Araştırma Makalesi
Research Article

Analysis of the Cyber Security Strategies of People's Republic of China

Çin Halk Cumhuriyeti'nin Siber Güvenlik Stratejilerinin Analizi

Ali Burak DARICILI[*] - Barış ÖZDAL[**]

Abstract

People's Republic of China (PRC) is the rising power of the international system, considering its large surface area and natural resources, high and efficient population structure, developing economy inclined to technology use, veto power owned in the United Nations' Security Council, powerful military, and increasing cyber capacity are considered. The PRC has been planning its cyber security strategy within the purposes of enabling economic growth, developing its military capacity, procuring globally newly emerged technologies within cyber espionage operations, and allowing the security and continuation of the current internal system. As a result, the correlation between PRC's actual cyber security strategies and ancient war concepts, PRC's laws and regulations, institutional structures, official papers, documents, and plans for cyber security area will be analyzed in this paper. Then, the paper will examine the basic characteristics of the PRC's cyber security strategy and thus try to establish a perspective on the PRC's potential cyber security policy in short and medium term.

Keywords: *People's Republic of China, Cyber Strategy, Cyber Space, Cyber Security, Cyber Capacity.*

---

[*] Ph.D., Faculty Member, Bursa Technical University, Faculty of Humanities and Social Sciences, Department of International Relations, e-mail: ali.daricili@btu.edu.tr.
[**] Prof. Ph.D., Uludağ University, Faculty of Economics and Administrative Sciences, Department of International Relations, e-mail: barisozdal@gmail.com.

Geliş Tarihi/Received: 28.02.2018
Kabul Tarihi/Accepted: 26.05.2018

2
Güvenlik Stratejileri
Yıl: 14
Sayı: 28

Öz

Çin Halk Cumhuriyeti (ÇHC) geniş yüzölçümü ve doğal kaynakları, büyük ve verimli nüfus yapısı, teknoloji kullanımına yatkın ve gelişen ekonomisi, Birleşmiş Milletler (BM) Güvenlik Konseyi'nde sahip olduğu veto hakkı, güçlü silahlı kuvvetleri ve artan siber kapasitesi dikkate alındığında uluslararası sistemin yükselen gücü konumundadır. ÇHC genel olarak siber güvenlik stratejisini ekonomik büyümesini sağlamak, askerî kapasitesini geliştirmek, küresel düzeyde yeni gelişen teknolojileri siber espiyonaj operasyonları kapsamında temin etmek ve mevcut iç sisteminin güvenliğini ve devamlılığını sağlamak amaçları kapsamında planlamaktadır. Sahip olduğu büyük nüfus, geniş internet altyapısı ve topluluğu dikkate alındığında, ÇHC'nin siber güvenlik stratejisi kapsamında attığı her adımın bir yandan küresel siber uzay alanını da etkilediği hatırda tutulmalıdır. Bu bağlamda ÇHC'nin siber güvenlik stratejisinin tüm detayları ile irdelenmesi, uluslararası ilişkiler disiplini ve siber uzay çalışmaları açısından önemlidir. Bu makalede öncelikle ÇHC'nin güncel siber güvenlik stratejileri ile kadim savaş konseptleri arasındaki etkileşim, ÇHC'nin siber güvenlik alanı ile ilgili kanun ve düzenlemeleri, kurumsal yapılanmaları, resmî belge, doküman ve planlamaları çalışmada analiz edilecektir. Daha sonra ÇHC'nin siber güvenlik stratejisinin temel özellikleri irdelenecek ve ÇHC'nin kısa ve orta vadede potansiyel siber güvenlik politikası hakkında bir perspektif oluşturulmasına çalışılacaktır.

Anahtar Kelimeler: *Çin Halk Cumhuriyeti, Siber Strateji, Siber Uzay, Siber Güvenlik, Siber Kapasite.*

Introduction

It is clear that the PRC has become an important global power in the recent years within the framework of its large surface area, the full population and the rapidly developing economic and military infrastructure. For this reason, the opinions, intentions, and plans of the PRC administratives in the military, political, economic and technological fields are closely followed by other states. Moreover, when the fact that 721 million of the 3.4 billion Internet users in the world are in the PRC is considered, the importance and effect of the PRC at the point of

setting global scale cyber security strategies is uncontroversial.

On the other hand, it shall be remembered that the PCR holds the most extensive cyber security specialist staff by the rate of the users in question and auditing, cybercontrol, and management of such a large internet community requires an institutional infrastructure and strategy.

However, in the post-Cold War era, states began to develop cyber security strategies to protect their armies and intelligence units as well as their citizens from potential threats that derive from cyber space. The reason for this is the fact that the states are aware of the need to take effective measures against attacks from cyber space area. In this context, states consider improving cyber capacities in both defense and attack as a new opportunity to develop their military capacities.

Despite the fact that new developments in cyber space area have improved the diversity and importance of new actors besides the states in the international system, it can be claimed that the developments in the cyber space reinforced the role of the state at the same time.

In this respect, the fact that planning any activities in the cyber space is simple and can be done without leaving any trace introduce new security risks to international system. But developing measures to eliminate these risks also has increased the importance of the states. In addition, it is also the case that the international system has been now more uncertain and anarchic, as a result of the cyber attacks derived from small groups or individuals.[1]

Within these evaluations depending on the developments in cyber space, many governments have established cyber security institutions and trained cyber experts and academics according to their cyber security strategies. In addition, when it is thought that all these large-scale plans and strategies can be planned and implemented

[1] See more at; A. Burak Darıcılı, ***Siber Uzay ve Siber Güvenlik; ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi***, Bursa, Dora Yayıncılık, pp. 33-35, 2018. Ahmet Naci Ünal, ***Siber Güvenlik ve Elektronik Bileşenleri***, Ankara, Nobel Yayıncılık, pp. 105-122, 2015.

successfully by only states, it can be argued that states have secured the role of the dominant actor in the international system.

At this point, the fact that the rules and institutions of international law controlling cyber space have not still been established leads to competitive politics rather than cooperation among states in cyber space. In this case, it can be claimed that the international system evolved into a more uncertain and insecure structure in accordance with the real-political paradigms.[2]

In this context, PRC, which considers developments in cyber space as both a threat to her security and an opportunity to improve her military capacity, aims to bring out plans and strategies like other states. It can be stated that significant developments are realized in cyber security policies in the 2000s; new plans and institutional structures are established; legislative regulations, which audit and control the national cyber space field are completed quickly as a result of rapid economic and technological growth which the PRC experienced. In other words, today, the PRC has reached the position of global superpower, which can dominate the cyber space field together with the United States (US) and Russian Federation (RF).[3] In the context of plans came up from the end of 1980's, PRC works to design the cyber security strategy rapidly, primarily for the aim of defense and then for the aim of attack, especially within the scope of cyber espionage operations, in relation to protect its domestic safety and stability. In this context, it can be argued that the PRC has primarily economic, political, and military objectives in the cyber security strategy. These objectives can be listed as follows:

• to procure state of the art technologies having significant influence within the context of cyber espionage operations to ensure economic growth and stability,

[2] See more at; Ibid., pp. 40-45.
[3] See more at: A. Burak Darıcılı and Barış Özdal, "The Analysis on the Instruments Forming the Cyber Security Capacity of Russian Federation", ***Bilig***, (83), pp. 121-125, Autumn 2017.

