Journal of Political Sciences & Public Affairs

Nurkulov, J Pol Sci Pub Aff 2017, 5:4
DOI: 10.4172/2332-0761.1000307

Short Communication Open Access

New Cyber Strategy of China and the Alterations in the Field

Nurkulov NO*

University of World Economy and Diplomacy, Tashkent, Uzbekistan

***Corresponding author:** Nurkulov NO, University of World Economy and Diplomacy, Tashkent, Uzbekistan, Tel: +998939003434; E-mail: nurshod.96@gmail.com

Received date: September 16, 2017; **Accepted date:** October 31, 2017; **Published date:** November 06, 2017

Introduction

Contemporary world politics has to tackle with various issues ranging from terrorism of different kinds to "information wars". Today's world is very much complicated and bringing about new spheres for actors to exercise, to compete and even to battle.

There is not a single power center that can drive the globe. Its number grew periodically following the collapse of former super power USSR. One of the states becoming a leader and locomotive of world economy is People's Republic of China. Today's China dares to compete with any super powers including the USA in majority of fields.

Under the development of technologies and industry the world is getting digitalized. This means we have 2 personalities - in reality and in cyberspace. At first glance digitalized world is easy to conceive. Because, you can easily store your data on internet or save it in your personal computer. However every single innovation has both pros and cons. The more developed the country the more developed cyberspace it possess and the data including sensitive one is always at risk to be touched by others. This is called hacking [1].

PRC has one of the most developed hacking systems on the globe. Especially in recent years Chinese hackers are captivating international concerns regarding actions they are carrying out. China has its own claims on the usage of internet and the protection of users involved. The United States - the birthplace of internet is in most cases primary target for China and this in turn raises the rhetoric question: Why China needs the US? To answer this question we have to deeply overhaul the development of Chinese internal and foreign cyber policy [2].

On the whole this research work is dedicated to take a close look at the Chinese cyber policy from home to global.

Main Part

Part I. New phenomenon - cyber space

China in cyber space: dynamics of development: On September 20, 1987, Professor Qian Tianbai sent China's first E-mail titled "Crossing the Great Wall to Join the World," marking the beginning of the use of Internet by Chinese.[1] In October 1990, the Chinese domain zone .cn was registered, and in the same year the e-mail service from this domain zone officially opened.[2] In 1994, the first Internet connection was made via the 64 bit/s Sprint line, and China was officially recognized by the international community as a country with a full set of Internet functions. Today the .cn zone became the record holder for the number of domains registered in it.[3]

Sun Tzu the Chinese strategist and scholar in his famous treatise "The art of war" expressed the main idea of the Chinese strategy according to which "…to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting".[4] Despite the past centuries, wisdom has not lost its relevance. Leading world powers seek to confront the enemy with bloodless methods, and instead of weapons increasingly use information technology and resources. But the palm of primacy in the information war is firmly preserved by China [3]. This is evidenced by the data and reports of various international and interdepartmental commissions investigating the trends in the development of modern information and communication technologies (ICTs) and the resulting threats to global security.

In 2012 on the Cyber-power Index compiled by the Economist Intelligence Unit and the consulting company Booz Allen Hamilton, China took only 13th place.[5] Does this mean that the data of the Western special services on the cyberspace of the PRC contradict the views of the compilers of the ratings and the Chinese themselves? Not at all. China realizes that in the event of a direct confrontation with especially the United States, its army and weapons are not yet able to provide an adequate response [4]. Therefore, in order to achieve and maintain parity with the West, the authorities are actively engaged in the development of cyber weapons, which in the case of an attack on China can disable the entire information infrastructure of the enemy.

Reducing dependence on Western ICT is seen as one of the important means of ensuring cyber security of the PRC.[6]

Currently, the Internet in China is very popular: at the end of December 2016 the number of Internet users in the country was 732 million people and as was mentioned above .cn zone became the record for the number of registered domains in it.

The rapid development and growing popularity of the Internet in China bore dual problem for the Leaders of the Communist Party in the 1990s. On the one hand, the country's authorities did not want to lose control over the situation in the country, on the other, the tasks of

1 "Evolution of Internet in China". China Education and Research Network. 01.01.2001.

