Bar-Ilan University (RA)
Faculty of Humanities
Library of Information science

אוניברסיטת בר-אילן (ע"ר)
הפקולטה למדעי הרוח
הספריה ללימודי מידע

Integrating cyber warfare into different types of warfare : the United states of America - case study / Harel Menashri

Abstract

The world of information systems and security has completely changed over the past few decades. The United States applied cyber warfare capabilities as early as the 1991 Gulf War, but the American intelligence had been involved in secret cybernetic activities for years before that. In view of this, I decided to look into the way the United States has been preparing for cyberspace operations.

The present research aimed to study the status of cyber related activities in the United States, the changes that have occurred in the offensive and defensive cyberspace capabilities of the United States armed forces, and the incorporation of cyber warfare into other types of warfare. The study covered events that have occurred in the past few years, especially during the time of the Obama administration.

The following issues were at its focus:

1. Characterization of the way the United States has built up its capabilities and has developed methodologies to guarantee its cyber supremacy.
2. Mapping out the official institutions involved in cyber warfare, the military and civilian authorities under which they operate, and their assessed budgets.
3. Current legislation in this sphere.
4. Characterization of the interdependency between different strategic infrastructures, and the influence this interdependence has on the decision to lunch cyber attacks against these infrastructures.
5. Identification of commercial companies involved in cyber warfare.
6. Identification and analysis of factors that restrain the decisions taken by United States power elements on the use of cyber combat means.

The study of these issues enabled drawing conclusions regarding the United States readiness to include cyber attacks in combat operations of the armed forces.

The methodology chosen for the research combined the qualitative and comparative approaches. It comprised content analysis of open source information dealing with attack and defense factors, and of information dealing with the protection of vital United States national infrastructures. Published studies and information on exercises and war games and on cyber warfare events were also analyzed. The primary sources included policy papers, legislations, resolutions and publications issued by the presidency, by other relevant government departments, and by congress research bodies and cyber warfare organizations. They also included congress hearings and budget books of federal bodies. The secondary sources included studies and professional literature dealing with information warfare and the world of cybernetics, articles published in investigative journals, information published in websites dealing with cyber warfare, and proceedings of various conferences.

The analysis of these sources yielded the following findings:

Cyber warfare methodologies developed in the United States

A full-blown cyberspace war is already underway. In the past decade, especially since President Obama took office in the White House, the administration has been busy putting together the legal and administrative foundations required to formulate a comprehensive strategy for offensive and defensive cyber warfare. National strategies have been outlined for cyberspace activity, and the Obama administration finalized the current strategy in 2011-2012.

Cyber warfare bodies

While the methodological work was in progress, the armed forces and intelligence bodies have been setting up cyber warfare units. Alongside them, defense and security units were being set up in the administration and in local institutes. A cyber warfare center – the Cyber Command – was set up next to the National Security Agency (NSA), with the NSA director also acting as its commander. The combat arms have recently set up cyber dispositions. In addition to protecting the military cyberspace and providing technological support, the missions defined for these dispositions explicitly included defeating any potential adversary, safeguarding the cyberspace supremacy, and attacking enemy cyberspace capabilities. The excessive number of organizations and organizational offshoots operating in the United States cyberspace created problems of control, compartmentalization, and command responsibilities among the different bodies.

Cyberspace legislation

As part of the extensive efforts the United States has been putting into international legislation, it has also been exploring the possibility of restricting the distribution and use of cyber combat means, along the same lines as the existing treaties restricting the distribution of weapons of mass destruction. These efforts have been repeatedly hampered by the defiant stance of Russia, China, and other countries.

Interdependency of infrastructures

The fact that infrastructures are interdependent obliges United States organizations preparing to attack foreign infrastructures to thoroughly investigate the correlation between the infrastructures they are targeting and other infrastructures – in the target countries, in the United States, and elsewhere. This is essential if they wish to avoid an attack that would affect infrastructures in the United States, or cause damage to other infrastructures in a way that could be construed as a war crime.

Involvement of commercial bodies in cyber warfare

Cyberspace is largely based on interconnected infrastructures operated by giant international corporations such as Cisco, Microsoft and other similar ones. The civilian market has considerable influence on cyberspace development and on the attack and defense capabilities of government agencies and military arms.

Checks and balances in using cyber power

American culture and democracy faces its policy-makers with significant checks and balances related to cyber attacks against civilian infrastructures. It would appear that attacks against purely military targets would be much easier to realize. Evidently, intelligence-collection operations are expected to continue, as well as operations designed to find access points to enemy systems, in preparation for a future attack.

The most important conclusion drawn from the above analysis is that no kinetic warfare would be successful without cyber warfare. The United States strategy clearly espouses incorporating cyber operations in kinetic ones, given that conventional warfare per se is no longer the best and most effective way to achieve one's goals in combat.

Defensive capabilities have a crucial role in handling and winning conflicts in an asymmetrical environment, such as that of the United States encounters with its cyber adversaries. There is an acute need to

balance between the ability to launch an attack and win it and the ability to deter the enemy and one's own protect infrastructures and assets.

The United States mode of operation assumes the existence of a cyber envelope for every military scenario. Normally, the ultimate goal would be to neutralize the enemy's defense systems before war breaks out, and thus ensure that the information and communication systems of the United States fighting forces are well protected. In this way, not only would the adversary's command and control systems be damaged, but other critical components would also be impaired, undermining the adversary's ability to throw its combat dispositions into action.

New insights gained in this research:

1. In cyberspace, the time element behaves differently than in other fields. It is often difficult – even impossible – to time the effect of a cyber attack in the same way the effect of a kinetic attack is timed. There are many reasons for this, for example, the great variety of hardware and software in the attack target, connectivity between the target's systems, the systems' bandwidth and the distance between them, system backups, etc. Consequently, the need arose to set up backup attack systems that would enable launching several attacks simultaneously in order to achieve the desired results.
2. The management of cyber combat requires rethinking and updating the definitions used in traditional systems. This refers particularly to the familiar traditional command chain that is in charge of combat management. The large number of cyber warfare bodies set up in various sectors gives rise to the question which of them would be in charge of managing a cyberspace battle. Would a single supreme commander be able to manage the virtual battlefield of information systems? Who is the commander and who are the fighting forces in real-time operations? What would the hierarchy be between military- security bodies and civilian bodies? Will the General Headquarters collaborate on a regular basis with civilian bodies such as the industry and the private sector?
3. The ability to take immediate decisions in reaction to enemy cyber operations is even more vital in cyber combat than on the traditional battlefield. One question that deserves to be explored is whether the reaction should correspond to the type of the attack, that is – be either kinetic or cybernetic. Based on the understanding that by attacking the command and control systems of the enemy it is possible to destabilize it, the question arises whether preference should be given to direct attacks against the

enemy's kinetic systems, or whether it would be best to use cyber warfare to disrupt all of the enemy's operational and logistic systems.

4. Each attack disposition must set boundaries and limits to its attacks or reactions, especially in situations where infrastructures would be paralyzed or destroyed, and civilian populations would suffer damages.

The general conclusion that arises from this research is that the United States seeks to carry out an offensive cyber operation prior to any kinetic operation, with a view to make a kinetic operation redundant in certain cases by destroying the enemy's resources and infrastructures.

System No.:
002385029