



A Russian Military Look at the Personnel Factor in Chinese Information Warfare Development

OE Watch Commentary: According to assessments by Russian General Staff analysts, the Chinese approach information warfare with some key principles. These include targeting the power supply of the server system or “master computer,” striking command and control systems and their various network components, “artificially overload[ing]” the adversary’s network to get direct control of the information flow, and software attacks in the form of viruses and unauthorized access. While their findings were not startling, the Russian analysts saw an emphasis on personnel and described the Chinese military and political leadership’s consistent and practical “steps to organize and conduct information warfare” with “personnel training, operational training, and direct conduct of and counter-action against information and psychological operations” on a “digital battlefield” that required “IT-savvy troops.”

According to the article, China has three categories of service members that are designated to become qualified in “information domination.” The first category is the highest command level of the PLA, who would have a focus on study of fundamentals of information technologies and IW concepts. The second category are PLA commanders, who study principles of information systems and the “forms and methods” (a key field of study in Russian military science) of conducting information warfare. The last category are officers, who know fundamentals of computer technology and programming, and are trained longer and more in depth on strategy, forms and methods, and applications.

It is interesting that the Russian analysts paid particular attention to age differentials of each group: over 40 for the first group, 30-40 for the second, and “generally 30 years of age or under” for the third group.

The Russian analysis also noted that Chinese information warfare specialists were trained in a number of centers including the PLA’s Communication Command Academy, the Information Engineering University, the Science and Engineering University and Tianjin University. Adding to this, according to the article, the PRC government recruits competent specialists from Chinese civilian, military, and state security institutions and from those Chinese who were educated abroad.

To ensure the loyal quality of the personnel developed for Chinese IW, the Russians stated that, through Communist Party control of the information infrastructure and mass media, the PRC is developing a “system of organized information” designed to “impact on the consciousness and minds of servicemen and civilians.” The Russian analysts believed that the Chinese considered this systemic psychological approach as a “key element of [China’s] military might.”

The Russian analysis also makes clear that the goal of their neighbor and putative partner is superiority and dominance in the information domain. **End OE Watch Commentary (Wilhelm)**



Vintage Chinese propaganda poster, showing the PLA. The caption reads, “The People’s Army is invincible”. The pilot (on top) holds a flagstaff and a copy of “Selected Works of Chairman Mao Zedong.”

Source: Wikimedia, https://en.wikipedia.org/wiki/File:Peoples_army.jpg#/media/File:Peoples_army.jpg, Fair Use

“...In order to prevail in information warfare, the Chinese military analysts believe that two important elements need to be created: a digital battlefield and IT-savvy troops.”



Continued: A Russian Military Look at the Personnel Factor in Chinese Information Warfare Development

Source: Р.А. Полончук, Т.А. Ганиев (R.A. Polonchuk, T.A. Gantiev), “Взгляды китайских военных специалистов на сущность и содержание информационной войны в современных условиях (Views of Chinese Military Experts on the Nature and Content of Information Warfare Today),” *Военная Мысль [Military Thought]*, No.3, 2020, p. 133-139.

The Chinese media report that the PRC’s military and political leadership has been consistently taking practical steps to organize and conduct information warfare in three main areas:

- *personnel training;*
- *improvement of the forms and methods of information warfare during CPLA operational and combat training;*
- *direct conduct of and counteraction against information and psychological operations.*

An analysis of Chinese military periodicals leads to the conclusion that a special training program for three categories of servicemen has been developed to train qualified personnel in information domination.

Category one is the highest command level of the CPLA. These are generally individuals over the age of 40. The main objective of their training is to study the fundamentals of information technologies and the concepts of conducting information warfare.

Category two is the commanders of the forces and units of the Chinese armed services. These are primarily individuals aged 30 to 40 years. The main objective of their training is to study the forms and methods of conducting information warfare, as well as to study the basic principles of the functioning of information systems.

Category three is the commissioned officers, who know the fundamentals of computer technology and programming and are generally 30 years of age or under. The main objective of their training is to study in depth the strategy, forms and methods of conducting information warfare, followed by their application in crisis situations. The training period for this group is longer than that of the first two groups.

The study program of each of the categories also includes the following topics to a greater or lesser degree:

- *strategy and tactics, methods and means of conducting information warfare;*
- *computer simulation;*
- *fundamentals of information technologies;*
- *principles of the functioning of telecommunication systems;*
- *in-house information security and measures to counter the technological tools of foreign intelligence services.*



China’s cyber policy appears to have three vectors —peace activist, espionage activist, and attack planner— that dominate China’s cyber policy. Some are always hidden from view while others are demonstrated daily. Three Faces of the Cyber Dragon is divided into sections that coincide with these vectors.

<https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-books/195610/download>