2 "Internet in China. Reference". RIA News. 01.13.2010 (RUS).

3 Galiya Ibragimova. "PRC strategy in the field of internet management and ensuring the information security". Security Index No. 1 (104), Volume 19. p. 170 (RUS).

4 The art of war by Sun Tzu. English version translated by Lionel Giles, originally published in 2010. p. 9.

5 Bob Gourley. The Cyber Power Index. 01.26.2012.

6 Galiya Ibragimova. "PRC Strategy in the field of internet management and ensuring the information security". Security Index No. 1 (104), Volume 19. p. 170 (RUS).

economic modernization, introduction of advanced technologies, and the alleviation of social problems were acute [5]. There was an understanding within the political elite of the country that the solution of these problems largely depended on the level of penetration of ICT into all spheres of public life.

Interactive technologies are an effective tool that can facilitate the work of social and state institutions as much as possible and create a kind of virtual democracy that has never been seen before in a country with a huge and diverse population [6]. But the Internet is very sensitive to the external influences of technology. Its free functioning in China would mean the penetration of ideas aimed at discrediting the political system of the state. The events in Tiananmen Square in 1989[7] made the country's leadership very sensitive to modern technologies. Then, through information resources, in particular the media, the West managed to shape the image of the PRC as an autocracy, where human rights are severely restricted [7]. This was not quite strange, I reckon. For these reasons, the Chinese government could not decide for a long time what position to take in relation to the Internet. But in 1996 the state gave a go-ahead for the development of a global network in the country[8], and interactive technologies were included in the official plans for the development of Chinese science and technology.

China's strategy for the implementation and development of Internet technology is different from the Western approach [8]. "The Internet is a tool of work, not a means of time spending"[9],[10] - this slogan, widely spread in the country, clearly reflects the authorities' attitude to new means of mass communication.

The Chinese regime has attempted to impose greater control over internal networks, both to suppress domestic opposition and to block penetration from outside the country. It has surrounded the country with a Great Firewall[11], also referred as the Golden Shield Project, which is an Internet censorship and surveillance project operated by the Ministry of Public Security (MPS)[12].

Mastering with networking techniques by the Chinese, as well as obtaining information useful to the nation, according to the authorities, can create new jobs, raise the standard of living of the population, accelerate the development of backward regions, form a new progressive Chinese nation, which means making China a self-sufficient power and Help it to take the leading positions in the world in all spheres of life [9].

China's Internet strategy at the first stage was based on borrowing the technological achievements of developed countries and adapting them to the specifics of their own economic, political, social and cultural development. At the second stage, the Chinese leadership began to create high-tech industrial zones and technology parks, where Internet technologies developed and technical personnel were brought up.[13]

In November 2005, China adopted the State Strategy for the Development of Informatization for 2006-2020.[14] The main directions of the development of the Internet were formulated in it. An important task was the promotion of the Internet in the economy to adjust the economic structure, as well as the transformation of the method of economic growth and the promotion of informatization for the construction of a harmonious society. However, among the first tasks that the Internet is called upon to address is the improvement of the quality of medicine and the access of the broad masses of Chinese to education [10-13].

The Government encourages the use of the Internet for research and business development. An important direction of China's policy was also the introduction of e-government.

The control methods that exist in China do not at all mean that the Internet in the country lags behind the western trends in the development of the global network. China's Internet governance system is very flexible and provides for various relaxations for certain categories of users: scientists, media workers, businessmen, including foreign investors [14]. The Chinese market of Internet services is one of the fastest growing, which especially attracts the attention of investors.

Hong ke – The red hackers

Any attempt to comprehend the problems of cyber security lies in the absence of a single terminology base. In this regard, it is necessary to clearly delineate and dilute the notions of cyberspace and the information space; cyber security and, on the other hand, information and information-psychological security (as well as any other activities whose ultimate goal is to influence people, groups of people or society as a whole through information and communication technologies).

