The Fifth Dimension of Combat Research—The Influence of Cyberspace in Information Warfare

Fang Yuan¹*, Hualiang Chen¹ and Junzhi Meng²

¹College of Information and Communication, National University of Defense Technology, Xi’an, China
²Railway Public Security Department, Xi’an, China

*Corresponding author. Email: 616747153@qq.com

Abstract. Cyberspace as the fifth dimension of combat, it has occupied a pivotal position in information operations. In this paper, the concept, composition and characteristics of the cyberspace operations are expounded in general, and the threats of cyber warfare are discussed. Finally, the enlightenment brought by cyberspace warfare is summarized.

Keywords: information warfare, cyberspace, cyberspace operations.

1. Introduction
Cyberspace, as the fifth largest area coexisting with land, sea, air and sky, is rapidly becoming a new battleground for conflicts between nations and the next border that needs to be protected in the name of national security. Since the United States proposed the cyberspace space, the cyberspace problem has attracted widespread attention in many countries around the world and has become a hot issue.

On May 29, 2009, President Obama’s speech at the White House’s release of the cyberspace policy review report clearly stated that cyberspace should be treated as a national strategic asset, and protecting the infrastructure would be a national security priority work¹. Since the United States proposed the cyberspace space, the cyberspace problem has attracted widespread attention in many countries around the world and has become a hot issue. Judging from the theory and practice of the cyberspace in the United States, the US military has begun to develop a series of development strategies for cyberspace and its operations, and is actively putting into action, and has achieved remarkable results.

The US Center for Strategic and International Studies (CSIS) released the US Cyber Security Progress Analysis Report in January 2011². The report believes that protecting the security of cyberspace has become an important challenge for US national security, but the United States is not prepared to respond. The analysis report shows how the United States relies on, but does not protect, the security posture of the cyberspace. Any country with global influence needs to rethink cyber security to accommodate this integrated global high-speed network.

Specific to the field of operations, the emergence of cyberspace has opened up an unprecedented new height and become a new high ground for the military. Whoever can seize the strategic commanding heights of the network electromagnetic space means who will control the system and the system. Some American scholars have pointed out that "the power of cyberspace in the 21st century is
as decisive as the mastery of sea power in the 19th century and the mastery of air supremacy in the 20th century." The cyberspace is becoming a new battlefield.

This paper expounds the connotation of cyberspace and discusses the threat of cyber warfare. Finally, it proposes the enlightenment and challenges brought by cyberspace and its operations.

2. Cyberspace overview
Cyberspace is an abstract concept in the field of philosophy and information.

In the literature, Professor Zhang Zhijun pointed out that the cyberspace is mainly a conceptual space, a spatial concept or a subjective space, rather than a physical space or a real space. This conceptual space is obviously not composed of a homogenous space in the real world, but consists of countless spaces that rapidly expand or rapidly shrink and have great differences in personality.

In 1984, American sci-fi writer William Gibson combined cyber and space into his cyberspace trilogy novel to become the word cyberspace. The novel describes the cyberspace where the network and human consciousness are integrated. This is the first place where cyberspace was born. It was meant to be a virtual space created by a computer information system that can be connected to the human nervous system. For more than 20 years, computer and network technology has developed rapidly, and cyberspace has gradually become a reality, and has become a "new world" generated in parallel with the material world based on computers, communication networks and electromagnetic space.

2.1. Cyberspace
Cyberspace is an area where cyberspace operations are part of information operations. It is not the same as the concept of information warfare proposed earlier. After entering the 21st century, the understanding of the connotation of cyberspace has been deepened. The new definition is: cyberspace is a global domain in the information environment, composed of interdependent information technology infrastructure networks, including the Internet and telecommunications. Nets, computer systems, and embedded processors and controllers. The cyberspace is the fifth dimension space after land, sea, air and sky. In the past, the fifth dimension space refers to the electricity space, or the electromagnetic space. In fact, cyberspace is a broader concept than electromagnetic space, and it contains Network system, so it is more scientific to replace electromagnetic space with cyberspace. According to this, the relationship between cyberspace and warfare concepts is shown in Figure 1.