• to control the internet in order to maintain the governance of the Communist Party of China (CPC) in the country and thus to control the local opponent movements, separatist foci, and possible social uprising attempts,

• to develop measures against hostile information warfare plans based on network technologies and to resist against the operations aiming at intervening in the internal affairs of the country,

• to establish an important counter/espionage structure against the cyber espionage activities planned against the CPC by the foreign intelligence services,

• to support the military capacity within the opportunities made possible through state of the art technologies in cyber space field and, at the same time, to build plans against critical infrastructures of potential hostile military powers, and

• to organize information warfare strategies and cyber-attack activities based on network technologies against the areas and governments in a target.

On the other hand, an active planning of cyber security strategy of a global superpower like the PRC requires an overall evaluation of many variable paradigms and potential threat foci and plans by the future objectives in question within the context of these evaluations.

Also, it shall be known that PRC is tight lipped in all the processes of establishing any strategies about national security including the cyber security plans of the PCR and it is in a particular effort to hide its real intentions.[4] In this context, all the processes influencing the establishment of these strategies in question shall be examined in detail for analyzing the cyber security strategy of the PCR in detail. In this respect, the decision-making processes in a determination of a country's security strategies, keeping in mind that it is directly in relation with the social heritage of that country, the influence of the

[4] Ibid., p. 9.

PRC's ancient war concepts in shaping the outlines of the contemporary cyber security policies shall also be analyzed.

1. The Correlation between PRC's Cyber Security Strategies and Ancient War Concepts

The social heritage and its contribution to the formation of the theoretical background of cyber strategic processes in current cyber strategy analysis are often neglected. However, there is the social and cultural heritage factor, which determines the decision-making processes and the decisions of the actors, who are in these processes in the strategic plans of a state regarding security field.

For example, in the shaping of the current cyber policies of the RF, the "war" of the Russian political elite is considered a political movement style and an honorable image, which are refrained throughout the history. In this context, the strategic mind of the RF considers the cyber space as a new military struggle and conflict area and acknowledges the technological developments as new opportunities to improve the military capacity. It sets up new cyber defense and attack plans in this direction.

Chinese culture covers successes in many diverse areas whose history traces back to 10,000 BCE and which is flourished in the geographies dominated and influenced today by the CPC. One of the most important names of this archaic cultural past is the military strategist Sun Tzu of Chinese origin, who lived in Wu State (contemporary China) in 500 BCE and he is considered one of the pioneers of the realpolitik approach. The opinion that Su Tzu has indicated in his work ***Art of War*** as "All warfare is based on deception; hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near"[5] influences the shaping of the PRC's security policies today. In other words, the process of shaping of a strategic approach is based on how much can you benefit from "cheating" and camouflage" practices, as

[5] Sun Tzu, ***Savaş Sanatı***, (Translated by Pınar Erturan) Ankara, Remzi Kitapevi, 2016, p. 13.

Su Tzu has implied in his work mentioned. The cheating and camouflage opportunities are prevalent in the cyber space because of the asymmetrical and unanimous structure, which enables to hide time and source of the threat.

At this point, in accordance with Su Tzu's ideas, Mao Tse-Tung's statements in ***On Protracted War*** are as follows: "...to keep the enemy in the dark about where and when our forces will attack." This, he goes on, creates a basis "for misconceptions and unpreparedness on his part... In order to achieve victory, we must as far as possible make the enemy blind and deaf by sealing his eyes and ears and drive his commanders to distraction by creating confusion in their minds."[6] These are essential concerning analysis of the PRC's cyber strategy today. As can be seen, Tse-Tung suggests that deceiving the enemy and manipulating its decision-making processes is necessary for victory and developing strategies accordingly to the successor governors.

General Wang Pu Feng has taken necessary steps in realizing the cultural mind through practical approaches in 1995. The Chinese People's Liberation Army (PLA), which is referred in this respect, brings forward that the computer systems of the PLA can be used as a new instrument of both information warfare systematics and conventional military capacity and enabled initiation of extensive plans within PLA in this direction.[7] For us, another important reason why Feng has initiated such kind of an attempt is that the PCR's monitoring, as monitored by worldwide, of the great success of the US in integrating the opportunities based on network technologies with the classical warfare abilities in the First Gulf War.

---

[6] See more at: Samuel B. Griffith, ***Communist China's Capacity to Make War***, (Published by the Council on Foreign Affairs), https://www.foreignaffairs.com/articles/asia/1965-01-01/communist-chinas-capacity-make-war (Accession Date: 16.09.2017).

[7] See more at: Pierluigi Paganini, ***China admitted the existence of Information warfare units***, http://securityaffairs.co/wordpress/35114/security/china-admit-cyber-army.html, (Accession Date: 16.09.2017).

Moreover, review of some of the statements in the book named ***Unrestricted Warfare*** written in 1999 by the colonels Qia Liang and Wang Xiangsui, retired from PLA, is worthy of note in the context of archaic Chinese culture's influence on the contemporary cyber strategic mind. In this respect, Liang and Xiangsui stated that "the PRC can overcome a struggle with a state stronger than itself through benefitting from technological advantages instead of using military power, for example the increasing dependency of the US on network technologies is a very important asymmetrical advantage and wars will be carried out in cyber spaces where weapons are not used instead of military fields in the future."[8]

It is evaluated that these thoughts of the colonels are also the basis of the modern cyber security strategy of the PRC. The PRC wants to gain an advantage by developing a sophisticated cyber plans and systematics against countries, which have more powerful armed forces and technological advantages than itself, such as the US, through benefitting from the unanimous and asymmetrical structure of the cyber space. It tries to realize the measures which it has developed or will develop towards achieving this goal through hiding and camouflaging its actual intention using low profile political approaches. At this point, it can be indicated that the modern military, security, and intelligence plans of the PRC are shaped within the principle of "collect as much information as possible about the enemy, keep your information and intentions secret".

Another article written by the General Li Bingyan, retired from PLA, in accordance with the opinions mentioned above, states that "while strategy is important for Eastern societies, technological advantages are important for Western societies and, in this context, West gives great importance only having military and technological

[8] See more at: Liang Qiao and Xiangsui Wang, ***Unrestricted Warfare***, (Unofficial translation of the book is available at http://www.c4i.org/unrestricted.pdf), 1999, PLA Literature and Arts House, pp. 204-225.

power but efficient results can be achieved with lower military and technological capacity as is done by the Eastern societies".[9] It can be claimed that this approach is also valuable for us in understanding the decision making processes forming the modern cyber security strategy of the PRC.