The use of an information space to influence minds is not equivalent and is not even directly related to the impact of ICT on software and hardware, information and communication networks, as well as information transmitted in such networks [15]. We have to distinguish the principle distinction between actions in cyberspace and actions in the information space. Actions in cyberspace are limited with internet, computer lines and more precisely, an electronic environment in which any actions with information and interaction are carried out by using digital signals. Whereas actions in information space is far wider concept and information can be demonstrated in any space proper for delivering[15,16].

7 This day in history: Jun 04. "Tiananmen Square massacre takes place".

8 "Evolution of Internet in China". China Education and Research Network. 01.01.2001.

9 Galiya Ibragimova. "PRC Strategy in the field of internet management and ensuring the information security". Security Index No. 1 (104), Volume 19. p. 171 (RUS).

10 Galiya Ibragimova. "PRC Strategy in the field of internet management and ensuring the information security". Security Index No. 1 (104), Volume 19. p. 171 (RUS).

11 James van de Velde. "War in Peace" The American Interest. 09.06.2016.

12 Desmond Ball. "China's Cyber Warfare Capabilities". Security Challenges, Vol. 7, No. 2 (Winter 2011) p. 99.

13 Ibid. p.171.

14 Zhongzhou Li." China's Informatization Strategy and its Impact on Trade in ICT Goods and ICT Services". Geneva 4-5 December 2006.

15 Yakushev Mikhail Vladimirovich, Chairman of the Board, PIR Center. "Cyberspace and military conflicts: doctrinal approaches to terminology". The Russian Center for Policy studies. 13.12.2013 (RUS).

US military analysts rank Huawei Technologies (one of the largest companies in the country, specializing in telecommunications) as the main threat to US security, not only in the information, but also in the military sphere.[17] This is due to the fact that the company maintains close ties with the Chinese military. In particular, the founder and permanent head of Huawei Technologies, Zheng Zhenfei served in the People's Liberation Army of China (PLA) in before. Based on this and many other similar facts, conclusions are drawn that Huawei's technologies, including those in the United States, include hardware bookmarks and other malicious spyware[18].

The spread of malware is not the only harm that is attributed to China in cyberspace. In the reports of Western intelligence services, the PRC is called one of their main countries, from which the threats of information security originate [16]. China cannot, as before, show its ignorance and innocence in conducting cyber-attacks and intelligence in the US cyberspace. According to Northrop Grumman[19], which was preparing a report for the US-China commission on economic and security relations "Occupying information height: China's is acquiring ability to conduct computer network operations and cyber espionage," the Chinese army already has units specializing in conducting operations in the Cyberspace[20]. The existence of a division of cyber war, which is called the Blue Cyber Army, was openly acknowledged by Chinese Defense Minister Geng Yangsheng[21222324]

The effectiveness of Chinese cyber-units is due to close cooperation between government structures, military and hackers. The Chinese military see the success of modern fighting in the ability to control information and information systems of the enemy.

Northrop Grumman's report reflects specific doctrinal intentions, as well as information on China's financial support for systematic cyber espionage. The main provisions of the information warfare strategy are reflected in the Chinese Military-Political leadership. They were included in the document in 2002, when the PLA announced an increasing need to confront enemies in high-tech wars. At the same time, the main guidelines of China's defense policy were formulated, with a special emphasis on the modernization of the armed forces through their informatization. In the document for the first time appeared the formulation for "Fighting Local Wars Under Informationized Conditions", necessitating the transformation of the armed forces of China.[25]

Chinese hackers call themselves as hongke (red guest) by analogy with the Chinese word for hacker - heike (black guest). In 1999, after American aircraft mistakenly bombed the PRC embassy in Belgrade[26], they organized attacks on US government websites, which resulted in the first hacked website of the White House.[27] Similar actions were taken in May 2001, when a Chinese fighter and an American reconnaissance aircraft collided over the island of Hainan.[28] According to the estimations of the Chinese themselves, 1036 American sites were hacked, including 18 military and 39 government sites then.[29]

By and large, as the economic capacity grows China demonstrates all possible tools in order to prevail and overcome the barriers in the front [18-21]. Barriers in this extend could be some competing states such as, USA, India, Vietnam and others. This is especially carried out in terms of military objectives and sometimes referred as espionage and the government is used to be viewed as aggressive in cyber policy by Western scholars and policymakers. However this trend is on the verge of shift due to the adoption of the first ever in history PRC National Cyberspace Security Strategy. In the next chapter I will examine it further and more detailed.

