Chinese Definitions of Information Warfare

Since the 1990s, Chinese experts and theorists have been analyzing the concept of information warfare (*xinxi zhanzheng* 信息战争) with great interest. In fact, they started to offer definitions and insight into information warfare (IW) as early as 1985.
When the Gulf War broke out in 1991, Chinese military followed the progress of the war closely. In the post-war period, many military institutions in China devoted themselves to intensive study of the operations *Desert Storm* and *Desert Sword*, and considered them as marking the transition from the industrial age to the information age. As one Chinese officer observed, the Gulf War "compelled many Chinese strategists to realize the way of war-fighting was experiencing a fundamental transformation and a new form of military was about to emerge from the fading industrial age."[1] The Gulf War highlighted the growing centrality of IW, and it was used as the model for Chinese when studying future wars. Chinese interest in this area intensified further in the aftermath of the NATO air campaign over Kosovo.[2]

It is interesting to point out that most Chinese analysts understand IW as "information war" rather than "information warfare" as viewed by the Western thinkers. While American military experts consider IW as a way of fighting, Chinese specialists regard IW as the fight itself. In the words of the Chinese IW specialist Wang Pufeng, "information war refers to a kind of war and a kind of war pattern, while information warfare refers to a kind of operation and operational pattern."[3]

This paper seeks to offer an overview of the definitions of information warfare as formulated by the Chinese experts Shen Weiguang, Wang Pufeng, Wang Baocun, Liang Zhenxing, and Yuan Banggen.

Shen Weiguang

Dr. Shen Weiguang (沈偉光) put forward the concept of information warfare as early as 1985 by publishing a book entitled *Information Warfare* that was later excerpted as an article in *Liberation Army Daily*. Many consider him as the father of Chinese information warfare. However, Chinese IW doctrine did not achieve an analytical focus until the Gulf War in 1991.

In 1996, Shen has offered a definition of IW that was one of the first from a Chinese perspective. According to Shen:

> "In a military sense alone, information warfare refers to both side's attempt to gain the initiative of the battle through their control over information and flow of intelligence. With the support of information, both sides intend to comprehensively apply military deception, operational secrets, psychological warfare, and electronic warfare to destroy the enemy's information systems, block the flow of the enemy's information, and create false information to affect and weaken the enemies command and control capability. At the

[1] Wang Baocun, "China and the Revolution in Military Affairs." In: *China Military Science*, 4 (2001), 151.
[2] Yoshihara Toshi, "Chinese Information Warfare: A Phantom Menace or Emerging Threat?" Strategic Studies Institute, US Army War College, 2001, 1-42, 8-9.
[3] Khurshid Khan, "Understanding information warfare and its relevance to Pakistan," In: *Strategic Studies*, 32/33.4/1 (2012/2013), 138-159, 143.

same time, they must ensure that their command and control system is not damaged in the same way by the opponent."[4]

This initial definition did not address information dominance (制信息权 *zhixinxiquan*) (which is similar to the American concept of "information superiority") and information operations – just control. He listed the main tasks of IW as disrupting the enemy's cognitive system and its trust system, because "whoever controls information society will have the opportunity to dominate the world", he wrote in his book *The Third World War – Total Information Warfare*. Additionally, if a population loses faith in its government or military, the adversary has won.[5]

In 1999, Shen defined IW more broadly as involving two sides in pitched battle against one another in the political, economic, cultural, scientific, social, and technological spheres. War is fought for information space and resources. He also defined IW narrowly as the confrontation of warring parties in the field of information. The essence of IW, Shen believes, is to force your enemy to surrender without having to fight by using information superiority. This definition stresses superiority instead of control as was proposed in his 1996 definition of IW. To the Chinese expert, IW is not limited to times of conflict or crisis, but it is ongoing. Furthermore, Shen defined two types of war: the violent kind that occurs on the battlefield, and its non-violent opposite, which he defines as "deterrent war." While the violent type is temporary in duration and mostly limited in scale, the deterrent one occurs off the battlefield, taking up all the "space and time" not covered by violent war. In deterrent war, opposing forces are said to convert their power into information and deterrence.