It can be argued that the concept named "Integrated Network-Electronic Warfare (INEW)", which was planned regarding the warfare possibilities based on network technologies by General Dai Qingmin in 2002, is one of the most explicit effects of the cultural heritage in question. In this regard, Qingmin gave special importance to "deception, intelligence, and physical destruction" levels in his concept and determined that the cyber capacity of PLA shall be constituted with the forms of "operational security, deception, computer network attacks, electronic warfare, intelligence, and physical destruction" and thus planned the integrated use of Electronic Warfare (EW) and Computer Network Warfare (CNW).[10]

On the other hand, the governments of PRC bring forward harsh legal regulations and punishments time to time in order to control the world's most significant internet infrastructure in their country for maintaining the internal stability and security. It is clear that naturalization of these legislations by most of the Chinese society has not been too much trouble, despite the various social unrests and harsh criticisms of the West. This situation can be considered in terms of "service before self" understanding in Chinese culture.[11] Restriction of individual's rights and freedoms by the authority (dynasty in the past or CPC

---

[9] Diane E. Patton, ***Evaluating U.S. and Chinese Cyber Security Strategies Within a Cultural Framework***, (A Research Report Submitted to the Faculty in Partial Fulfillment of the Graduation Requirements for the Degree of Master of Operational Arts and Sciences), April 2016, http://www.dtic.mil/dtic/tr/fulltext/u2/1031380.pdf (Accession Date: 12.09.2017), p. 7

[10] Monika Chansoria, ***Informationising' Warfare: China Unleashes the Cyber and Space Domain***, (Paper by Centre for Land Warfare Studies), http://www.claws.in/images/publication_pdf/1270592252MP_20.pdf, (Accession Date: 12.09.2017), p. 7.

[11] Chansoria, op. cit., p.8.

government today) for the sake of social welfare, peace and security are considered as a typical situation within this cultural context by the ordinary PRC citizens.

Another critical point shall be highlighted after the evaluation we have carried out within the context of the effects of archaic Chinese culture on the PRC's cyber security strategy. This critical point is that the literature used regarding cyber security studies in PRC is different from the literature used in the West. In this respect, after the differences are discussed, the details of the papers and documents of the PRC's official cyber security strategy will be studied.

2. The Terminology of Concepts Used within Cyber Security Concept in PRC

The identification differences between the cyber security terminology used in the West and the terminology used in the PRC is important in order to understand the cyber security strategy of the PRC. In this context, generally "information security" or "network security" terms are used in the Chinese terminology instead of cyber security concept. "Network/*wangluo*" is used instead of the cyber word in official, academic, and military terminology and cyber space concept denotes to the "network space/*saibo kangjian*" concept. "Network warfare/*wanglua zhan*" concept is used instead of the concept of cyber warfare.[12]

As can be understood from the different uses of the terms in question, Chinese specialists and academicians explain every relevant term about the cyber developments with a broader viewpoint and use the concept of "informatisation" instead of using cyber. This concept is described as "the transition process from industrial society to information society". The "cyber space" concept is a sub-concept of the definition of "network space" and is described by the specialists and academics as

[12] See more at; The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), ***China and Cyber Attitudes, Strategies, Organizations***, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf, (Accession Date: 13.09.2017), p. 9.

"the communication field which consists of the data processing of the humanity and the cyber space where large part of the world population is involved in".

At this point, the cyber security concept is described as "software and physical security of computers, networks, information systems and processes" in the terminology of the West. The "network security" concept, which corresponds to this term, is conceptualized as "information systems and the content of the information are inseparable and connected parts of the information security". Another difference is about the definition of "cyber warfare" in the Western terminology and the definition of "information warfare", which is used instead of it in the Chinese terminology. While both of the concepts in question are described as "any intelligence operation or method planned through information technologies", this concept is used in describing the psychological warfare operations of mainly the US and the ones with Western source, purely and simply.[13]

The different definitions we mentioned above are mainly due to two reasons. The first of these is the socialist government system of the PRC. The explanation of the results of the developments based on the network technologies, which are explained within the context of the concepts of cyber space and cyber security and whose results are considered with the definitions such as cyber strategy, cyber-attack, cyber power, information warfare, cyber propaganda etc within this ideological approach is a requirement for Chinese cyber security specialists. Another reason is about the reactional attitude of the PRC against the US and the Western world on the literature shaped around the concept of cyber space and the attempts and operations of them for dominating the literature and the academic studies. Thus, PRC has the effort to develop its own stance and genuine system and becoming a global alternative against the US and Western hegemony in the fields of military, economic, cultural, political, social, and cyber space.

[13] See at more; Ibid., pp. 9-10.

3. The PRC's Official Papers, Documents and Plans on Cyber Space

The end of the 1980's, which is the time when the civilization and commercialization period of the internet started, is also the period in which the PRC's official plans on cyber security is brought forward. The PRC initiated its first official attempt on information technologies on the national level in 1986 by establishing the structure named "State Economic Information Management Leading Small Group". "State Informatisation Leading Group (SILG)" was founded with the decisions taken in 1999 and 2001. Later, "State Network and Information Security Coordination Small Group (SNISCSG)" has begun working as a sub-study structure of SILG in 2003. The main purpose of these groups is the development of PRC in the fields of information technologies. Later, it has been decided that Chinese governments shall encourage local investments in the field of information technologies in the PRC's 10th Five Year Development Plan published in 2001.[14] The main reason of this decision can be claimed that it is their determination and evaluation on the importance of the role of information and network technologies in short and medium term in terms of increasing the global competition capacity of the PRC government. In this regard, the rapid development of PRC in information and network technologies is significant.

"Document 27" was declared by SNISCSG in 2003. This document was prepared according to Mao Zedong's "active defense"[15] strategy. This document aimed at development of local technologies in the field of information technologies, the establishment of coordination between the institutions working in this field, and increasing the budget for the sectors in question. Establishment of a new structure and dissolution of the SNISCSG in 2008 following its successful studies

[14] Ibid., p. 11.
[15] Active Defence is a concept of Mao Zedong which indicates the strategy proposing that an aggressive policy shall not be followed without an attack against the PRC.

carried out in accomplishing the objectives in question have been decided in accordance with the new technological developments. There is open source information on which the structure will run the duties, which were carried out by the SNISCSG after the closing of this institution. Accordingly, the situation emerged with SNISCSG shall be evaluated within the framework of "hiding the real intentions" tendency which we have examined before regarding the strategic plans of PRC.

"The National Programme for the Development of Science and Technology in the Medium and Long Term, 2006-2020", which was declared by the State Council of the PRC, is critical concerning the development of PRC in contemporary technology and informatics. PRC has determined the development of informatics and network technologies through local sources as the main objective and put forward the argument that this objective shall be in accordance with the aim of increasing the quality of life and the standards of the Chinese people. The coordination between the institutions, which have not been successful in establishing such coordination in the fields of informatics and technology until 2006, has been achieved through this program and an important step has been taken in reaching the current technological level PCR has today. This program does not have a military purpose. Various plans have been proposed for the purposes of encouraging the informatics sector and increasing energy sources, establishing the water demand, developing environmental technologies, encouraging intellectual rights and PRC's having a competitive economic structure.[16]

As is seen, the PRC governments placed great importance to technological development in the field of cyber security, production of national and local software-hardware through using equity capital, and maintaining these production processes with the support of state-funded institutions and organizations. As a result of this strategic approach,

[16] The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), ***China and Cyber Attitudes, Strategies, Organizations***, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf, (Accession Date: 13.09.2017), p. 12.

significant developments have been achieved, critical strategic documents were prepared, and new organizational structures were established in the field of cyber security after 2010.

In this regard, a strategy named "New Policy Opinion (NPO)" has been declared by the State Council's Information Office (SCIO) in 2012. The main purpose of this strategy is to encourage the information sharing among the institutions which are active in the field of technology and to provide protection of information and technology security within national interests under the coordination of State Council. The main difference of this strategy from previous documents is that this strategy has new objectives such as enabling information security for state organizations and individuals beyond allowing economic and technologic development and preventing the social manipulation and espionage operations originating from network technologies.[17]

A new organization has been established in 2014 named "Central Leading Small Group for Internet Security and Informatisation". It has been decided that the operations of this organization will be directed by the PRC presidents and thus the importance placed by the PRC on cyberspace-based developments has tried to be highlighted. The main objective of the working group is determined as establishing the required coordination and common political initiative within the aims of developing internet security and informatics sectors among state organizations.

