Journal of Defense Management
ISSN: 2167-0374
Fayutkin, J Def Manag 2012, 2:4
DOI: 10.4172/2167-0374.1000110
Review Article
Open Access

The American and Russian Approaches to Cyber Challenges

Dan Fayutkin*
Defence Force Officer, Israel

Abstract

Cyber warfare presents new challenges to western governments and private organizations. The gravest danger posed on western governments is a strategic threat on their central information infrastructure, which necessitates the development of new approaches to effectively respond to such cyber challenges. This manuscript discusses the main stream American and Russian approaches to cyber warfare based on official documents, briefings and relevant research. The manuscript then identifies the cyber challenges Israel faces and offers a response by recognizing the lessons provided by the US and Russian approaches. The manuscript analyzes the US and Russian Approaches to Cyber Security according three parameters: Cyber Security definition and its place in the National Security Concept; Doctrinal & Practical Basis for Cyber Security and a legal basis for Cyber Security.

Keywords: Cyber challenges; Global terrorism; Cyber warfare; Cyber security; Political leaders

The US Approach to Cyber Warfare and Cyber Security

US cyber security definition and its place in the national security concept

United States President, Barack Obama has identified cyber security as "one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter" [1].

The central problem in regards to cyber warfare for the US is that the cyber threat is defined under the same categories as conventional and non-conventional threats, such as global terrorism and weapons of mass destruction.

Today, the central goals of American cyber security include: establishing a front line defense against immediate threats by creating or enhancing shared situational awareness of network vulnerabilities; defending against a full spectrum of threats by enhancing US counter intelligence capabilities; increasing the security of the supply chain for key information technologies; strengthening the future cyber security environment by expanding cyber education, coordinating, and redirecting research and development efforts across the Federal Government; working to define and develop strategies to deter hostile or malicious activity in cyberspace [2]. To meet these challenges, the US government developed a cyber security concept based on the traditional strengths of the American government and private systems: the build-up of a comprehensive approach and its implementation on high-technology solutions.

The American government and security institutions need to develop real institutional concepts that can be implemented as a framework for future defense and security activities. A significant challenge in cyber warfare is developing a fast reaction capability and an effective response to cyber activities from hostile entities. Those concerned about security are discovering that the borders between systems are becoming less transparent. Currently, few computers are islands (although most of those that need to be still are) and borders continue to fade every time users cannot differentiate between what is happening on their own machines and what is happening on others [3].

The US national strategy emphasizes the need for America to secure its cyberspace [4]. Yet, it is also necessary to define the significance of cyber security and cyber warfare, not only in terms of economic damage, but in terms of national security. The intensive developments of cyber capabilities worldwide, demonstrate that different political leaders share the concern of the potential power in cyber space and technologies.

Cyber capabilities make it possible to strike strategic infrastructures. The use of computer-based cyber technologies could disrupt banks, social services, power stations and other vital organizations simultaneously. Extreme political organizations like Al-Qaeda and other organizations such as Hezbollah, which use terror for as a means of carrying out their political objectives, could utilize their cyber capabilities in order to enhance anti-western and anti-Israel sentiment, in non-western countries.

The US government has defined cyber space generally and the internet specifically, as a new war domain. This new security domain is connected within the information environment, consisting of independent networks of information technology, infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers [5]. The former CIA Chief, Leon Panetta stated the Internet was "the battleground of the future", that the United States must be prepared to win [6]. Amongst this preparation, the American cyber security concept and strategic doctrine planners must progress with new conceptual and doctrinal documents, which will define the characteristics of the new domain and the main principles of force employment in the cyber domain.

The definition of cyber space as a new domain of warfare has created a debate on the basic terms and paradigms that are connected to this new domain. A necessary question is how will the cyber domain be connected with classical military activities and cyber warfare? Will current military forces be employed for cyber military operations or will it create new kinds of military forces, which will be solely cyber-oriented? The classification of cyber as an independent domain will influence the nature of the goals set out during a military campaign.