Wang Pufeng

"In the near future, information warfare will control the form and future of war."

Prominent among IW specialists in China is Major General Wang Pufeng (王普丰), former Vice-President of the Academy of Military Sciences Beijing. In his seminal work *Information Warfare and the revolution in military affairs* (1995), Wang defined information warfare as follows:

"Information war is a product of the information age which to a great extent utilizes information technology and information ordnance in battle. It constitutes a "networkization" (*wangluohua* 网络化) of the battlefield, and a new model for a complete contest of time and space. At its center is the fight to control the information battlefield, and thereby to influence or decide victory or defeat."[6]

Later, the specialist elaborated his definition:

"Information war is a crucial stage of high-tech war… At its heart are information technologies, fusing intelligence war, strategic war, electronic war, guided missile war, a war of "motorization" (*jidong zhan*), a war of firepower (*huoli*) – a total war. It is a new type of warfare."

[4] Robert E. Neilson (ed.), *Sun Tzu and Information Warfare: A collection of winning papers from the Sun Tzu Art of War in Information Warfare Competition* (Washington, DC: National Defense University Press, 1997), 46.
[5] Timothy L. Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice from 1995-2003* (Fort Leavenworth, Kansas: Foreign Military Studies Office, 2004), 32.
[6] Wang Pufeng, *Information Warfare and the revolution in military affairs* (Beijing: Junkeyuan chubanshe, 1995), 37.

In his paper entitled "The Challenge of Information Warfare" (1995), Wang analyzed the way the US had used information technology to win battles. Wang urged the Chinese military, to "strive for an active approach in a reactive situation and use every means possible to destroy the opponent's information dominance and transform our inferior position in information."[7] Information dominance (*zhixinxiquan*) is a central component in IW, defined as the ability to defend one's own information while exploiting and assaulting an opponent's information infrastructure.

Wang Pufeng asserted that "warfare has shifted from ground warfare to even more intangible space, such as in electromagnetic fields." Communication is key in modern warfare, and the "C4I systems (communications, guidance, control, computers, and intelligence)" form the central nervous system. When dealing with information warfare, the goal is to "obtain timely information, to understand the enemy and ourselves". Wang also suggested that China should improve their arsenal in the hopes that the "enemy becomes terrified and worried, providing an image of an effective threat."[8]

In his discussion of IW in 2000, Wang further distinguished information war from information warfare: Information war refers to a kind of war and a kind of war pattern, while information warfare refers to a kind of operation and a kind of operational pattern.

Wang Baocun

Senior Colonel Wang Baocun (王保存), expert in IW at the Academy of Military Sciences, did an extensive analysis on the concept of IW.

In 1997, he divided IW into various components. He described the forms, nature, levels, distinctions, features and principles of IW. He listed forms of IW as peacetime, crisis, and wartime; the nature of IW as reflected in offensive and defensive operations; levels of IW as national, strategic, theater, and tactical; distinctions of IW as C2 (command and control), intelligence, electronic, psychological, cyberspace, hackers, virtual, economic, strategy and precision. He listed features of IW as complexity, limited goals, short duration, less damage, larger battle space and less troop density, transparency, the intense struggle for information dominance, increased integration, increased demand on command, news aspects of massing forces, and the fact that effective strength may not be the main target. He stated that the principles of IW were decapitation, blinding, transparency, quick response, and survival. His definition and analysis offered some of the most important insights into Chinese IW.

Chinese Views of Future Warfare, published in 1998, laid down the first useful foundations for understanding the Chinese perspective on information warfare. The article "Information Warfare" written by Wang Baocun and Li Fei (two senior PLA colonels at the time), has offered a more concrete Chinese understanding of IW:

[7] Simone Foxman, "Recent cyberattacks could be part of a Chinese military strategy started nearly 20 years ago," *Quartz*, March 14, 2013. Retrieved from https://qz.com/62434/recent-cyberattacks-could-be-part-of-a-chinese-military-strategy-started-nearly-20-years-ago/ (accessed March 9, 2022).