The fact that the unit called "Central Leading Small Group for Internet Security and Informatisation" will operate under PRC presidency also shall be evaluated as an important strategic approach in terms of taking fast and exact decisions in the field of cyber security. Thus, PRC has aimed at reducing the loss of time in decision-making

[17] See more at: Adam Segal, ***What to Do About China's New Cybersecurity Regulations?***, https://www.cfr.org/blog/what-do-about-chinas-new-cybersecurity-regulations (Accession Date: 14.09.2017).

processes originating from bureaucracy and the misjudgments in the field of cyber security.

It is also seen that important developments are experienced in the PLA in the field of cyber security strategy based on the above-mentioned strategic steps taken. As a result, China's Military Strategy was declared by the PRC Ministry of Defense on 26 May 2015. This document pointed out important points such as rapid development of information society, the PLA's necessity of establishing new plans which will synchronize with these new conditions, informationization of the wars, as well as the facts that even local conflicts are influenced from this informationization process and changed their formats, that it is a necessity for PLA to synchronize its warfare systems, command structure and all of its military elements with the network technology, that PLA shall evaluate the cyber crisis and cyber operations as new threat and take measures against them.[18]

The PRC government, which has considered scientific developments originating from space technologies depending on the new initiatives within the cyber security field as a new opportunity area for improving its military capacity, has taken steps in the direction of developing its cyber capacity within the field of space technologies. In this framework, the summary in the document named "National Cybersecurity Strategy" published by the Cyberspace Administration of China on 27 December 2016 stated the points that cyber space is an area which may create new threat for the security of the country, that any kind of scientific, technical, legal, diplomatic, and military measures will be taken by the PRC in order to eliminate the dangers originating from this area, that any kind of espionage and intervention attempts targeting the internal security of the Chinese government will be interrupted without hesitation, that measures will be taken in order to protect the critical infrastructure of the country, and that PRC will

[18] See more at: USNI News, ***China's Military Strategy***, https://news.usni.org/2015/05/26/document-chinas-military-strategy, (Accession Date: 14.09.2017).

support an economy with open market, transparency, and competition conditions and encourage the increase international investments of the local companies within informatics and technology sectors.[19]

Another critical point of reference in the development of cyber capacity regarding space technologies is "International Strategy of Cooperation on Cyberspace" which was published by PRC Ministry of Foreign Affairs and Cyberspace Administration of China on 1 March 2017. To summarize it shortly, this document included the points that militarization of the cyber space and use of it as an area for deterrence is being opposed, that attempts such as these damage to international security and stability, that cyber space shall be audited and controlled by a multi-sided governance, in which these sides shall be states, international organizations, international companies, non-governmental organizations, and even individuals, that United Nations (UN) is an appropriate ground for determining the auditing committees in question, that foreign investments of international informatics and technology companies will be encouraged, that any kind of support will be given to the foreign companies for them to make investments in the country providing that public benefit and national security will be watched, that the governance of the internet will not be monopolized, and that PRC prefers a multi-sided governance system.[20]

In this context, it can be stated that the document in question brings forward the point that cyber space shall not be militarized and not be used as an area for deterrence, referring to the claim that "increasing cyber power and cyber challenges of RF poses serious threat for the security of the US, and especially PRC became a threat in term of cyber espionage operations for the US", which was present in the document named "National Security Strategy" declared by the US in

[19] See more at: China Copyright Media, ***National Cybersecurity Strategy***, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/ (Accession Date: 14.09.2017).

[20] See more at Xinhuanet, International Strategy of Cooperation on Cyberspace, http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm (Accession Date: 14.09.2017).

February 2015.[21] The request on governance of the internet and the cyber space with a multi-sided system shall be considered as a result of the long-term policy, which symbolizes the opposition of the PRC against the hegemony of the US.

As it is seen, advancement of internet, network technologies, and informatics sectors, encouragement of local technologies on this matter, procurement of cyber securities of state organizations and individuals, prevention of possible cyber operations, espionage, and manipulation activities from hostile states against the country are heavily involved in the paper, along with the documents and plans of the PRC on cyber security. In order to achieve these goals, small working groups were set up, which were established based on periodic developments. It is aimed to govern the cyber security of the country, which has the world's largest internet community, through a single authority and rapid decision-making processes without facing bureaucratic obstacles through such a structure. There is a language encouraging peace and cooperation in the documents and strategies; it is emphasized that the cyber security of the country will be defended resolutely against manipulations and leakages of the foreign countries.

4. Actors in the PRC Cyber Security Strategy Management

Actors in the PRC Cyber Security Strategy Management can be divided into civil and military sides. The civil side consists of CPC, official institutions affiliated to Chinese government and working groups, telecommunication, technology, informatics companies, which are globally active, hacker groups, and cyber civil militia. The military side consists of units within PLA.

The top decision-making bodies of the civil side are Politburo Standing Committee, State Council, and Central Military Commission as in all decision-making processes of PRC. The authorities in question are the basic structures, which take decisions on large-scale initiatives

[21] A. Burak Darıcılı, "Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi", ***Journal of International Studies***, 1 (1), 2017, p. 7.

regarding cyber security strategy of PRC.[22]

On the other hand, there are various institutions, which are founded with the instructions of super-structures in question. For example, Ministry of Industry and Information Technology (MIIT) was established in 2008 and has similar duties and responsibilities with Department of Homeland Security of the US.[23] "The National Computer Network Emergency Response Technical Team/Coordination Centre of China" (CNCERT) is a non-governmental organization founded in 2002 acting under MIIT and it is responsible for the detection of malicious software in the networks of the country and development of necessary measures against them and informing MIIT about the processes. MIIT also has a body called the "State Administration for Science, Technology and Industry for National Defense" (SASTIND), which drafts guidelines, policies, laws, and regulations regarding science, technology, and industry for national defense. Prior to the establishment of MIIT, a separate body called the "Commission for Science, Technology and Industry for National Defense" (COSTIND) carried out similar tasks.[24]

"The Ministry of Public Security" (MPS) is an organization researching the cyber crimes and taking measures towards protecting the critical infrastructures. MPS also has an important duty in counter-espionage by acting as an auditing body over the Chinese technology companies and products to be exported. "Ministry of State Security" (MSS) is responsible for all counter-espionage plans including espionage operations originating from hostile services and procurement of domestic intelligence service need of the PRC. At this point, it shall be stated

---

[22] The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), ***China and Cyber Attitudes, Strategies, Organizations***, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf, (Accession Date: 13.09.2017), p. 19.
[23] See more at; Darıcılı, "Demokrat Parti Hack…", op. cit., pp. 8-9.
[24] The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), ***China and Cyber Attitudes, Strategies, Organizations***, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf, (Accession Date: 13.09.2017), p. 16.

that the duties and authorities of the MSS is broad and extensive in terms of playing an important role in the intelligence structure of the PRC. Resisting against the opposition movements against the CPC and information warfare operations originating from hostile countries are among the duties of this organization. In this respect, it can be stated that MSS has the same duty and responsibility with "*Federalnaya Slujba Bezopasnosti*" (FSB) of the RF and "Federal Bureau of Investigation" (FBI) of the US.[25] MPS and MSS both operate under the State Council.[26]

Other organizations, which operate under State Council, are "State Encryption Bureau" meeting the crypto needs of the state institutions and "State Secrets Bureau" managing all the significantly secret networks systems.27 On the other hand, "Chinese Institute of Contemporary International Relations", which acts directly under MSS, the "Chinese Academy of Engineering", and the "Chinese Academy of Sciences" have essential duties in research of the cyber space-based technologies. Tsinghua University, Peking University, Academy of Military Science and the PLA Information Engineering University and Cyber Security Association of China have significant contributions in developing technologies in question and training specialists regarding the subject.

