Bond University
ePublications@bond

EASSC Publications East Asia Security Centre

11-29-2013

The Semantics of Cyber Warfare 网络战的语义

Jason Fritz
Bond University, jfritz@bond.edu.au

Follow this and additional works at: http://epublications.bond.edu.au/eassc_publications

Part of the International Relations Commons

Recommended Citation
Jason Fritz. "The Semantics of Cyber Warfare 网络战的语义" East Asia Security Symposium and Conference 东亚安全座谈谈论会. Beijing. Nov. 2013.

http://epublications.bond.edu.au/eassc_publications/42

This Conference Paper is brought to you by the East Asia Security Centre at ePublications@bond. It has been accepted for inclusion in EASSC Publications by an authorized administrator of ePublications@bond. For more information, please contact Bond University's Repository Coordinator.

The Semantics of Cyber Warfare

网络战的语义

Jason Fritz
PhD Candidate
Bond University

Peer-reviewed Conference Paper
2013 East Asia Security Symposium and Conference
同行互评会议论文
2013东亚安全座谈谈论会
http://epublications.bond.edu.au/eassc_publications/

For information about this paper or the East Asia Security Symposium and Conference Peer-reviewed publishing site, please contact the Editor-in-Chief Jonathan H. Ping
想要了解关于论文、或东亚安全座谈讨论会同行互评出版地址的信息，请联系总编辑
乔纳森•H•平
jping@bond.edu.au

The Semantics of Cyber Warfare

Abstract: The study of cyber warfare in China suffers from the same excess of overlapping terminology as in English documents. This paper will analyze key cyber warfare terms from authoritative sources and show that all of them can be broken down into three fundamental branches that are common to both the People's Republic of China and the United States of America. The three branches are: Information Operations, Computer Network Operations, and Net Centric Warfare. Streamlined categorizing can aid the efficiency of research and improve inter-agency structure. Additional benefits include more accurate threat assessment, limiting media and public misunderstanding, and increasing transparency to forward cooperation, understanding, and trust.

Key Words: China, Computer Network Operations, Cyber Warfare, Electronic Warfare, Hacking, Information Operations, Information Warfare, Net Centric Warfare

网络战的语义

摘要：在中国，对网络战的研究与英文文件一样，饱受术语过度重叠之苦。本文将分析来源权威的关键网络战术语，并展示这些术语都可以分解为三个基本类别，在中国和美国都很常见。这三个类别分别是：信息战，计算机网络战，和网络中心战。简化归类可以帮助提高研究效率、改进机构间结构。其它有利之处还包括更精确的威胁评估、限制媒体和公众误解、增加透明度以促进合作、理解和信任。

关键词：中国，计算机网络战，网络战，电子战，黑客，信息战，信息战争，网络中心战

THE SEMANTICS OF CYBER WARFARE

Introduction

The People's Republic of China (China) and the United States of America (US) are both seeking protection from and advantage through cyberspace as the fifth domain of warfare.[1][2][3][4] With the growth in cyber warfare as a field of study, the amount of cyber related terminology has also grown. Examples of key terms prevalent in Chinese government and military literature include informationization (xinxi hua; 信息化), information confrontation (xinxi duikang; 信息对抗), system of systems operations (tixi zuo zhan; 体系作战), and integrated network electronic warfare (wangdian yitizhan; 网电一体战).[5]

Shen Weiguang, "who many consider the father of Chinese Information Warfare", criticized the US for not having a universal definition, yet he then proposed vague terms such as war in the information age, information fighting, information resources, information space, information territory, and information weapons.[6] Adding further to the confusion are the introduction of terms by other prominent Chinese authors such as masquerade technology, take home battle, technology aircraft carriers;[7] battlefield information environment, computer network space, digitized armed forces, direct information warfare, information supremacy, network forces, network psychological warfare;[8] informatized thought, informatized warfare, intangible war, media warfare, network people's war, and system attack warfare.[9] All of these have overlapping, unclear, contradictory, and/or missing elements, and their exact definition varies between authors.

---

[1] US-China Economic and Security Review Commission, "USCC 2012 Annual Report," November 2012, http://origin.www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf.

[2] Information Office of the State Council of the People's Republic of China, "The Internet in China (White Paper)," June 8, 2010, http://china.org.cn/government/whitepaper/node_7093508.htm.

[3] Information Office of the State Council of the People's Republic of China, "The Diversified Employment of China's Armed Forces (White Paper)," April 16, 2013, http://www.china.org.cn/government/whitepaper/node_7181425.htm.

[4] Whitehouse.gov, "Cyberspace Policy Review," May 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[5] Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," U.S.-China Economic and Security Review Commission, Northrop Grumman, March 7, 2012, http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf

[6] Timothy L. Thomas, Dragon Bytes (Fort Leavenworth, Kansas: US Government Printing Office, 2004), 32, 38.