![Figure 1. Relationship between cyberspace and warfare concepts.](image)

2.2. Characteristics
The cyberspace overlaps with the land, sea, air, and sky in the time domain and airspace. As the fifth-dimensional combat field, the cyberspace has its own characteristics.
High speed. Information is transmitted over the network in cyberspace and can reach the speed of light. Cyberspace provides a quick way to make decisions, quickly strike, and quickly realize battle expectations.

Open. The electromagnetic space and information network space are open, and anyone can enter the cyberspace and become a cyber person.

Mutagenicity. The cyberspace operations are not affected by time and distance, and can achieve battle effects in an instant. The cyberspace is constantly changing, and it is necessary to constantly adjust the cyber attack and cyber defense measures according to the battle situation.

3. Cyber battle: A real and growing threat
The US military and security agencies have long incorporated the concept of "information warfare" into military doctrine and warfare planning. John Alger, former dean of the School of Information Warfare and Strategy at the National Defense University, wrote that the information war "is designed to protect, exploit, destroy, and reject information or information resources in order to achieve a favorable position, goal, or victory against the enemy." In August 2006, the US Secretary of Defense instructed the information warfare to "protect the military decision-making from enemy attacks, affecting and reducing the enemy's decision-making ability. Thus gaining information superiority, resulting in my advantageous position. Information warfare directly serves the country. A security strategy that uses all elements of national power to influence the perception and behavior of the enemy in a synchronized and coordinated manner."

3.1. US and cyber security
The US government has long recognized the dangers of its information technology infrastructure vulnerability, and in recent decades, cybersecurity issues have risen with the world's major events and political situations. The cyber war was highly valued during the Clinton administration, but with the "9.11" time, the threat of terrorism replaced the cyber threat as the main threat. However, after the 2007 cyber war against Estonia, the US government seems to be taking this issue more seriously.

The Obama administration announced in February 2009 that it is launching a 60-day inter-agency review of various federal cybersecurity programs. Statements on this review show that they are taking this issue seriously: "The national security and economic health of the United States depends on the security, stability and integrity of our national cyberspace, whether in the public or private sector. The President believes We can uphold the rule of law and protect the right to privacy and civil liberties while protecting our country's critical network infrastructure."

In addition, the US military regards its offensive cyber warfare as its high degree of confidentiality, which needs to be highly valued by us. A report in the 2009 New York Times showed that "the United States has made tremendous progress in the maturity of cyber tactics." The report writes: The most peculiar innovation in the plan is to let the Pentagon programmers sneak into Russian or Chinese computer servers and destroy a "botnet" before it is released to the United States... or the US intelligence agency activates The malicious code secretly embedded on the computer chip allows the United States to seize the command of the enemy computer through remote control over the Internet. This is of course an attack that officials are worried about and that may be targeted at various targets located in the United States (usually through Chinese-made chips or computer servers).

3.2. Stuxnet: The first "network missile"
Stuxnet is a malware. It was first discovered in June 2010 and has since made a huge stir in the entire computer security community. Most malware is used by cybercriminals to steal data, such as credit card information and business plans, or to use computers to form botnets. Stuxnet was designed to silently destroy infected computers, making it a new and deadly malware that targets Siemens' software systems, designed for large industrial facilities such as nuclear power plants operating system.
Stuxnet sneaked into a computer and looked for a specific Siemens programmable logic controller (PLC) setting, a digital fingerprint. If the target has been found, then inject its own code into the operating system: if it is determined that the system is not its target, thenContinue to move without causing any harm. Once Stuxnet injects new code into the PLC device, it will cause some important aspects of the plant's systems to silently fail until damage is caused. It can be seen that Stuxnet will choose a very specific goal of the real world, "a cyber weapon that crosses the digital kingdom to the physical world and destroys certain things."