As is seen, small working groups, such as SILG and SNISCSG acting with central authority and responsibility in the administration of the PRC cyber security policies, have essential functions. The most important reason for founding these kinds of structures is to prevent potential bureaucratic delays, which may arise within the high population and large surface area of PRC. These structures operate being directly answerable to the top decision-making actors. For this reason, they can take effective decisions without losing time in the strategy-setting processes.

---

[25] Darıcılı, "Siber Uzay ve…", op. cit., p. 99.
[26] Darıcılı, "Demokrat Parti Hack…", op. cit., p. 18
[27] See more at: Jon Lindsay, Chinese ***Civilian Cybersecurity: Stakeholders, Strategies, and Policy***, (Report from Workshops held at the University of California, San Diego April 2012), https://ndc.gov.bd/lib_mgmt/webroot/earticle/147/China_and_Cybersecurity.pdf (Accession Date: 16.09.2017), pp. 6-8.

Some of the telecommunications, technology, and information technology (IT) companies originating from China operate on a global scale and they are among the leading companies concerning their revenues. The best-known companies are China Telecom, Huawei, Lenovo, and China Unicom. The management level and shareholders of such companies are directly linked to the CPC and the PLA.[28] Some of these companies' global activities are frequently discussed in the context of their links with the PRC and they are subject to various restrictions in the Western world, due to the fact that their products and services may be the sources of PRC-based cyber espionage operations. Moreover, regarding these companies' investments in the Western world, their attempts to purchase Western-based companies can be a matter of discussion for similar reasons.

Chinese hacker groups and cyber militia structures are other issues, which should be addressed within the PRC's cyber security strategy. In this context, hacker groups operate independently or in the name of PRC in cyber space. As is known, there are many such groups behind numeraous attacks taking place on a global scale. At this point, the claims that the RF obtained the e-mails of some of the directors of the "Democratic National Committee" (DNC) in 2016 through cyber-attack and various state-supported criminal hacker groups and that it leaked some of these e-mails to the public shall be remembered. As considered in these claims, the RF has benefitted from some hacker groups connected to secret services in its cyber operations. Accordingly, the RF President Vladimir Putin claimed that "patriotic hacker groups may have made such plans under their own initiatives."[29]

Although it seems that the use of illegal hacker groups for efficient cyber operations under the auditing and the control of secret services is an advantage, the condition of the PRC is different in this

---

[28] See more at: RSAC, ***Comparative Study: Iran, Russia &PRC Cyber War***, https://www.rsaconference.com/writable/presentations/file_upload/hta-w01-comparative-study-iran-russia-prc-cyber-war_copy1.pdf (Accession Date: 15.09.2017).
[29] See more at: Darıcılı, "Demokrat Parti Hack…", op. cit., pp. 16-18.

regard. The PRC considers that if it supports these kinds of groups, the groups in question might act against itself when they get out of control and that this may result in internal unrest and manipulations against CPC if they involve in interaction with various opposition movements and hostile intelligence services in this direction.[30]

On the other hand, by its very nature, there is limited open source information on the hacker groups, which are claimed to be in connection with the PRC. However, the Red Hacker Alliance is the most important group that has been linked to the PRC and whose name and some activities have been unraveled publicly. There are thousands of members of this group who believe in Chinese nationalism as it is claimed in open sources and they transfer highly valuable information to relevant PRC institutions through industrial and technology espionage operations within the scope of their activities abroad.[31]

The PRC, as discussed earlier, has the world's most populous internet community among internet users and experts. The experts in question are the primary element of the cyber militia structure of the PRC. In this context, all scientists, experts, engineers, and network technology capable citizens working in the telecommunication, information, and technology areas are natural members of this militia structure for PRC. It is alleged that these individuals are not directly associated with the CPC but have occasional exercises within the scope of contingency planning and that they got training for lines of action against cyber-attacks against the PRC during these exercises.

The units under the CPC are also essential to reveal the cyber-attack capacity of the PRC. The CPC has not declared a specific

---

[30] See more at: Tim Stevens, ***Breaching Protocol: The Threat of Cyberespionage***, Academia.edu, http://www.academia.edu/1158361/Breaching_Protocol_The_Threat_of_Cyberespionage (Accession Date: 16.09.2017).

[31] See more at: Tobias Feakin, ***The Cyber Dragon***, (Report by the Australian Strategic Policy Institute, 2013), https://www.aspi.org.au/publications/special-report-enter-the-cyber-dragon-understanding-chinese-intelligence-agencies-cyber-capabilities/10_42_31_AM_SR50_chinese_cyber.pdf (Accession Date: 16.09.2017), pp. 4-5.

doctrine contrary to the armed forces of the US and the RF. Instead, making several references to the subject in the "Military Strategic Guidelines" which are published in every 10 or 15 years has been sufficient for them. These references only state the importance of network technologies for today's conflicts and that CPC has to integrate the new generation technologies into its armed capacity and the rising importance of information warfare.[32]As discussed earlier, this can seem surprising for a culture that has considered the importance of intelligence, intelligence gathering, tricks, and manipulation since Sun Tzu. In fact, this initiative stems from the fact that the real intentions and plans regarding cyber space are intended to be concealed.

In 1986, the PRC initiated "Program 863". The main objective of this program is to develop a specific and comprehensive intelligence gathering systematics to overcome the technological diversities with the Western world in the key sectors. The perspective this plan has provided CPC to initiate a series of reform processes, which has reached today.[33] Accordingly, Communications Department of PLA General Staff Department was restructured into the Informatisation Department, together with establishing several smaller information-related departments in the PLA regions following the several plans made in time.[34] Three new structures were established in 2015. These new structures are PLA Rocket Force, the PLA Strategic Support Force, and the Army Leadership Organ. However, the Strategic Support Force (SSF) has also been given a status equal to the professional service branches by today. It also will likely formulate the core of China's information warfare effort by comprising

[32] See more at: The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), ***China and Cyber Attitudes, Strategies, Organizations***, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (Accession Date: 13.09.2017), pp.19-26.

[33] Nigel Inkster, "Chinese Intelligence in the Cyber Age", ***Survival: Global Politics and Strategy***, , 55, (1), 2013, p. 50.

[34] See at more: Thomas L. Timothy, ***Three Faces of the Cyber Dragon***, Forth Leavenworth, KS. Foreign Military Studies Office, 2012, pp. 69-72.

forces in the space, cyber, and electromagnetic domains, thus finally it will gather China's military-related informatisation activities under one umbrella.[35] In addition to these, it has been claimed that SSF controls all the cyber operations of CPC in the cyber space together with the decisions taken by some sources in the recent years.