The definition of cyber space as an independent war domain will

***Corresponding author:** Dan Fayutkin, Defence Force Officer, Israel, E-mail: dan.fayutkin@gmail.com

Received February 03, 2012; **Accepted** Jujy 26, 2012; **Published** July 28, 2012

Citation: Fayutkin D (2012) The American and Russian Approaches to Cyber Challenges. J Def Manag 2:110. doi:10.4172/2167-0374.1000110

also change military force employment concepts. The development of cyber capabilities will push the development of new operational concepts, which will concentrate on the ability to strike an enemy's command, control infrastructures and systems in order to win wars.

As a means of providing an effective response to cyber challenges, security organizations and militaries, first need to define the operational missions, required capabilities and force structures across the cyber spectrum [7]. According to the official American approach, government security organizations need to develop systems and procedural hedges against the most worrisome cyber vulnerabilities and threats [8].

US Doctrinal and Practical Background for Cyber Warfare and Cyber Security

The United States military has declared that future war is likely to involve the exploitation of cyberspace [9]. The US military envisions cyber space as part of the future battle field. Consequently, the US military doctrine defines that cyber superiority will be a prerequisite for the successful conduct of practically any expeditionary operation [10].

The Cyber superiority defined by the Army doctrine is one that will ensure operational freedom of action. Therefore, the effective use of cyber space would enhance the advantage of synergy, in all operations of US Armed Forces [11]. The Armed forces view computer platforms, which are integral parts of cyber space, as a base for effective synergy of operational planning and command & control efforts. The US Army identifies cyber space and cyber capabilities as new elements for military operations, which could improve their overall effectiveness. The Army Conceptual Framework analyzes cyber space as a new operations domain, which could change future conflicts and force employment. The functional approach of the US Military Doctrine comes from basic warfare paradigm; the army is dominant and other components of operational domains have only support functions. Therefore, the US Military Doctrine, in its Cyber Space Operations Concept Capability Plan, doesn't analyze possible military conflict scenarios, in which cyber threats will have the dominant role.

Legal & Diplomatic Initiatives as Part of Cyber Warfare

The widespread opinion of US government institutions is that cyber warfare requires greater international legal and diplomatic initiatives - both bilateral and multilateral. Nations have a mutual interest in limiting any resort to cyber warfare. A limitation could help prevent the destruction of both governmental and civil infrastructure and protect the welfare of millions of people. Recognizing this, as early as July 2000, the Russian Federation submitted to the United Nations General Assembly a draft resolution, "Principles of International Information Security," that would prohibit the creation and use of tools for a cyber-attack [12]. The US government and legal institutions provide the idea of consolidation of international efforts of different countries in order to build a coalition against cyber challenges. Yet, western countries have not yet developed a united law basis concerning cyber warfare. It is essential that a consolidation of laws and norms will take place, in order to provide better opportunities for legal efforts against cyber terror and the use of cyber space for hostile activities. The United States and other nations need to create a sustainable global legal structure that promotes cooperation among nations to confront cyber warfare, similar to the laws that govern the use of force and armed attacks [13].

The Russian Approach to Cyber Warfare and Cyber Security

Russian cyber security definition

The Russian Security Concept provides a new prospective system of force management on the basis of new cyber technologies. According to the Russian Defense Minister Serdjukov, the Russian Federation Government plans to provide command and control systems for all strategic regions, with the first systems to be sent to the North Caucasus region of Russia [14]. The development of cyber defense systems and capabilities is a part of a comprehensive preparation by the Russian military to provide adequate defense prior to possible offensive efforts. In addition, the Russian Ministry of Defense has made organizational changes in order to build-up special departments for cyber security and information systems. For example, in 2010 a new position was created – deputy of Defense Minister for Information [15].