[8] Wang Pufeng, "The Challenge of Information Warfare." In: *China Military Science,* Spring 1995. Retrieved from https://irp.fas.org/world/china/docs/iw_mg_wang.htm (accessed March 10, 2022).

"IW is combat operations in a high-tech battlefield environment in which both sides use information technology means, equipment, or systems in a rivalry over the power to obtain, control, and use information. IW is a combat aimed at seizing the battlefield initiative; with digitized units as its essential combat force; the seizure, the control, and use of information as its main substance, and all sorts of information weaponry and systems as its major means."[9]

Wang and Li also described IW as consisting of five major elements and two general areas. The five elements are:

- Substantive destruction, the use of hard weapons to destroy enemy headquarters, command posts, and command and control information centers
- Electronic warfare, the use of electronic means of jamming or the use of antiradiation weapons to attack enemy information and intelligence collection systems such as communications and radar
- Military deception, the use of operations like tactical feints (simulated attacks) to shield or deceive enemy intelligence collection systems
- Operational secrecy, the use of all means to maintain secrecy and keep the enemy from collecting intelligence on our operations
- Psychological warfare, the use of TV, radio, and leaflets to undermine the enemy's military morale.

The two general areas are information protection (defense) and information attack (offense). Information protections means preventing the destruction of one's own information systems. Information attack refers to attacking enemy information systems.[10]

In his 1999 IW discussion, Wang Baocun distinguished between IW and informatized war, defining IW as a form of fighting and part of a complete war, and informatized war as an entirely new form of war. IW would gradually become informatized war, Wang described, but this would not be happening until the middle of the 21st century when informatized forces will be available. Wang's discussion included cognitive aspects of IW and again an emphasis on control.

Moreover, Wang focused on perceptions and beliefs as he described the perception structures, perception systems, and belief systems as IW components. He defined perception structures as "all things that an individual or a group considers correct or true, regardless of whether these things that are considered correct or true have been obtained through perception or belief." Perception structures referred to as composed of perception systems, "systems which are established and operated in order to understand or observe verifiable phenomena by turning such phenomena into perceptible realities and subsequently to make decisions or take action on the basis of intuitive understanding of such realities." Belief systems "guide testable empirical information and such information and consciousness that cannot be tested or are hard to test."

Liang Zhenxing

PLA expert Liang Zhenxing argued that information warfare included all types of war fighting activities that involve exploitation, alteration, and paralysis of an enemy's information

[9] Wang Baocun and Li Fei, "Information Warfare," in *Chinese Views of Future Warfare*, Michael Pillsbury (ed.), Washington, DC: National Defense University Press, 1997, 328.
[10] Wang and Li, "Information Warfare," 328-329.

and information systems, while protecting one's own information and information systems. Liang believed that the essence of IW is to render the operational space unclear or indistinct to enemy forces and transparent to one's own forces. This was one of the first Chinese definitions to highlight the defensive, as well as the offensive nature of IW.[11] Moreover, Liang stressed the importance of including Chinese characteristics in the Chinese definition of IW, but at the same time it also should be in line with the international definition.

Yuan Banggen

Yuan Banggen (袁邦根), Chief of General Staff Headquarters Communication Department and a member of the State Council Leading Group for Informatization Work, stated that IW is "the struggle waged to seize and keep control over information, and the struggle between belligerent parties to seize the initiative in acquiring, controlling and using information". Capitalizing and sabotaging the opposite party's information resources, information system, and informatized weapon systems is the method used. Moreover, Yuan defined information operations (IO) as specific IW operations. IW is the core of informatized warfare, whereas information operations are manifestation of information warfare on the battlefield. IO means information wars in the narrow sense, that is the military field, and they are normally integrated, high and new technology countermeasures. In his article, Yuan also discussed informatized forces and battlefields, which are two components of IW.

