Center for Cyber Security and
International Relations Studies

China: An Evolutionary Analysis of its Cyber Strategy

Written by: Tullio Aversa

Abstract

Today we can observe how China has moved ever further in the implementation of its plan to return to being one of the richest and most powerful countries in the world after centuries, but in order to succeed it has to face its various challengers. First of all, the current world ruler: The United States of America.

Among the different battlefields in which these States clash there is the relatively new one of the cyber realm where China is trying to put a spoke in the wheel of its competitors. And precisely in this field, the steps forward made so far in the last twenty years are many and quite considerable.

The very purpose of this paper will therefore be to retrace the various processes that have led China to become that strong international player, feared by the Americans, glancing the decisions and strategies implemented by itself in the IT environment, taking into account the difficulties concerning the finding of certain and valid information due to its reticence in making public many of the official documents in this regard.

Keywords

China, USA, Cybersecurity, Cyberwar, Conflict.

1. Introduction

When man thought he had conquered all the kingdoms of the world: earth, water, air and space, here is a new domain, the digital one of cyberspace[1] and it is in this battlefield that many of those silent wars between states are carried on today.

A kingdom defined by many without a flag and yet the recent history shows us how in reality nations succeed in any case to exploit this land to carry out their plans.

[1] The notional environment in which communication over computer networks occurs. Oxford Living Dictionaries, https://en.oxforddictionaries.com/definition/cyberspace.

A world (that of the Internet) in which United States are still the masters but sees the emergence of other forces in the field as, indeed, China, which is currently recognized as the greatest threat to US hegemony.

The comparison does not concern only possible direct attacks against the enemy, but also an ideological fight.

If on the one hand we have the United States whose aim is to keep a free internet, on the other hand we see China fighting for a nationalization of the web.

Through this action the ultimate goal of Beijing is to eliminate American hegemony in cyberspace, because, as history shows: until a space remains free is the strongest that commands.

To help China in this intent, some key events in recent history have been very helpful, such as:

- The revelations of Snowden, who have unmasked how Washington keeps all American citizens under control;
- The fight against jihadism, in order to block the proselytists of the web.

Therefore, the task of this paper will be to retrace the history of the evolution of cyber in the People's Republic of China, focusing on what is its history and analyzing how China moves today in certain sectors such as cyber-security and cyber-war.

2. History

2.1 General Development

Over the course of time, China has witnessed a huge expansion of its Internet.

The number of users has increased enormously in just a few years, passing from about 384 million users in 2009 to 731 million in 2016, 53.2% of the population[2].

But how did they reach this goal? Surely, we can find an answer in the great economic development of the country. With the growth of the middle and rich class, the demand for information and services of the people has also grown[3].

But proceeding step by step, let's now look at the evolution of the online network from the 90s to today.

The first Chinese internet network was created in 1994 but was still rather slow. It is only a year later that they will have more performing connections, albeit relegated to medium and large cities only.

[2] China Internet Network Information Center, Internet Statistics, https://cnnic.com.cn/IDR/BasicData/index_1.htm.

[3] W. Howlet, "The Rise of China's Hacking Culture: Defining Chinese Hackers", California State University - San Bernardino CSUSB ScholarWorks, 6-2016, p. 35.

But as in every other country in the world, soon the web becomes a meeting place for many people who start to exchange their ideas and consequently also ideas that went against the communist party and its policies.

So, in 1998 the construction of "The Golden Shield" began, commissioned by the Ministry for Public Security, which consists of an instrument to guarantee the security of the nation and its internet network[4].

The program is divided into various sectors managed by different offices, including the Bureau of Public Information and Network Security Supervision, which manages the program called Great Firewall, whose purpose is to check and, in the case, to censor the potentially harmful data to the system who goes in and out of China.

The aim is to increase the instruments and therefore the efficiency of the state police and to guarantee greater defense against external threats[5].

Completed in 2008, although it has already been in operation since before, it has allowed not only to increase the internal and external defenses but also to increase the economy of the country.

The golden Shield, in fact, going to block some of the largest western sites has allowed the emergence of new Chinese companies offering alternative services to the best-known Google, Amazon or Youtube with Baidu, AliExpress, and Youku, just to name a few.

In addition to all this, the shield has allowed the birth of a generation of digital natives particularly good in the use of techniques such as the creation of backdoors[6], firewalls[7] and the use of proxies[8] to be able to see what was hidden behind the barrier imposed by State. Thus, were born the so-called Netizens (from the union of internet and citizens) i.e. those people deeply immersed in the cyber world[9].

While this was very positive, given the formation of many groups of hackers close to the ideas of the party, on the other hand led those who did not agree with their policies of censorship to revolt, also giving rise to harsh revolts as that of 2005 made by student, also in a fairly aggressive way[10].

