The Brave New World of the 5 Day War

Where Cyber and Military Might Combined for War Fighting Advantage.

Paul M. Joyal, Managing Director

Public Safety and Homeland Security

Russian Views on Electronic and Information Warfare

"The growing role of information-technology is rapidly lowering the barrier between war and peace."

Mary C. FitzGerald

www.nationalstrategies.com

Briefing

“Warfare has indeed shifted from being a duel of strike systems to being a duel of information systems”

- In the Early 1980’s, Marshal Ogarkov, then Chief of the Soviet General Staff, first noticed a new “revolution” occurring in military affairs. According to the Russian military, they recognized two major information technologies which today are said to be “ the most formidable weapons of the 21st century” which are comparable to weapons of mass destruction.

  I. Reconnaissance, surveillance, and target acquisition (RSTA) systems

  II. “Intelligent” command-and-control systems

- Under conditions of parity in nuclear and conventional weapons, superiority in reconnaissance, command and control, and electronic warfare is said to be the main factor in raising the qualitative indices of weapons and military equipment, which will have a “decisive” effect on the course and outcome of combat operations.

NSI
Strategy. Insight. Results.

Russian analysts Yevgeniy Korotchenko and Nikolay Plotnikov conclude in 1993:

“We are now seeing a tendency toward a shift in the center of gravity away from traditional methods of force and the means of combat toward non-traditional methods, including information. Their impact is imperceptible and appears gradually… Thus today information and information technologies are becoming a real weapon. A weapon not just in a metaphoric sense but in a direct sense as well.”

NSI
Strategy. Insight. Results.

Two Aspects of Parity and Defense Sufficiency (1993)
Russian Admiral V.S. Pirumov

"... that a war's main objective, shifting away from seizure of the opponent's territory and moving towards neutralizing his political or military-economic potential - eliminating a competitor - and ensuring the victor's supremacy in the political arena or in raw materials and sales markets."

NSI
Strategy. Insight. Results.

General Viktor Samsonov, Chief of the Russian General Staff stated 23 Dec 96

"The high effectiveness of 'information warfare' systems, in combination with highly accurate weapons and 'non-military means of influence' makes it possible to disorganize the system of state administration, hit strategically important installations and groupings of forces, and affect the mentality and moral spirit of the population. In other words, the effect of using these means is comparable with the damage resulting from the effect of weapons of mass destruction."

Strategy. Insight. Results.

Developments to this doctrinal understanding have evolved in the 90’s with the dynamism of the information era

I. Today information warfare doctrine has expanded to include target country information systems, communications networks and economic infrastructure. The role of intelligence services accelerated these developments**.** US and coalition forces learned important information on warfare operations during the first Gulf War contributed to these developments.

II. Cyberspace has clearly emerged as a dimension to attack an enemy and break his "will" to resist. This is an extension of the traditional Soviet intelligence “Active Measure” doctrine. Active Measures are an array of overt and covert techniques for influencing events and behavior, and the actions of targeted foreign countries.

nsi

Strategy. Insight. Results.

Information age technologies have created a new cyberspace environment in which to conduct warfare.

- Russia's response to the information age highlights the potential for challenges to the existing military balance and global security. This was brought vividly home during the 5 Day Russian Georgian War.
- Countries around the globe are increasingly vulnerable to information warfare as cyberspace and social networking increases dependence expands. The gap between the emerging information age environment and the doctrine, capabilities and strategies for defending against and prosecuting information warfare are now being globally confronted.

Strategy. Insight. Results.

Tectonic shift in military affairs:

6th Generation warfare will change the laws of combat and the principles of military science

1. The Russians foresee impending sixth generation of information warfare technology as a potential for cyber warfare to inflict decisive military and political defeat on an enemy at low cost and without occupying enemy territory
2. Thinking of the enemy as a system is the basis to understanding how cyberspace could be used to exploit warfare.

nsi

Strategy. Insight. Results.

Nature of Information Warfare

- Information Warfare (IW) has three components that encompass the totality of actions which ensure victory over the opponent in the information sphere.

  I. First Component→ a complex of measures for acquiring information on the opponent and the conditions of the conflict (radioelectronic, meteorological, the engineering situation etc.)

  II. Second Component→ to gain knowledge on information support of the opponent's troop and weapon control (“information opposition”). It includes measures to block the acquisition, processing, and exchange of information (troop and weapon control.)

  III. Third Component→ to defend against the opponent’s information opposition (“information defense.”)

Strategy. Insight. Results.