Conclusion

The Chinese IW experts mentioned in this paper have demonstrated a keen interest in understanding and defining the theoretical concepts necessary to conduct IW in future conflict. Even though the definitions of IW have varied and evolved over time, their analysis still represent the central starting point for current Chinese discussions on IW.

As noted earlier, Chinese definitions of IW dovetail closely with the notion of "information dominance". In fact, the aim of IW in the Chinese literature is to establish information dominance, the ability to establish control of information and information flow at a particular time and within a particular space. It entails the ability to collect more information, manage it faster, and employ it more precisely than the adversary.[12] The notion of disrupting the adversary's command and control capabilities is also central in the Chinese definitions of IW. The literature often presumes that locating and then successfully attacking the enemy's center of gravity is achievable. Another subtheme that emerges in the literature is the influence of Chinese strategic tradition, more precisely Sun Tzu's "The Art of War" (*Sunzi Bingfa* 孙子兵法). This demonstrates Chinese efforts to internalize IW within a familiar strategic framework.[13]

[11] Khan, "Understanding information warfare and its relevance to Pakistan," 144.
[12] Dean Chen, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (California: Praeger, 2017), 39-40.
[13] Toshi, "Chinese Information Warfare: A Phantom Menace or Emerging Threat," 14-15.

References

Chen, Dean. *Cyber Dragon: Inside China's Information Warfare and Cyber Operations.* California: Praeger, 2017.

Foxman, Simone. "Recent cyberattacks could be part of a Chinese military strategy started nearly 20 years ago." *Quartz,* March 14, 2013. Retrieved from https://qz.com/62434/recent-cyberattacks-could-be-part-of-a-chinese-military-strategy-started-nearly-20-years-ago/ (accessed March 9, 2022).

Khan, Khurshid. "Understanding information warfare and its relevance to Pakistan." In: *Strategic Studies*, 32/33.4/1 (2012/2013), 138-159.

Neilson, Robert E. (ed.). *Sun Tzu and Information Warfare: A collection of winning papers from the Sun Tzu Art of War in Information Warfare Competition*. Washington, DC: National Defense University Press, 1997.

Pillsbury, Michael (ed.). *Chinese Views of Future Warfare*. Washington, DC: National Defense University Press, 2002.

Thomas, Timothy L. *Dragon Bytes: Chinese Information-War Theory and Practice from 1995-2003*. Fort Leavenworth, Kansas: Foreign Military Studies Office, 2004.

Thomas, Timothy L. "Like Adding Wings to the Tiger: Chinese Information War Theory and Practice." Retrieved from https://community.apan.org/cfs-file/__key/docpreview-s/00-00-06-31-06/2000_2D00_10_2D00_01-Like-Adding-Wings-to-the--Tiger_2D00_Chinese-Information-War-Theory-and-Practice-_2800_Thomas_2900_.pdf (accessed March 5, 2022)

Toshi, Yoshihara. "Chinese Information Warfare: A Phantom Menace or Emerging Threat?" Strategic Studies Institute, US Army War College, 1-42, 2001.

Wang, Baocun. "China and the Revolution in Military Affairs." In: *China Military Science*, 4 2001.

Wang, Pufeng. *Information Warfare and the revolution in military affairs*. Beijing: Junkeyuan chubanshe, 1995.

Wang, Pufeng. "The Challenge of Information Warfare." In: *China Military Science,* Spring 1995. Retrieved from https://irp.fas.org/world/china/docs/iw_mg_wang.htm (accessed March 10, 2022).

Wang, Baocun and Li, Fei. "Information Warfare." In: *China Military Science,* June 1995. Retrieved from https://irp.fas.org/world/china/docs/iw_wang.htm (accessed March 10, 2022).