Part II. National cyberspace security strategy

(i) Expected alterations in the cyber policy framework:

On December 27th, 2016 Chinese government announced the National Cybersecurity Strategy.[30] The strategy consists of 4 chapters and each chapter includes subchapters.

I. Opportunities and challenges

II. Objectives

III. Principles

IV. Strategic tasks.

16 Yakushev Mikhail Vladimirovich, Chairman of the Board, PIR Center. "Cyberspace and military conflicts: doctrinal approaches to terminology". The Russian Center for Policy studies. 13.12.2013 (RUS).

17 Galiya Ibragimova. "PRC Strategy in the field of internet management and ensuring the information security". Security Index No. 1 (104), Volume 19. p. 175 (RUS).

18 "A former Pentagon analyst said that China can block the entire telecommunications mechanism on equipment that it sold to the US". Military-political review. 13.06.2012 (RUS).

19 Northrop Grumman - One of the most high-tech companies of the US military-industrial complex engaged in developments in the field of electronics and information technology, aerospace, shipbuilding, etc. In addition, the corporation is developing advanced weapons for the US Department of Defense, as well as research aimed at improving the means and methods of protecting information.

20 Galiya Ibragimova. "PRC Strategy in the field of internet management and ensuring the information security". Security Index No. 1 (104), Volume 19. p. 176 (RUS).

21 "In China, they created a detachment of cyber warriors". 05.27.2016 (RUS).

22 Ibid.

23 Shane Harris. "China Admits It Has a Cyber Army". Real clear world. 03.18.2015 "China Reveals Its Cyberwar Secrets". 03.18.15.

24 Jason R. Fritz. "China's Cyber Warfare: The Evolution of Strategic Doctrine". Lexington books. USA-2017. p. 48.

25 Bryan Krekel, Patton Adams and George Bakos. "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage". Northrop Grumman Corp. 2012. p. 14.

26 PETER LEE. "The Bombing of the Chinese Embassy in Belgrade in 1999, Reconsidered". Counterpunch. 05.25.2015.

27 "Hackers attack U.S. government Web sites in protest of Chinese embassy bombing". CNN. 05.10.1999.

28 "Pro-China Hackers Invade US Govt Websites". China Daily 04.30.2001.

29 Alexander Gabuev. "Yellow cyber threat China is preparing for the wars in the network". 15.02.2011 (RUS).

30 Paul Rosenzweig. "China's National Cybersecurity Strategy". 12.27.2016.

First chapter gives the general view on the core opportunities and challenges. For in instance cyberspace is gaining more ground day by day, new channels for the dissemination of information, new spaces for production and life, new drivers for economic development, new carriers for cultural flourishing, new platforms for social governance, new territories for national sovereignty and finally new nodes for interaction and cooperation are becoming real because of it. Cyberspace is either can serve as grave challenges [22]. Cyber penetrations harm political security, cyber-attacks threaten economic security, harmful online information corrodes cultural security, online terrorism, law-breaking and crime are destroying social security, international competition in cyberspace is rapidly unfolding. At the end of the first chapter opportunities are estimated greater though both coexist in cyberspace.

The Second chapter regards to the objectives and it is easy to figure out that all of them are inferred from the Chinese national ideology. Peace, security, openness and order are core objectives of PRC in Cyberspace. The country which set up strict rules for internet usage puts openness as its objective is the point that surprises others. However, basically this openness applies to the following meaning: "Without distinction between large and small, strong and weak, poor and rich, all countries worldwide, and especially developing countries, are to be able to share in development opportunities, share in development outcomes, and participate fairly in cyberspace governance."

One of the crucial points in this strategy is the first principle that sounds: Respecting and protecting sovereignty in cyberspace. No country should engage in cyber hegemonies, uphold double standards, use the network to interfere in the domestic affairs of other countries, or engage in, connive in or support online activities endangering other countries' national security [23]. Peaceful use of cyberspace, governing cyberspace according to the law and comprehensively manage cyber security and development are other 3 principles based on which China conducts its future cyber policy.

