(U) PLAA Command and Communication Group

(U) This infographic describes the Peoples Liberation Army Army (PLAA) Command and Communication Group. The command and communication group establishes the communications and network architecture necessary to support the operational system. The PLAA places a high priority on information systems that are adaptable and reliable, enabling them to operate in a variety of battlefield conditions or when under electromagnetic or network attack by enemy forces. Communications systems are automated wherever possible, enabling critical information to be rapidly distilled and then passed to the appropriate consumer. The PLAA prefers to use a top-down and centralized approach to its information systems, ensuring interoperability across disparate units.

The command and communication group is also responsible for establishing and monitoring the control measures that control information systems within its combat area— functions such as assigning radio frequencies, deconflicting electronic emitters, and ensuring network security. Finally, the command and communication group is responsible for protection of the operational system's network backbone. In an operational system designed around a CA-BDE, the CA-BDE's communications company within the service support battalion likely forms the basis for the command and communication group.

Note. The Chinese concepts of electromagnetic attack and electromagnetic defense comprise what both China and the U.S. refer to as electronic warfare (EW).

Electromagnetic Protection. Electromagnetic protection contains those measures put into place to resist enemy electromagnetic attack. There are two main modes of electromagnetic protection: counterelectronic reconnaissance and counterelectronic jamming. Counterelectronic reconnaissance is the use of both active and passive means to prevent enemy collection on friendly IW systems. This includes active suppression of enemy collection systems, concealment of friendly electromagnetic signals, the use of decoy or spoof signals to confuse enemy collection, and physical targeting of enemy collection systems. Counterelectronic jamming consists of those systems and techniques that either eliminate or weaken the effects of enemy jamming. This includes hardening IW systems, using of more powerful or more resistant emitters, and carefully monitoring information to weed out disinformation planted by the enemy.

PLAA Tactical Communications Systems

	Designation	Type	Frequency Range	Power Output	Notes
	VRS-1	VHF Radio	30-88 MHz 108-174 MHz 225-420 MHz	15W	The VRS-1 Chinese VHF Radio is mainly used for the cooperative communication among Army, Navy and Air Force.
	TBR-120A or BWT-119	VHF Radio	20 - 79.975 MHz	6W	the main Regiment-Battalion level general purpose transceiver in PLA infantry units
	TBR001A	VHF Radio	46.5 – 49.5 MHz	0.5W	It is designed to communicate between squad leaders and platoon/company commanders. It could also be used as a repeater in the battlefield.
	BT-1 (ZT-1)	VHF Radio	30-88 MHz	4W - Manpack 50W - Vehicle	Chinese VHF Radio manpack FH radio is designed for combat operations.
	TBR-119	SDR	100kHz – 2 GHz	20W/100W	The TBR-119 Chinese SDR Transceiver is a multi-purpose vehicle/backpack tactical radio station with all the functions of traditional ones. It supports SSB, CW, AM, FM, DMR.

Note. The Chinese concepts of network attack and network defense comprise what both China and the U.S. refer to as cyber warfare.

Network Protection. Network protection encompasses those measures put into place to resist enemy network attack. There are two main types of network protection: computer virus defense and hacker defense. Each seeks to proactively protect friendly hardware, software, and networks from both overt and covert enemy intrusion. Network defense is both an active and passive activity. Passive defense seeks to prevent, disrupt, or delay intrusion, while active defense seeks to identify and stop intrusion after it occurs. Due to the extensive use of computer networks, along with the wide variety of hardware and software in use, network defense is seen as a highly difficult—though highly important—tactical task.

Sources:
https://odin.tradoc.army.mil/WEG; https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34236-ATP_7-100.3-001-WEB-3.pdf