The Institute of International Security Problems in cooperation with the department of International Policy of the Moscow State University prepared a research study on "Cyber Wars and International Security", which accepted by the Russian Defense Ministry. The research focuses on the cyber policy of the US and China, analyzing principles of cyber operations and other activities in cyber space. The research also analyzed the main paradigms of the US doctrine on cyber wars and force build-up, the organizational structures for cyber wars and basic principles of Chinese cyber warfare strategies. Former Deputy of the Russian Defense Ministry, Kokoshin stated that the threats of cyber and information warfare are current problems threatening national security.

Therefore, it is imperative to develop basic concepts for information wars in cyber space. The achievement of cyber superiority is one of the most significant challenges nations currently face. Without cyber superiority it is impossible to succeed in modern conflicts [16].

The research conducted by IISP has defined cyber warfare as part of information war. Cyber and Information warfare have profound influence on reality; on people and their cognitive and emotional processes, weapons and command and control systems and on decision-making processes [17]. According to the study carried out, the development of a response to these challenges must be organized on an interdisciplinary basis and include researchers from different branches – political analysts, sociologists, psychologists, military specialists, and media representatives. Russian cyber researchers agree with the US approach for cyber security in that the comprehensive approach for cyber warfare and cyber security is the best plan for victory in this domain.

Russian Doctrinal and Practical Background for Cyber Warfare and Cyber Security

The Russian Military Doctrine identifies that current military force employment is a complicated and sophisticated process. Rapid development of weapons and war concepts has transformed military conflict into a dynamic and complicated process, which includes military activities in all physical domains.

Information warfare and deception activities increase the difficulties of understanding your enemy's goals and specific military activities [18]. As a result, cyber capabilities play a significant role in operational planning and force employment.

According to the Russian context, the current trend of cyber

security policy is the legalization of cyber weapons on a state level. In Russia, special units work on the development of computer viruses. A legal basis for the development of offensive information weapons will be organized in different countries shortly [19]. The planning and deployment of systems for information resources defense, in order to stop political, economic and ecological damage from enemy cyber activities against Russia has been implemented.

The Russian President and Defense minister emphasize the development of organizational structures for effective preparations against information challenges on all levels of command and within the defense industry. Further, the development of a united system for providing information has been declared as one of the main trends in the Russian Ground Forces build-up. The Russian Ground Forces is set to develop information infrastructures for command and control processes based on new information technologies [20].

The development of independent information systems and infrastructures will reduce dependence on countries using software from the Microsoft Corporation and the US in general. The lack of international laws concerning cyber security is a result of a policy without united norms, which gives opportunities to influence cyber infrastructures in target states. Different countries are able to use cyber space for a range of activities against each other to achieve strategic goals.

Legal & Diplomatic Initiatives as Part of Cyber Warfare

In an effort to limit the potential threat of cyber warfare, the Russian Federation has created a legal basis for cyber challenges. At the same time, Russian security institutions developed and implemented technologies for defending strategic information. The significant challenge for Russia is the ability to become fully independent from western software programs and Internet resources. Considering the lack of software and hardware developed within Russia, the Russian governmental and private organizations remain highly vulnerable to cyber threats.

The Russian Security Concept provides a new prospective system of force management on the basis of new cyber technologies. According to the Russian Defense Minister Serdjukov, the Russian Federation Government plans to provide command and control systems for all strategic regions, with the first systems to be sent to the North Caucasus region of Russia [21]. The development of cyber defense systems and capabilities is a part of a comprehensive preparation by the Russian military to provide adequate defense prior to possible offensive efforts. In addition, the Russian Ministry of Defense has made organizational changes in order to build-up special departments for cyber security and information systems. For example, in 2010 a new position was created – deputy of Defense Minister for Information [22].

The Russian President and Defense minister emphasize the development of organizational structures for effective preparations against information challenges on all levels of command and within the defense industry. Further, the development of a united system for providing information has been declared as one of the main trends in the Russian Ground Forces build-up. The Russian Ground Forces is set to develop information infrastructures for command and control processes based on new information technologies [23].