[7] Ibid.

[8] Timothy L. Thomas, Decoding the Virtual Dragon (Fort Leavenworth, Kansas: US Government Printing Office, 2007), 117.

[9] Timothy L. Thomas, The Dragon's Quantum Leap (Fort Leavenworth, Kansas: US Government Printing Office, 2009).

In addition, both the US and China have multiple government and military agencies putting forward their own definitions and competing to take the lead in this field within their respective states. As a further complication, China in particular lacks transparency of endorsed cyber doctrines. This makes contemplating one definitive set of definitions problematic, as there are a multitude of them even within a single military branch.

This paper asserts that there are three fundamental branches of cyber warfare. Regardless of which name is attached to these branches, they are structurally distinct, and all previous terms can be placed within one of these three, thereby helping to bring clarity to this field of study. Rather than introduce new terms, this paper will use existing best-fit terms. These are: Information Operations (IO), Computer Network Operations (CNO), and Net Centric Warfare (NCW). These terms are US-centric; however they have the benefit of having been used extensively in authoritative open source material over a relatively long period of time.

This paper will use Chinese examples to illustrate their cross-cultural application. While the terms chosen may be open to debate, the category they denote below remains valid. As shown in Figure 1 and Table 1, their distinguishing characteristics are whether or not they are connected to the Internet, involve hacking, or involve traditional military hardware. These might seem like obvious distinctions, yet they remain absent from prominent definitions. It is important to note that the terms cyber warfare and information warfare will be considered interchangeable, and they represent the broadest term encapsulating the other three. Further, this paper will not delve into the pre-existing debate over the definitions of "hacking" and "cyber war" as this is discussed at length by other authors and these words have already entered common use by officials and the media.[10]

Figure 1: Linear Venn of Cyber Warfare Branches

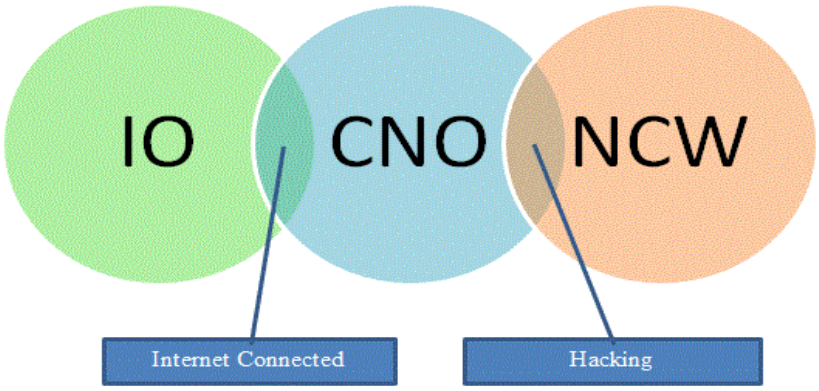


Table 1: Comparison of Cyber Warfare Branches

	Computer Networks	Internet Connected	Hacking	Military Hardware
IO	Yes	Yes	No	No
CNO	Yes	Yes	Yes	No
NCW	Yes	No	Yes	Yes

[10] Joseph Weiss, Protecting Industrial Control Systems From Electronic Threats (New York: Momentum Press, 2010).

Information Operations

IO as outlined here utilizes data that is publicly available on the Internet to one's advantage and does not involve hacking (unauthorized access). Examples of IO include media and information control, psychological operations (PSYOPS), propaganda, soft power, recruitment, and disinformation. More specifically, government agents who clandestinely promote online news articles and comments that portray their country or administration in a positive light fall under the category of IO. Terrorist group websites that post propaganda videos, attempt to recruit members through online means, or embed hidden data within a publicly available image file are also using IO. Shutting off portions of the Internet, filtering/blocking websites, monitoring user activity, using Internet activity for prosecutions, and censorship also fall under this category as long as no hacking was involved. In the case of China, the state has much more control over the Internet and requires less hacking. IO offers many opportunities for US-China cooperation and trust building such as restricting or monitoring tools used to aid terrorism and cyber bullying, or even working on methods to enhance domestic surveillance and management of a population during a crisis.

