of History* (London: Weidenfeld & Nicolson, 1953).

[69] Piret Pernik, *Hacking for Influence—Foreign Influence Activities and Cyber-Attacks* (Tallinn, Estonia: International Centre for Defence and Security, February 2018).

[70] Ibid.

Military Review

WE RECOMMEND



Recorded Future

CYBER THREAT ANALYSIS

Beyond Hybrid War:
How China Exploits Social Media
to Sway American Opinion

By Insikt Group

CTA-2019-0306

Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion details research conducted by the Insikt Group on methods employed by diverse agents of the People's Republic of China to manipulate U.S. popular opinion through the use of sophisticated influence campaigns. This study compares the efforts of Chinese state-run social media influence operations with those of Russia. Differences in techniques are reputedly derived from China's distinctly different foreign policy goals and strategic global ambitions. The research details how the Chinese state employs a plethora of state-run media to exploit the openness of American democratic society to sow social and political discord while simultaneously promoting a utopian perception of the Chinese government and communist party by intentionally misrepresenting their character. To view the complete analysis, visit https://www.recordedfuture.com/china-social-media-operations/.