As another result of the reform processes, two executive bodies of the PLA General Staff Department, the Third and the Fourth Departments, were established. Third Department (3/PLA) is also known as the technical department. It operates in coordination with the 2/PLA, which has duties and responsibilities in the intelligence field. At this point, as mentioned before, it can be stated that the operations similar to the intelligence gathering operations of MSS are carried out by thr 3/PLA; but the 3/PLA undertakes the plans regarding the technical side of the objectives in question and the remaining duties are carried out by the 2/PLA. In this context, it can be claimed that the 3/PLA is mainly responsible for meeting the needs of the "Signal Intelligence" (SIGINT) and it plans its operations accordingly; thus, it has a similar function with "National Security Agency" (NSA) of the US.36 Another organization which operates in coordination with the 3/PLA in gathering technical intelligence, especially SIGINT, is the "Military Region Technical Reconnaissance Bureau" (TRB). This organization serves in even military regions and it is independent of the 3/PLA. Like the 3/PLA, the TRBs' responsibilities include not only computer network exploitation, but also cryptology and communications intelligence. [37]

---

[35] See at more: John Costello, ***The Strategic Support Force: China's Information Warfare Service***, The Jamestown Foundation, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=45075&cHash=9758054639ab2cb6bc7868e96736b6cb#.V6RA_Lt95aQ (Accession Date: 17.09.2017).

[36] See more at: Inkster, op. cit., pp. 46-49.

[37] The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), ***China and Cyber Attitudes, Strategies, Organizations***, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (Accession Date: 13.09.2017), p. 23.

Fourth Department (4/PLA) has duties and responsibilities in meeting the needs of CPC about "Electronic Intelligence" (ELINT) and resisting to the ELINT operations against the country. It also fulfills tasks such as taking measures against attacks originating from computer networks.[38] It can also be stated that the 4/PLA has responsibilities which are similar to the duties carried out by MSS, and, at this point, it operates in coordination with the 2/PLA and the 3/PLA; but it carries out the plans on the meeting the ELINT needs of these responsibilities.

Another initiative was also launched in the CPC in 2014. In this context, the "Opinion on Further Strengthening Military Information Security Work" was published by the Central Military Commission and the CPC's directives for the military in the information security field were declared. Chinese Ministry of National Defense declared China's Military Strategy in March 2015, based on its Defense White Paper dated 2015. The Defense White Paper is vital in terms of the significance given by CPC to the development of information warfare abilities. These documents have focused on the points that CPC shall develop its cyber powers, watch out for the threats coming from the cyber space, develop its information warfare abilities, and increase the cyber defense capacity.

It can be claimed that PRC wants to develop its military capacity through benefitting from the opportunities and abilities based on cyber space amply and, moreover, it aims to contribute to the economic development of the country by using these opportunities for industry and technology espionage.

---

[38] See more at: Bryan Krekel, ***Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage***, (Report by Northrop Grumman, http://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-066.pdf), (Accession Date: 17.09.2017), p. 44.

5. Regulations of the PRC for the Control of the National Cyber Space Area

The PRC enforces some measures to provide the cyber defense systematics through sophisticated methods, besides developing an efficient cyber-attack capacity. In this context, the Cybersecurity Law, which was put into force on 1 June 2017 in order to provide cyber security of the PRC, shall be examined, as it reflects the contemporary situation in the country. In this respect, the Cybersecurity Law consists of the regulations on the following subjects:[39]

• The Cybersecurity Law pays more attention to the protection of personal information and individual privacy regarding personal information protection. It standardizes the collection and usage of personal information. Enterprises should focus not only on "data security", but also on "individual privacy protection", which is of greater significance. Some measures were taken towards keeping the personal information of the PRC citizens secure; especially the commercial activities of the foreign global companies, which procure the personal information of the PRC citizens, are kept in control and standards were set by this regulation.

• This Law presents clear definitions of network operators and security requirement regarding these network operators. Most of the larger financial institutions may become "network operators". There are mechanisms for auditing of the commercial activities of the foreign network operators active in the PRC and thus resisting against the cyber espionage activities, which may rise through these companies.

• This Law places higher demands on the protection of critical information infrastructure. It specifies the scope of crucial information infrastructure. It also have the objective of protection of the critical infrastructures of the PRC and aims to increase the cyber defense capacity

[39] See more at: KPMG, ***Overview of China's Cybersecurity Law***, https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf, (Accession Date: 20.09.2017).

of the country against extensive cyber-attacks against the PRC.

• Foreign enterprises and organizations normally need to transfer information outside China due to the restrictions on the transfer of personal information and business data overseas. The Cybersecurity Law stipulates that sensitive data must be stored domestically.

• Penalties for violating the Cybersecurity Law include the suspension of business activities; serious action may lead to the closing of business or the revocation of licenses in line with penalties put into enforcement. The maximum fine may reach RMB 1.000.000.

As is seen, the official authorities of the PRC obtain extensive powers on the issue of control over the internet through the law in question. The responsibilities of the internet operators are increased in connection with providing conformity between the service they give and these regulations; and this law puts an obligation over the individual users to use their real names in their transactions in the internet. The first global company, which faced the compelling provisions of this law, has been Apple. In this respect, the PRC government has warned Apple to remove the VPN[40] applications in the AppStore in PRC in July 2017. Amazon, another leading company in the world, has informed their customers about cancelling its services if the use of unapproved VPN's is detected, in accordance with this law.[41]

There are also other steps taken by the PRC to make its cyber defense stronger. Some of these steps include the banning of some social media applications originating from the Western world; encouraging the use of national social media applications; and banning some websites altogether. For example, PRC government has banned the operations of Facebook with a decision taken in 2009, which was a

[40] VPN is the abbreviation of the term Virtual Private Network and it is a service, which enables you to connect to the internet via another IP address. VPN makes your connection secure and enables your connection, passwords, and identity to be hidden while connecting to any network.

[41] See more at: Yeni Medya, ***Çin'in Büyük Güvenlik Duvarı:Sansürde 21 Yıl***, https://yenimedya.wordpress.com/tag/buyuk-guvenlik-duvari/, (Accession Date: 21.09.2017).

very popular website in those days. The main reason of this ban is to prevent the social movements, which might rise through this social media platform. Moreover, after 2009, the PRC government has tried to popularize the use of national and local social media applications through investment and incentive plans and a significant progress has been made by the year 2018. Also, it should be known that the usage of national and local social media applications in PRC is under serious auditing and control. The ban on Facebook was followed by the ban on other social media applications having foreign origins, such as Twitter and Snapchat. Moreover, CPC has banned the commercial internet applications, which build friendship, through comprehensive and strict internet regulations enforced in 2010 and it has also regulated the use of internet in public spaces and taken precautions against opening web page or blog.

There is another very significant project, which the PRC has put into force to control the cyber space. This is called "the Great Firewall of China", which is officially known as "Golden Shield Project". This project is the Chinese government's project for internet censorship and surveillance. It was initiated by the Ministry of Public Security (MPS) in 1998 and has been updated periodically. If we take into consideration the fact that an efficient and sophisticated initiative like the Golden Shield Project has been put into force in the late 1990's, which is the time when internet has just begun commercializing and civilizing, it shall be interpreted as a really important development in showing that PRC has reached the opportunity and ability towards increasing its cyber defense capacity in the cyber space by these years.[42]

On the other hand, the project in question is used by MPS actively today, depending on the three-stage systematic stated below.