Strategic tasks for China in the field are mainly protecting, augmenting ties and cooperating with other states concerning the cyberspace. In addition, resolutely defending sovereignty in cyberspace, resolutely safeguard national security, protect critical information infrastructure, strengthening the construction of online culture, attacking cyber terrorism, law-breaking and crime; perfect network governance systems enhancing cyberspace protection capabilities and strengthening international cooperation in cyberspace are fixed as strategic tasks on the paper.

Within the following strategy PRC is expected to change the way it carried out its global cyber policy [24]. However their attitude towards cyber affairs heavily depends on their partners' behavior and their own real objectives. As I mentioned above Chinese primary target is USA. In late September 2015, Chinese leader Xi Jinping and former the US leader Barack Obama agreed on cooperation in the fight against hackers. But Hacker attacks from China continued even after this agreement. According to the founder of CrowdStrike Dmitry Alperovich, hackers used a program known as Derusbi. Previously, this program was used in attacks on the defense company VAE Inc. and the insurance company Anthem Inc.[31] Recently American experts again claiming that China committed cyber-attack against THAAD which was brought to South Korea to defend from DPRK threats. John Hultquist, the director of cyber espionage analysis at FireEye, told CNN: "China uses cyber espionage pretty regularly when Chinese interests are at stake to better understand facts on the ground".[32]

Following the meeting of Trump and Xi relations in the sphere mitigated.[33] "Financial Times" posted that a Chinese hacker group the Conference Crew, known for targeting US defense and aerospace companies has shifted its focus to critical infrastructure across Asia following a US-China deal on electronic espionage, according to cyber security company Fire Eye [25]. Analyst Bryce Boland, FireEye's Asia-Pacific chief technology officer stated that "The most likely use of the information or access that's being collected is for understanding the adversary and understanding their tactics — who's involved in decision making". Nations where attacks have been recorded include India, Indonesia, the Philippines and Vietnam, while organizations in Hong Kong and Macau have also been targeted, according to FireEye.[34]

It is true that China's demands are growing and therefore the authorities are striving for global dominance and trying to make happen their ever willingness to dominate on the globe. Cyberspace serves as an effective tool to make counterparts cautious.

ii. "Cyber sovereignty" – Chinese global dominance pretentions:

The term "cyber sovereignty" was first used well before the rise of President Xi Jinping and China's Internet czar, Lu Wei (the director of a powerful cybersecurity strategy group comprising China's top leaders) - it first appeared in a government white paper in 2010 [26]. But it really started becoming used heavily after Xi came to power and Lu got his job. They basically made up a new title for Lu — the Cyberspace Administration of China — and a lot of the control of the Internet seem to have become focused in one organization and on one role.[35] China fed up with the control by external forces in the sphere, does not share the existing traditions in regards to internet with the US and like current economic extends trying to implement the space where they would not have to comment all their actions. This concept is also included in recent first National Cyberspace Security Strategy.

China is very critical of the existing international Internet governance regime, where the main functions for assigning names and Internet addresses are assigned to the US-based Internet Corporation for Assigned Names and Numbers (ICANN).[36] In various international forums where Internet governance issues are discussed, representatives of China have always severely criticized ICANN's activities, accusing it of complicity with the Americans. China's rejection of ICANN's activities has intensified after the issuance of

31 "Cyberattacks from China to the US continued after the treaty against hackers". RBC News. 10.19.2015 (RUS).

32 GARETH DAVIES. "Chinese hackers 'tried to infiltrate a company linked to US-built THAAD missile system set up in South Korea'". Mailonline. 04.27.2017.

33 Patrick Tucker. "As Trump Meets China, US Worries About Beijing's Supercomputers and Industrial Espionage". Government Executive. 04.07.2017.

34 Jeevan Vasagar in Singapore and Leo Lewis in Tokyo. "Chinese hackers shift focus to Asia after US accord". Financial Times. 04.27.2017.