The emergence of Stuxnet shocked the world, and cyber security researcher Ralph Langer once said: Until a few days ago, people believed that such an attack was impossible... Stuxnet is a 100% cyber attack weapon designed to destroy the physical world. An industrial generation process.

3.3. Cyberspace weapon

Since the 1990s, a number of military and defense companies in the United States have begun research and development of Cyberweapons. The cyber weapons that they already have are divided into two categories. The first category focuses on reconnaissance or influence of enemy computer networks or communication networks. Its combat styles include virus implantation, denial of service, information tampering, network sniffing, malicious code, logic bombs, etc., for example, the US military The "Suter" system is capable of entering and attacking enemy computer networks and communication command systems by wireless means; the other is to combat or destroy enemy physical infrastructure for major warfare purposes, including high-energy microwave weapons, transients. Electromagnetic devices, microorganisms that are interested in integrated circuit chips, micro/nano robots that destroy circuits, and the like.

On September 6, 2007, eight Israeli warplanes escaped the Syrian Russian air defense radar network and raided the Syrian nuclear target. The Israeli Air Force launched the US-developed cyber warfare weapon Shute, which compares the acquired enemy information with the pre-established Syrian air defense system database through real-time reconnaissance. After confirming the error, it immediately injects "misleading" information and infiltrates. In the C^I of the Syrian air defense system, misleading algorithms and data are implanted to obtain completely false air information. The actual “highest threat level” is evaluated as “no threat”, thus misleading its air defense combat system. The conclusion of "nothing is safe". The essence of Shute technology is to mislead and control the network of enemy air defense systems. It is higher than destroying and destroying network components. It is not direct electronic interference or physical damage to the enemy air defense system, but it is hidden into the enemy air defense combat network system, which will mislead the algorithm. And the false data is implanted into the signal processing and communication system at the end of the enemy air defense information transmission system, so that the enemy can not get the attack target information and it is difficult to effectively counterattack, thus ensuring the completion of the combat mission.

"Shutter" is a highly confidential airborne electronic attack capability research project of the US Air Force, headed by the US Air Force Big Safari office. According to reports, the US military used the EC-130H, RC-135 and F-16 aircraft to perform the "Shutte 1" to "Shutte 5" demonstrations during the joint expeditionary exercises. "Shut 1" was demonstrated in 2000 to monitor what the enemy radar operator saw; "Shut 2" was demonstrated in 2002 to control enemy networks and command enemy sensors; "Shut 3" demo In 2004, links related to time-sensitive targets, such as battlefield ballistic missiles or mobile surface-to-air missile launchers; the "Shutte 5" demonstration was designed in 2008 to meet the Air Force's newly established Cyberspace Command. Mission requirements, providing a tactical-level battlefield space view that synchronizes dynamic, non-dynamic, and support operations against mobile, networked enemy systems. From the demonstration process, the attack ability of Shute is similar to hacker attack, intrusion, residency, surveillance, and control. It uses wireless injection, using high-power radiation sources such as SPEAR pod, AESA. Array implementation.
4. Cyberspace and its enlightenment to war
The United States attaches great importance to and develops cyberspace. It is not a temporary rise and a show. It is a strategic decision made by examining the cyberspace and profoundly understanding the cyberspace and its status from the overall perspective of its national security interests. Cyberspace combat is an inevitable outcome of the development of the information age to a certain stage. In the face of cyberspace operations, attention should be paid to actively responding and making a difference. The development priorities of cyberspace operations should be strengthened in conjunction with the relevant requirements of information operations.