[42] See more at: Standfort, ***The Great Firewall of China: Background***, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformation China/the-great-firewall-of-china-background/index.html, (Accession Date: 20.09.2017).

These stages are operated as indicated below:[43]

I. Stage : Blocking the Domain Names and IP Addresses.

II. Stage : Censorship on Keywords; in other words, if any content is a pre-detected "critical" by the government, blocking of this message.

III. Stage : The detection of VPN's; in other words, if they are used, taking criminal action against this.

Conclusion

The attacks originating from cyber space has reached to a dangerous and sophisticated level due to the developments in the internet and network technologies today. Within this scope, cyber threats are seriously and negatively influencing the national and economic security of the countries. It is obvious that developments based on internet and network technologies will influence the entire world profoundly. Civilianization and commercialization of the internet as of 1990's is followed by important progress in all areas of telecommunication technologies, and especially smart phone technologies. The opportunities and conveniences provided by the internet have resulted in the formation of a new power factor in political, military and economic life, besides everyday life. This also has led to discussion on the new concepts, which are identified as cyber space and cyber security, in the security studies and analyses.

Warfare, attack, and defense strategies and plans of the countries have started to evolve into an incredibly sophisticated and complicated structure as a result of technological developments based on internet. We also face with ordinary internet users as asymmetrical threat risks due to the new technical possibilities as a result of widespread use of internet all over the world. All these developments have increased the activities of individual or state-sponsored hackers in global scale; the countries, non-governmental actors and individuals are faced with new

[43] See more at: Yeni Medya, loc. cit.

concepts and threat risks such as "hacking" and "leaking".

On the other hand, the US, RF and the PRC, which are the hegemonic powers in the global system within the scope of the current political, economic, and military possibilities, consider the cyberspace-based developments as new possibilities to keep their skills and even to increase the level of their skills in order to develop their military capacities. In this context, besides the great powers in question, all the countries in the world have accelerated their strategies and plans towards developing their cyber-attack and defense capacities within the possibilities and abilities in the cyber space, which is an art factual digital area.

In this context, countries have started to change their classical security understandings as a result of the enormous developments in the informatics and information technologies. The objective of taking measures against new threat foci, which have become asymmetric because of the anarchic and unanimous structure of the cyber space, has been emphasized in the countries' new security understanding. Now, setting up cyber space activity as a new field of struggle towards the final end of providing the security of the states has become very important in order to ensure the national security of a state. In this sense, countries want to benefit from these opportunities in order to primarily secure themselves against the cyber-attacks, espionage and manipulation possibilities supported with new generation techniques based on network technologies and subsequently to realize their objectives within their national interests.

The PRC has started to spread on effort to reach an efficient cyber-attack and defense capacity within the plans manifested in the late 1980's by following the developments in question. Thus, the PRC has become an efficient cyber power in the cyber space today.

The PRC also has tried to develop its cyber security strategy, having the purposes of enabling economic growth, developing its military capacity, procuring globally newly emerged technologies within cyber espionage operations, and enabling the security and continuation of the current internal system in which CPC is at the center. This effort is not

an unjust political approach regarding the national interests of the PRC, when it is compared to the similar plans of other countries in the international system and evaluated within the realpolitik paradigms. In this respect, the PRC authorities have taken the cyber space, which has been developed beginning from the ends of the 1980's, when the civilianization and commercialization of the internet began, into consideration with its suitable opportunities in commercial and military areas and they also have seen the cyber space as an area, which consists of serious threats against internal and external security, and thus they have started to establish their plans in this direction.

On the other hand, since every step taken by the PRC in the field of cyber security have impact on the structure of the world's largest internet community; it shall be monitored by the rest of the world. In this context, it shall be considered that the PRC wants to have over its territory and to accelerate its efforts on creating an alternative to the West by establishing and maintaining the opponent politics against the advantages, which Western world and especially the US have.

It can be expected that Shanghai Cooperation Organization (SCO), to which the PRC has contributed with the aim of influencing the international system through its opposition to the US and Western countries within its foreign political interests, will maintain its main feature of being an international ground for the PRC's attempts to develop hegemony in the cyber space field via an interaction with the RF in the future.

It shall also be expected that the PRC will not loosen its control over the internet through the laws which it enforced recently and that it may strengthen these laws in necessary conditions in order to control the possible opponent social and separatist movements by keeping the permanent organization based on the CPC. It is possible that the PRC will maintain its control over the investments of informatics companies, social media applications and internet-based brands originating from the Western countries in short and medium term.

Özet

Çin Halk Cumhuriyeti (ÇHC), 1980'lerin sonlarına doğru ortaya konan planlamalar kapsamında etkili bir siber kapasiteye ulaşmak için ciddi çaba göstermeye başlamış ve günümüzde siber uzayı domine etme imkân ve kabiliyetine sahip etkili bir siber güç haline gelmiştir. Bu makalede genel ve soyut yaklaşımlarla değerlendirdiğimiz üzere, ÇHC ekonomik büyümesini sağlamak ve askerî kapasitesini artırmak için etkili bir siber güvenlik stratejisi geliştirmeyi önemli bir hedef olarak belirlemiştir. Bu hedefini gerçekleştirmesi için planlamalar ve stratejiler geliştirmek de ÇHC yönetimi tarafından güvenlik ve dış politika önceliklerinden biri olarak tespit edilmiştir.

Bu noktada güvenlik ve dış politika önceliklerine bakıldığında, ÇHC yönetiminin, henüz tam anlamıyla bir süper güç olmadığının farkında olarak, yeni stratejiler belirlediği görülmektedir. Ancak ÇHC'nin nihai hedefi süper güç olmaktır. Bu itibarla son yıllarda ÇHC'nin uluslararası ilişkilerde kendine olan güveninin arttığı ve girişkenliğinde görünürde bir artış gerçekleştiği de ileri sürülebilir. Öte yandan, ÇHC'nin siber güvenlik stratejisinin söz konusu tespit ve değerlendirmeler doğrultusunda şekillendiği de iddia edilebilir. Bu itibarla, ÇHC genel olarak ekonomik büyümesini sağlamak, askerî kapasitesini geliştirmek, küresel düzeyde yeni gelişen teknolojileri siber espiyonaj operasyonları kapsamında temin etmek ve Çin Komünist Partisi'nin (ÇKP) merkezde olduğu mevcut iç sisteminin güvenliğini ve devamlılığını sağlamak için siber güvenlik stratejisini planlamaktadır. Diğer bir deyişle, ÇHC'nin siber güvenlik stratejisinin analizi ile aynı zamanda ÇHC'nin güvenlik ve dış politika stratejilerinin de bir nevi tahlili yapılabilecektir.

Bununla birlikte, sahip olduğu büyük nüfus, geniş internet altyapısı ve topluluğu dikkate alındığında ÇHC'nin siber güvenlik stratejisi kapsamında attığı her adımın bir yandan küresel siber uzay alanını da etkilediği hatırda tutulmalıdır. ÇHC'nin siber güvenlik stratejisinin tüm detayları ile irdelenmesi, uluslararası ilişkiler disiplini ve siber uzay çalışmaları açısından önemlidir.