35 Ibid.

36 "About the ICANN History Project".

the .tw Taiwan domain, officially considered by China as a province within the national territory[37]. The main requirement of the PRC is the dissolution of the corporation and the creation of a truly international organization that manages the Internet under the auspices of the UN [27,28].

As I mentioned above in recent years, Chinese leaders have pushed the idea of "cyber sovereignty" — the notion that each country's government should maintain independent control over what content is available online within its own borders. Numerous countries censor online content they deem illegal, but cyber sovereignty takes on a new dimension in China, where global web giants such as Google, Facebook, YouTube, Twitter and Instagram are blocked.[38] The government is encouraging Chinese versions of these sites like Baidu and Sina Weibo, to operate in China which has the world's highest Internet connectivity.[39]

PRC is calling its BRICS partners to endorse the idea.[40] India may be reluctant to accept the Chinese model because much of the Indian IT industry is linked to western markets, where the Internet is largely free. Chinese officials maintain that the internet is free in China, and only a small section of websites that "undermine" the country's national interests are banned. But officials did not explain how these international sites hurt China's national interests.[41]

In brief the PRC government aims at augmenting its dominant position in the cyberspace.

Conclusion

Today most of the world populations use internet for different purposes. The development of science and technology is encouraged and sponsored by states. Sometimes the competition between countries may lead to brilliant results but sometimes this may cause the collision and ramifications may be worse than before.

Internet is the achievement of new and recent development of science and technology. 21st century has brought a broad usage of IT in every field.

The word "cyber" is seen to have negative meaning. Indeed this is the same as internet and digital affairs.

Based on the analysis of Internet development trends and cyber policy in China and the methods used to ensure information security, it can be concluded that firstly, the global network in the Middle Kingdom (Zhong Guo -中国 – China in Chinese means Middle Kingdom) is seen as a specific innovation environment within which the formation of a new China and its growth into the world undergo. For this, the country strives to make full use of the economic and propaganda capabilities of the Internet and other interactive technologies. Secondly, main supporter and engine of the Chinese Internet is the state, and only it determines what dangers and opportunities can conceal in the total informatization of a country with a population of more than one billion people. Thirdly, the authorities benefit from the appearance of a relatively cheap mass media, powerful enough in terms of the possibility of influencing foreign audiences and at the same time quite manageable, to limit the reverse effect. Fourthly, a distinctive feature of the Chinese Internet is a clear regulation of not only technical and organizational procedures, but also user behavior in the virtual space. It is not customary to talk about freedom of speech in China at all, and the Internet here is a free zone only theoretically. In fact, users have a number of responsibilities and are forced to reckon with the restrictions imposed on the use of the network by regulatory authorities. Fifthly, in the interests of achieving a leading position in the world arena, China is actively engaged in the development of cyber resources. The PRC leadership is finding it increasingly difficult to show its ignorance and innocence in conducting active intelligence of radio electronic means and penetration into cyberspace of foreign states. The effectiveness of Chinese cyber-attacks is explained by close cooperation between government structures and hackers as I stated above.

To expand China's opportunities in cyberspace, the PLA is actively interacting with commercial organizations and the education sector, which facilitates access to advanced research and technology, including military and dual-use telecommunications systems. Reducing dependence on the information and communication technologies of the West and developing its own innovative capacity are seen as important means of ensuring cybersecurity of the PRC.

"Soft power rests on the ability to set the political agenda in a way that shapes the preferences of others".[42] Joseph Nye's concept is also very much appreciated by the government and Cyberspace for China is also the ground for Chinese propaganda. Through broad investment in Internet technologies, in particular aimed at stimulating the creation of media on the Internet and the development of social networks, China seeks to form a positive image of the state on the international scene and to soften the negative perception of some problems of domestic political development by the foreign audience through the creation of the effect of pluralism of opinions. At the same time, in an effort to expand the information channels broadcasting from China, the authorities of the country are trying to control the impact of foreign media on the Chinese audience. But in an environment where Internet technologies continue to actively develop and are being introduced into the life of Chinese society, it becomes increasingly difficult for authorities to monitor and filter traffic and content.