4.1. Focus on the theory of cyberspace operations
The concept of cyberspace is a big thing for the future development of the country and the military, and must be given enough attention. At this stage, we will carry out research on cyberspace issues, and we will focus on two aspects: First, we must thoroughly study the basic connotation of cyberspace, and clarify its essence, mechanism of action, development trend, etc., and fully consider its The impact of traditional national and military security and development, and the corresponding countermeasures. Second, in combination with China's national conditions and military conditions, we deeply understand the challenges and opportunities that cyberspace brings to us, recognize the severe threats we face, and propose the guiding ideology, goals, supporting technologies, and strengths of cyberspace development. Construction, warfare use and other issues.

4.2. Focus on the cyberspace offensive target
Through electronic interference, anti-radiation strikes, directed energy weapons, cyber warfare to achieve physical strikes, repressive interference, deceptive interference, etc., can effectively destroy the cyberspace physical infrastructure and reduce the ability of enemy cyberspace to obtain external information, thus ensuring The cyber operation of the squad has been implemented smoothly. Attacking the key parts of the enemy cyberspace can play the role of “carrying the whole body”, so the target is mainly the key network nodes and equipment, such as the command post communication hub, the air communication relay platform, the communication satellite, etc. It can also use the electromagnetic pulse generated by high-power microwave weapons and electromagnetic pulse bomb explosion to instantly form super peak power, forcibly inject into the key electronic information system of enemy cyberspace, burn electronic components, and use suppressed electronic interference to disrupt communication of enemy wireless networks. Frequency bands; in addition, "Shuttle" technology can also be considered to attack enemy network systems.

4.3. Take effective measures to defend the cyberspace
Handle the relationship between cyberspace development and security, prevent re-development and neglect security; formulate and improve military regulations, and stipulate network electromagnetic space warfare tasks and battle guidelines in the military's information system-based system. Incorporate cyberspace operations into the joint military system of the whole army, promote the construction of joint operations capabilities, and establish a unified cyberspace battle leadership organization of the state and the military from a strategic level to centrally command operations and achieve unified planning and management of operations; The awareness of security precautions, the establishment and improvement of a network defense mechanism combining military and civilian integration, unified command and coordination, and ready to implement full spectrum network electromagnetic operations.

5. Conclusion
This paper analyzes and summarizes the development, concept, composition, characteristics, weapons, battle processes, information warfare with cyberspace, and the implications of cyberspace operations for military development. In the United States, the research, exploration and experimentation of cyberspace operations are fully carried out. In the process of gaining absolute superiority and control in
the field of cyberspace operations, the parties concerned must fully implement the "information system-based system combat capability to become the basic form of combat capability. The famous assertion. Information warfare has strong cross-correlation with cyberspace operations, and information warfare covers cyberspace operations. Therefore, the development of US cyberspace space combat sums up its enlightenment on military development, which is conducive to information warfare. Achieving greater information superiority has certain reference significance for information warfare.

References
[1] R. Oosthuizen, L. Pretorius. Assessing command and control system vulnerabilities in underdeveloped, degraded and denied operational environments[C]. Proc. of the 18th International Command and Control Research and Technology Symposium, 2013: 1–17.
[2] Fei Gao, Weixiang Gao, Wei Wang, et al. Simulation Modeling of Command and Control Process Based on Entity[J].Command Control and Simulation, 2012, 34(3): 116-120.
[3] Sun Liang. Thoughts on the Philosophy of Science in Cyberspace. School of Information, Shandong University of Science and Technology.
[4] Xuejun Yang, Jinshu Su. Reflections on China's Network Electromagnetic Space Security Strategy. National Defense Science and Technology, 2010(4).
[5] Singh Vivek, Singh Garima, Pande Suparna. Emergence, self-organization and collective intelligence-modeling the dynamics of complex collectives in social & organizational settings[C].//International Conference on Computer Modeling and Simulation, 2013.
[6] International Strategy For Cyberspace. Prosperity, Security, and Openness in a Network World.
[7] Zongpeng Shi et al. Analysis of the composition and characteristics of information space in modern warfare. Journal of Naval University of Engineering (Comprehensive Edition). Volume VII, Issue 4.