Information Warfare

- The ultimate objective of IW is to achieve information dominance over the opponent
- Russians define IW as a complex of measures for information support, information opposition, and information defense.
- The ideas and material foundations of information weapons were formed simultaneously with the development of society’s information environment.
- An adversary's targets include: telecommunications, space based sensors, communications and relay systems; automated aids to financial, banking and commercial transactions; supporting power productions and distribution systems; cultural systems of all kinds; and the whole gamut of media hardware and software that shapes public perceptions.
- The Chinese Liberation Army Daily reportedly advocated the recruitment of civilians to aid in the cyber attacks. There is evidence that Russian special services have also recruited “hackivists” and criminal groups.

Computerization of Information Warfare

- Russia has a well-documented offensive cyber attack program. It has developed tactics and weapons designed to produce dominance in the information “battle space.” Experts list the following information in which effect attack systems:

  a) Computer Viruses

  b) Logic Bombs

  c) Systems to suppress the exchange of information in telecommunications networks, its falsification, and the transmission of needed information (Denial of Service (DOS) attacks).

  d) Techniques and systems that permit the introduction of computer viruses and logic bombs into state and corporate information networks and systems and their remote control.

  e) Malware

Russian intelligence services have a history of employing hackers against the United States.

1. In1985, the KGB hired Markus Hess, an East German hacker, to attack U.S. defense agencies in the infamous case of the “Cuckoo’s Egg.”436
2. Both FAPSI and the FSB, (KGB successor organs), are believed to have potent information-gathering programs, which have led to increased suspicions over possible attempts at espionage.

Russian FSB continues to employ hackers

1. Sergei Pokrovsky, the editor of the Russian hacker magazine Khaker, confirmed that the FSB employs hackers for both foreign and domestic espionage.
2. As evidenced by the Chechen conflict, Russian secret services under sponsorship of the government will not hesitate to use cyber warfare to further their agenda and to protect what they deem to be matters of national security.

Psychological Operations and Information Warfare

1. According to Russian military scientists new weapons will exert a deep influence on the methods, ultimate objectives and definitions of victory in future wars.

2. The use of new information and cyber weapons will be directed primarily at achieving the most important political and economic objectives without direct contact of the opposing forces and without armed combat .

3. These weapons and techniques are designed to destroy the state and societal institutions, create mass disorder, degrade the functioning of society, and ultimately the collapse of the state.

Reflexive Control of the enemy is the goal of PYSOPS and A/M

1. Russian general officers stress that to achieve success the entire process of warfare must be kept under control---including that of the enemy.
2. The target of enemy control is the opposing decision-making commander or national leader. This is called reflexive control.
3. Its goal is to create an atmosphere of pressure to force the target into decisions objectively leading to its own defeat. This can be “being intimidated” to not act or “being lured with advantage” to act against its own interests.
4. This utilizes disinformation, concealment and deception as means to achieve this end.

CYBERWAR
The New “Active Measure”

1. Intelligence subunits of the new cyber military are involved in preparing and conducting psychological operations reinforce the actions of sabotage and reconnaissance, military intelligence and public information services during combat operations.
2. The organization of such is regulated by special directives and manuals developed by military and intelligence services.
3. These CYBER PSYOPS support combat operations in the preparatory period of combat and during combat.

Russian Cyber Warfare Doctrine also addresses the optimum time to strike.

- Prior to an “information strike”, all targets should be identified (including enemy information systems), enemy access to external information should be denied, credit and monetary circulation should be disrupted, and the populace should be subjected to a massive psychological operation--including disinformation and propaganda.

In preparation for conflict, computer networks and databases are penetrated before the beginning of combat operations by agent and other methods.

- Micro-organism cultures are introduced which then eat away electronic components. The employment of information weapons in the concluding phase of a major regional conflict is similar to their use in peacekeeping operations.

Combined information and military operations are required

- Estimates have shown that the use of information weapons must be constantly accompanied by the limited or threat of use of conventional weapons, especially high-precision weapons.

Information Warfare Wrap Up

- The Russians argue that information war occupies a position between “ cold” war and “hot” war.
- The result of an information war is disrupted functioning of elements of the enemy infrastructure.
- “Hot” war uses conventional and/ or mass destruction weapons, it is aimed not at material but at “theoretical” objects.
- At the same time , such objects and systems can be destroyed while their material basis is preserved.

nsi
Strategy. Insight. Results.

Russian-Georgian War

1. The Cyber attack on Georgia illustrates an important detailed example of information warfare as a prelude to military conflict.
2. But this was only part of a more extensive “active measure” campaign that begun much earlier.
3. July 3: One month before Russia’s invasion into Georgia, separatists try to assassinate Dimitri Sanakoyev, Head of the Temporary Administration of South Ossetia.
4. Georgia’s internet infrastructure experienced coordinated barrages of millions of attacks (distributed denial of service DDOS) beginning on July 20th.