Cyberspace is wide and the countries involved utilize it as effective foreign policy tool. PRC is one of the strongest hackers land and most of the states including USA always feel threats from them. Feeling as the world's superpower China dares to push its own structure for internet. China is unwilling to change its present cyber policy since its national interests may remain at risk. Since the military might is not as powerful as of some other superpowers, China in the case of direct confrontation banks on its developed digital technologies and experts. Chinese authorities never officially divulge from what country there may emerge threats but it is easy to find out reviewing its policies. And in cyberspace China mainly acts not as there are some threats but

37 Mikhail Yakushev. "Internet-2012 and INTERNATIONAL policy". Security Index No. 1 (104), Volume 19. p. 34 (RUS).

38 Matt Sheehan. "Here's How China's Trying To Rewrite The Rules Of The Global Internet". Huffpost. 12.16.2015.

39 Saibal Dasgupta. "China trying to rope India, Russia in cyber pact against West". Times of India. 03.02.2017.

40 "China offers the BRICS countries the idea of "cyber-sovereignty". Portal Rodon 07.03.2017 (RUS).

41 Ibid.

42 Joseph S. Nye "The paradox of American power: Why the World's Only Superpower Can't Go It Alone". Oxford University Press, 2002, p. 9.

cyber-attacks is seen an instrument to give response against any actions improper to national interests.

All in all PRC has very peculiar stance on these affairs as a whole.

References

1. Jason RF (2017) China's Cyber Warfare: The Evolution of Strategic Doctrine. Lexington books.
2. Joseph SN (2002) The paradox of American power: Why the World's Only Superpower Can't Go It Alone. Oxford University press.
3. Lionel G (2010) The art of war by sun TZU.
4. Desmond B (2011) China's Cyber Warfare Capabilities. Security Challenges 7: 2-99.
5. https://idsa.in/system/files/book/book_ASR2016.pdf
6. https://www.the-american-interest.com/2016/09/06/war-in-peace/
7. Mikhail Yakushev (2012) Identity in cyberspace: towards a global compact. Journal Security Index: A Russian Journal on International Security 18: 33-44.
8. Yakushev Mikhail Vladimirovich Chairman of the Board, PIR Center. Cyberspace and military conflicts: doctrinal approaches to terminology. The Russian Center for Policy studies.
9. Zhongzhou Li (2006) China's Informatization Strategy and its Impact on Trade in ICT Goods and ICT Services.
10. A former Pentagon analyst said that China can block the entire telecommunications mechanism on equipment that it sold to the US. Military-political review.
11. Harris S (2015) China Admits It Has a Cyber Army. Real clear world.
12. Cyberattacks from China to the US continued after the treaty against hackers.
13. CNN (1999) Hackers attack U.S. government Web sites in protest of Chinese embassy bombing.
14. http://www.china.org.cn/english/12150.htm
15. Davies G (2017) Chinese hackers 'tried to infiltrate a company linked to US-built THAAD missile system set up in South Korea.
16. Jeevan Vasagar in Singapore and Leo Lewis in Tokyo (2017) Chinese hackers shift focus to Asia after US accord.
17. Sheehan M (2015) Here's How China's Trying To Rewrite The Rules Of The Global Internet.
18. Dasgupta S (2017) China trying to rope India, Russia in cyber pact against West.
19. Krekel B, Adams P, Bakos G (2012) Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage.
20. (2001) Evolution of Internet in China.
21. About the ICANN History Project.
22. This day in history: Jun 04. (1989) Tiananmen Square massacre takes place.
23. China offers the BRICS countries the idea of "cyber-sovereignty".
24. http://carnegie.ru/2017/10/04/china-and-russia-s-dangerous-entente-pub-73310
25. Gourley B (2012) The cyber power index.
26. Tucker P (2017) As Trump Meets China, US Worries About Beijing's Supercomputers and Industrial Espionage.
27. Rosenzweig P (2016) China's National Cybersecurity Strategy. Lawfare.
28. Lee P (2015) The Bombing of the Chinese Embassy in Belgrade in 1999, Reconsidered. Counter Punch.