This categorization fits closely with a declassified 2003 document by the US Department of Defense, titled Information Operations Roadmap.[11] The Information Operations Roadmap includes CNO and Electronic Warfare (EW) by name. However, those two branches have continued to develop in their own right, and the novel portion of IO within the Information Operations Roadmap was the Internet PSYOPS and non-hacking operations. Using the term cyber PSYOPS would be too narrow to capture the essence of this branch, and the sometimes used term 'media and information control' is not as catchy or prominent. Other cyber related activities which fit the criteria for IO include piracy of multimedia and software, the cloning of popular websites, the Golden Shield/Great Firewall, and the Green Dam Youth Escort content-control software. Readily available free web sources, such as blogs, photo uploading, video uploading, podcasts, torrents, and social networking sites have given powers to individuals that were once restricted to large media outlets. Attempts to block these new forms of distribution were seen during the 2009 Ürümqi riots, the 2008 Tibetan unrest, the 2003 SARS outbreak, and numerous local protests. Conversely, online users are increasingly volunteering to enter large amounts of personal data which can, and have been, used for prosecutions.

Computer Network Operations

CNO includes computer network attack (CNA), computer network defence (CND), and computer network exploitation (CNE). The defining characteristics of CNO are hacking into a computer or network, via the Internet. If those two criteria are met, the remainder of the definition is fairly consistent amongst authors. CNA includes the ability to disrupt, deny, degrade, deceive, or destroy, and it utilizes traditional hacker tools like DDoS, viruses, worms, Trojans, and so forth. CND is defending against attack or exploitation, and can include digital forensics. By the definition given thus far CND debatably fits the criteria for IO; however it is more firmly rooted in CNO and is widely considered to be a component of CNO. Opportunities for US-China cooperation and trust building that align more closely with CND than IO include combating spam, botnets, malware, and organised crime. CNE is typically theft, eavesdropping, and setting up for an attack. Examples of CNE that China has

[11] US Department of Defense, "Information Operations Roadmap," October 30, 2003, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

been accused of include Titan Rain, Operation Aurora, and GhostNet.[12][13][14] Closed networks which are hacked into, but do not directly involve military hardware, are an example of CNO. This includes military and intelligence closed networks such as the US NIPRNet, SIPRNet, and JWICS. The term closed network is applied loosely here as more open source research is needed to determine exactly how separate these networks are from the Internet. These are highly secure networks; however they appear to be remotely accessible, use much of the same infrastructure as the Internet, and are vulnerable to traditional hacking tools. Further, while they aid in military operations, they serve a much larger role than being a part of a weapon system.

Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems are also semi-closed networks that fit most appropriately in the branch of CNO. These computer networks are responsible for electricity distribution, nuclear power, waste management, and water treatment. The technical specifications for ICS hacking is different than that of traditional hacking, however it shares much more in common with CNO than it does with the military hardware of NCW. The Stuxnet and Flame worm incidents belong to this subcategory of CNO. USB drives were used to infiltrate the closed network, but once that was complete the attackers were able to remotely update and exfiltrate data from computers located in foreign countries, meaning there was at least the capability of Internet connectivity prior to the infiltration. A truly closed network would have no wireless transmission and share no physical connections to broader Internet infrastructure. Further, while some of these networks are at least semi-closed off from the Internet, many are not. Outside of cyber warfare, ICS and SCADA belong to a category known as critical infrastructure. Other critical infrastructure such as banking, transport, public health, emergency services, and civilian communication are much more firmly rooted in the Internet, and therefore fall under the CNO category when hacked. It feels appropriate to keep ICS and SCADA together with the rest of critical infrastructure in cyber warfare categorization.

Net Centric Warfare

NCW refers to advanced military weapons systems, communication, and situational awareness that utilize closed computer networks (sometimes called air-gapped). This means that they can be hacked into, however not through the Internet. Examples of NCW include military unmanned aerial vehicles (UAV) and satellites or EA-6B Prowlers attempting to jam enemy radar and disrupt specific improvised explosive devices. NCW is close enough with other terms to be considered synonymous. These terms include EW, Future Combat Systems (FCS), information confrontation, informationization, Integrated Network Electronic Warfare (INEW), Revolution in Military Affairs (RMA), and 'utilizing (or dominating) the full electromagnetic spectrum'. The electromagnetic spectrum includes things which are technically relevant to CNO, since it includes Wi-Fi and all that is visible to the human eye;

[12] Krekel, Adams, and Bakos, "Occupying the Information High Ground"
[13] Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network," Scribd, March 29, 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.
[14] Information Warfare Monitor, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," Shadowserver Foundation, April 6, 2010, http://www.nartv.org/mirror/shadows-in-the-cloud.pdf.

however authors are typically referring to NCW.[15] It includes radio waves, microwaves, infrared, ultraviolet, and X-rays, used for military communication, radar, weaponry, and situational awareness. Examples of EW that fall outside the realm of military targets also exist; however articles that mention EW in a cyber warfare context rarely note these cases. EW is most commonly noted as an attack element within NCW. Therefore, in the interest of bringing clarity to the vast amount of literature it is better to simply note special cases as they occur. Anti-access Area Denial (A2/AD) is also predominantly NCW.[16][17] Radar, over the horizon targeting, ship destroying missiles, stealth bombers, and jamming satellites all belong to NCW. Some individual components of A2/AD might be CNO, such as hacking into NIPRNet to disrupt force deployment,[18] but the majority of A2/AD components frequently discussed in articles are firmly NCW. On the other hand, embedding backdoors into microchips during manufacturing or embedding backdoors into infrastructure during construction belong to either CNO or NCW depending on which it is targeting.[19][20]