Conclusion

The USA and the Russian Federation definitions of the Cyber Security emphasize its significance for National Security. Both Approaches understand the influence of Cyber security on the achieving of National Security and Military goals.

The cyber doctrines of the Americans and Russians emphasize the most effective way for a successful defense against cyber challenges: The development of doctrines; operational concepts; and norms in international law in regards to cyber warfare and cyber security as the main elements for long-term cyber security.

The successful development of the Israeli cyber warfare approach depends on the implementation of US and Russian cyber warfare concepts. Future Israeli cyber warfare concepts cannot use the comprehensive American approach, because the current US cyber warfare conceptual framework provides a basis for consolidation of different governmental and non-governmental organizations, in order to develop effective response against cyber threats. On the other hand, when examining the Russian approach for cyber warfare, it is possible to use the interdisciplinary response to cyber space research as a fundamental basis for future concept development and operational activities.

As previously stated, Israel and its governmental, security and military institutions have superiority in all cyber technologies in comparison to their enemies. With this being said, the enemies of Israel are unable to cause significant damage to the necessary strategic infrastructures within the state. On the other hand, they could provide effective anti-Israeli information campaigns in order to consolidate a range of anti-Israeli organizations to disrupt or reduce the legitimacy of political and military efforts. An example of the information campaign against Israel is seen with the "Marmara" flotilla seizure, which presented Israel as an inhumane nation that used disproportional military force against "unarmed" civilians.

References

1. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative, January 2011
2. Executive Office of the USA President, The Comprehensive National Cybersecurity Initiative.
3. Libicki MC (2009) Cyberdeterrence and Cyberwar. RAND Corporation 1-238.
4. Mesic R (2010) Air Force Cyber Command (Provisional) Decision Support. Rand 1-23.
5. England G (2010) The Definition of Cyberspace, memorandum, Washington D.C., May 12, 2008 in R. Mesic et al, *Air* Force Cyber Command (Provisional) Decision Support(Santa-Monica: Rand Corp., 2010) 3.
6. http://securityindustrynewstoday.wordpress.com/2011/02/11/spy-chief-cyber-war-is-battleground-of-future/ 11 February 2011
7. Mesic R (2010) Air Force Cyber Command (Provisional) Decision Support, Rand, pp 1-13
8. Ibid, p. 14
9. TRADOC, Pam 525-7-8, Cyberspace Operations Concept Capability Plan 2016-202, p. 8
10. Ibid, p. 31
11. Ibid, p. 26
12. Malawer SW Law and Policy Proposals for U.S. and Global Governance. Virginia Lawyer 58: 30
13. Ibid pp 29-30
14. Itar-TASS, "Utverzhdina Konzepzija razvitija upravlenija vojskami do 2025 goda", October, 20,
15. GavrilenkoA (2010) Prioritety Novogo Veka Krassnaya Zvezda. Litovkin V (2010) Kibervoijnas sitemami upravlenija. http://nvo.ng.ru/realty/2011-02-04/11_cyberwar.html

16. Podzorov E (2011) Kiber Vojina I Informazionnaja Bezopasnost – novoe issledovanie.

17. http://www.centrasia.ru/newsA.php?st=1296307260

18. Antonov VI (2009) Obosnovanie Kompjuternoj Systemy upravlenija Vojaskami. In Military Thought No 4: pp 44

19. http://www.securitylab.ru/blog/personal/Zuis-blog/15045.php

20. Tichonov A (2011) Kprevoschodstvu na Sushe. Krassnaya Zvezda

21. Itar-TASS Utverzhdina Konzepzija razvitija upravlenija vojskami do 2025 goda.

22. Gavrilenko A (2010) Prioritety Novogo Veka. Krassnaya Zvezda.

23. Tichonov A (2011) Kprevoschodstvu na Sushe. Krassnaya Zvezd.