Gelecek dönem için bir perspektif oluşturulmaya çalışılması halinde ve ülkenin nüfus ve yüzölçümü büyüklüğü ile yıllardır ülkeyi yöneten yapının oluşturduğu yerleşik nizam dikkate alındığında, ÇHC'nin siber güvenlik stratejisi kapsamında ortaya koyduğu hedeflerin olumlu sonuçlarına tam anlamıyla ulaşması zaman alabilecek gibi gözükmektedir. Bu nedenle de ÇHC'nin, siber uzayda Amerika Birleşik Devletleri (ABD), Rusya Federasyonu (RF) veya Kuzey Atlantik Antlaşması Örgütü (NATO) üyesi diğer devletlerden biri ile yaşayabileceği potansiyel siber mücadele süreçlerinde, tıpkı diğer dış politik sorunlara bakışında olduğu gibi, tam anlamıyla etkili bir küresel aktör oluncaya kadar daha kontrollü bir siber güç profili izleyeceği de ileri sürülebilecektir.

Öte yandan, ÇHC'nin siber güvenlik alanında attığı her adımın, sahip olduğu dünyanın en büyük internet topluluğunun yapısında da değişikliklere neden olacağından, dünyanın geri kalanı tarafından yakından takip edilmesi gerekmektedir. Bu anlamıyla bakıldığında, ÇHC, küresel bilişim şirketleri için çok önemli bir pazardır ve ulusal siber uzay alanı ile ilgili yaptığı her hamle ve değişiklik söz konusu aktörler ve bu aktörlerin merkezlerinin yer aldığı devletler tarafından da dikkatlice izlenmektedir.

Bu noktada, ÇHC'nin küresel internet alanının yönetimi noktasında kendi güvenlik öncelikleri ve küresel ticari çıkarları dâhilinde başta ABD olmak üzere Batı dünyasının sahip olduğu avantajlara karşı muhalif politikaları devam ettirerek, Batı'ya karşı alternatif yaratma çabalarına hız vereceği ve kendi egemenlik alanını genişletmek isteyeceğinin de dikkate alınması gerekmektedir. ÇHC'nin bu yöndeki siber güvenlik alanına dair planlamalarının da siber uzayda ABD öncülüğündeki Batılı devletler ile siber rekabeti artıracağı da açıktır.

Bibliography

Books

DARICILI, Ali Burak, ***Siber Uzay ve Siber Güvenlik; ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi***, Bursa, Dora Yayıncılık, 2018.

TIMOTHY, Thomas L., ***Three Faces of the Cyber Dragon***, Fort Leavenworth, KS, Foreign Military Studies Office, 2012.

TZU, Sun, ***Savaş Sanatı*** (Translated by Pınar Erturan), İstanbul, Remzi Kitapevi, 2016.

ÜNAL, Ahmet Naci, ***Siber Güvenlik ve Elektronik Bileşenleri***, Ankara, Nobel Yayıncılık, 2015.

Articles and Book Chapters

DARICILI, Ali Burak, "Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi", ***Journal of International Studies***, 1 (1), 2017, pp.1-24.

DARICILI, Ali Burak and Barış Özdal, "The Analysis on the Instruments Forming the Cyber Security capacity of Russian Federation", ***Bilig***, (83), Autumn 2017, pp. 121-146.

INKSTER, Nigel, "Chinese Intelligence in the Cyber Age", ***Survival: Global Politics and Strategy***, 55 (1), 2013, pp. 45-66.

Reports

CHANSORIA, Monika***, Informationising' Warfare: China Unleashes the Cyber and Space Domain***, (Paper by Centre for Land Warfare Studies), http://www.claws.in/images/publication_pdf/1270592252MP_20.pdf, (Accession Date: 12.09.2017).

China Copyright Media, ***National Cybersecurity Strategy***, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/ (Accession Date: 14.09.2017).

COSTELLA, John, ***The Strategic Support Force: China's Information Warfare Service***, The Jamestown Foundation, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=45075&cHash=9758054639ab2cb6bc7868e96736b6cb#.V6RA_Lt95aQ (Accession Date: 17.09.2017).

FEAKIN, Tobias, 2013, ***The Cyber Dragon***, (Report by the Australian Strategic Policy Institute, 2013), https://www.aspi.org.au/publications/special-report-enter-the-cyber-dragon-understanding-chinese-intelligence-agencies-cyber-capabilities/10_42_31_AM_SR50_chinese_cyber.pdf (Accession Date: 16.09.2017)

GRIFFITH, Samuel B., ***Communist China's Capacity to Make War***, (Published by the Council on Foreign Affairs), https://www.foreignaffairs.com/articles/asia/1965-01-01/communist-chinas-capacity-make-war (Accession Date: 16.09.2017).

KPMG, ***Overview of China's Cybersecurity Law***, https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf, (Accession Date: 20.09.2017).

KREKEL, Bryan, ***Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage***, (Report by Northrop Grumman, http://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-066.pdf (Accession Date: 17.09.2017).

LINDSAY, Jon, ***Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy***, (Report from Workshops held at the University of California, San Diego April 2012), https://ndc.gov.bd/lib_mgmt/webroot/earticle/1476/China_and_Cybersecurity.pdf (Accession Date: 16.09.2017).

PAGANINI, Pierluigi, ***China admitted the existence of Information warfare units***, http://securityaffairs.co/wordpress/35114/security/china-admit-cyber-army.html (Accession Date: 16.09.2017).

PATTON, Diane E., ***Evaluating U.S. and Chinese Cyber Security Strategies Within a Cultural Framework***, (A Research Report Submitted to the Faculty in Partial Fulfillment of the Graduation Requirements for the Degree of Master of Operational Arts and Sciences), April 2016, http://www.dtic.mil/dtic/tr/fulltext/u2/1031380.pdf (Accession Date: 12.09.2017).

QIAO, Liang and XiangsuiWang, 1999, ***Unrestricted Warfare***, (Unofficial translation of the book is available at http://www.c4i.org/unrestricted.pdf), PLA Literature and Arts House.

RSAC, ***Comparative Study: Iran, Russia & PRC Cyber War***, https://www.rsaconference.com/writable/presentations/file_upload/hta-w01-comparative-study-iran-russia-prc-cyber-war_copy1.pdf (Accession Date: 15.09.2017).

SEGAL, Adam, ***What to Do About China's New Cybersecurity Regulations?***, https://www.cfr.org/blog/what-do-about-chinas-new-cybersecurity-regulations (Accession Date: 14.09.2017).

Standfort, ***The Great Firewall of China: Background***, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html (Accession Date: 20.09.2017).

STEVENS, Tim, ***Breaching Protocol: The Threat of Cyberespionage***, Academia.edu, http://www.academia.edu/1158361/Breaching _Protocol_ The_Threat_of_Cyberespionage (Accession Date: 16.09.2017).

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), China and Cyber Attitudes, Strategies, Organizations, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf, (Accession Date: 13.09.2017).

USNI News, ***China's Military Strategy***, https://news.usni.org/2015/05/26/document-chinas-military-strategy, (Accession Date: 14.09.2017).

Xinhuanet, International Strategy of Cooperation on Cyberspace, http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm (Accession Date: 14.09.2017).

Yeni Medya, ***Çin'in Büyük Güvenlik Duvarı:Sansürde 21 Yıl***, https://yenimedya.wordpress.com/tag/buyuk-guvenlik-duvari/ (Accession Date: 21.09.2017).