NCW is not only hacking into advanced military weapons and C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), but also the use of those systems. 'Military hardware' itself is a vague term as the computers used in CNO could be considered military hardware. However, military hardware here is referring to the advancement of traditional battlefield equipment. For example, tangible items which are used to deliver a physical strike like jets, missiles, and tanks, and the systems that are closely linked to their operation. There is some grey area here, since CNO is capable of causing physical destruction. However, this is uncommon in CNO and seems out of step with traditional military hardware. It is not as clear cut as the purpose of a tank on a battlefield. The tank might require computer networks to operate and communicate on some levels, but those are closed networks used by soldiers, and the tank is integral. Further, a remotely located UAV ground control station blurs the line of the battlefield, yet its purpose is clearly linked to military action if it is being used in military operations.

---

[15] US Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013," May 2013, http://www.defense.gov/pubs/2013_china_report_final.pdf

[16] Andrew F. Krepinevich, "Why AirSea Battle?," Center for Strategic and Budgetary Assessments, February 2010, http://www.csbaonline.org/publications/2010/02/why-airsea-battle/.

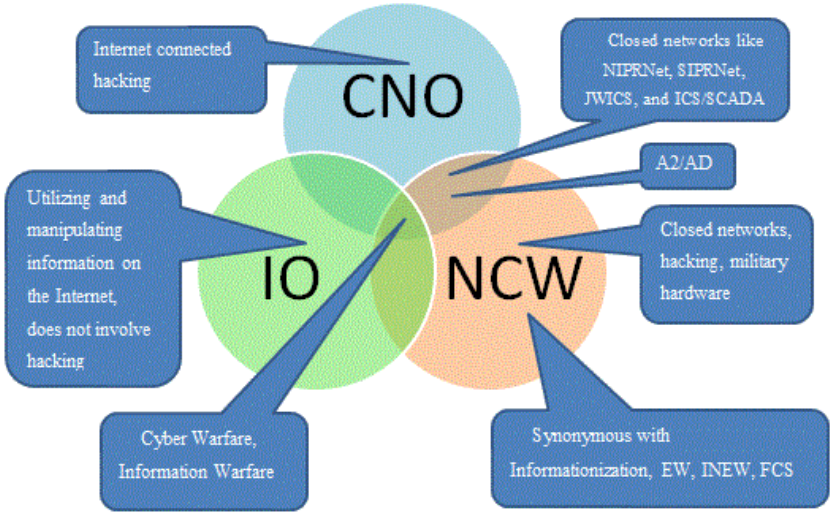
[17] Jan van Tol, Mark Gunzinger, Andrew F. Krepinevich, and Jim Thomas, "AirSea Battle: A Point-Of-Departure Operational Concept," Center for Strategic and Budgetary Assessments, May 18, 2010, http://www.csbaonline.org/publications/2010/05/airsea-battle-concept.

[18] Qiao Liang and Wang Xiangsui, Unrestricted Warfare, (Beijing: PLA Literature and Arts Publishing House, February 1999), http://www.cryptome.org/cuw.htm.

[19] Mike Rogers and Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," US House of Representatives, October 8, 2012, http://intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf

[20] John J. Tkacik, Jr., "Trojan Dragons: China's Cyber Threat," Heritage Foundation, February 8, 2008, http://www.heritage.org/Research/asiaandthepacific/bg2106.cfm.

Figure 2: Venn of Cyber Warfare with Select Callouts



Conclusion

The three branches of cyber warfare are Information Operations, Computer Network Operations, and Net Centric Warfare as displayed above in Figure 2. Key distinctions between them are whether or not they are: connected to the Internet, involve hacking, or involve military hardware. All three branches can be used in combination, as well as in combination with physical acts, yet their differences and the scope of this field warrant classification. Further research and promotion of these branches is needed to consolidate the plethora of English and Mandarin cyber warfare terminology. This will allow the study of cyber warfare to move forward as a whole, rather than be a continual process of introducing old ideas under new names. Additionally, it might reveal novel ideas that were initially lost in the crowd. These categories will also help new researchers limit the scope of their work by bringing order to a diverse range of cyber incidents and topics. Similarly it can aid in the decision of which government and military agencies should take the lead in different aspects of this emerging field and how they might coordinate their efforts. For international relations, promulgation of these categories can limit public misunderstanding, increase transparency, and reveal areas for mutually beneficial cooperation.