Today, Beijing's take on the web is still very strong and will probably grow in the next few years, as suggested by what came out from the National Online Propaganda Work

[4] W. Howlet, op. cit., pp. 37-38.

[5] By: Express Web Desk, “What is the Great Firewall of China?”, The Indian Express, 19-07-2017, http://indianexpress.com/article/what-is/what-is-the-great-firewall-of-china-4757848/ .

[6] A backdoor is a technique in which a system security mechanism is bypassed undetectably to access a computer or its data, https://www.techopedia.com/definition/3743/backdoor.

[7] software or firmware that enforces a set of rules about what data packets will be allowed to enter or leave a network, http://searchsecurity.techtarget.com/definition/firewall.

[8] A server that processes requests and forwards information between a client and another server, https://www.thefreedictionary.com/proxy.

[9] W. Howlet, op. cit., p. 42

[10] P. Pan, "Chinese Crack Down On Student Web Sites", The Washington Post, 24-03-2005, http://www.washingtonpost.com/wp-dyn/articles/A61334-2005Mar23.html.

Conference in 2016. Among the points made clear there was indeed that of reinforcing online propaganda. What then actually done[11].

2.2 Chinese Hackers' History

The first notable hacking activities carried out by Chinese groups took place between 1998 and 1999 following the riots in Indonesia against the Chinese minority, which, in a period of economic crisis was accused of holding most of the wealth of the country[12].

This led Chinese hackers to join for the first time in order to help their Indonesian cousins, attacking the government sites of the Jakarta government.

In 1999 the attacks were instead directed against Taiwan following the statements made by the then president Lee Teng-Hui on the "Two-States theory". Also here, the government sites were attacked, beginning the first Sino-Taiwanese war.

This war led to a new cataloging for Chinese hackers different from other groups. In fact, we have:

- Red hackers: politically active;
- Blue Hackers: more interested in the technology itself and in network security;
- Black Hackers: more prone to pure hackers ideal whose sole purpose is to test their skills[13].

In the rest of the world, on the other hand, we have:

- Black hat: immoral hackers dedicated to computer fraud;
- White hat: moral hackers dedicated to making systems more and more secure;
- Gray hat: those who explore the network to fill their curiosity and get noticed by the hacker community[14].

Also, in 1999 the bombing of the Chinese embassy of Yugoslavia took place. This affirms once and for all the birth of the Chinese red hackers, who opened their first site and began to attack all the enemies of the Chinese state (USA, Japan, Taiwan, South Korea, etc...)

Moreover, in 2001 the collision between an American spy plane and a Chinese military jet did nothing but fester relations between countries, and the attacks increased more and more between each other.

In 2003 two very important events represented what in a very similar way we still observe today.

- The attack surnamed "Titan rain" against the US where Chinese hackers managed to steal a lot of sensitive data from some US government sites;

[11] W. Howlet, op. cit., pp. 52-53.

[12] M. Ocorandi, "An Analysis of the Implication of Suharto's resignation for Chinese Indonesians", Worldwide HuaRen Peace Mission, 28-05-1998, http://www.hartford-hwp.com/archives/54b/083.html.

[13] W. Howlet, op. cit., pp. 74-79

[14] W. Howlet, op. cit., p. 56

- The declaration of the red hackers: " “The goal of this community: Is to grieve for the prior generation and to never forget the nation’s shame; to use history as an example for facing the future"[15].

This made it clear that from then on Chinese hackers would face all the enemies of their homeland, placing the USA at the top of their list of goals.

In 2012 there was another major attack against the Americans. Hiding malware Trojans in emails sent to different companies, the Chinese managed to steal terabytes of data regarding the factory secrets of many US industries. Attack considered as the greatest transfer of wealth in history[16].

And if at first, they tried to solve the issue diplomatically, the leak on the NSA’s PRISM project did not help the Americans much in June 2013 in a conference between Obama and Xi Jinping. The project consists in the possibility of intercepting the calls of the entire American population. And in their dialogue, if the American president tried to denounce the Chinese thefts, his Chinese counterpart countered by stating that the US had no right to tell China what was lawful or unlawful to do[17].

To date, Chinese attacks are becoming more precise and targeted, and therefore we must remain extremely vigilant in seeking and blocking any attempts to penetrate our IT systems[18].

3. Analysis of the Chinese’s Cyber Strategy

3.1 Cyber Sovereignty

The aforementioned Golden Shield has effectively entered as part of that idea of Chinese Cyber Sovereignty, i.e. a stronger state control over data flows in the network. A concept, as already mentioned, opposite to that of the American free internet.

This thought is based on two main assumptions:

- Avoiding the unwanted influence of other actors in the cyberspace of another country to prevent them from negatively influencing citizens' ideas;
- Give international organizations a central role on the governance of the Internet and lift the power in the hands of private individuals to give it back to the States and make sure that they can manage their digital lines in a completely autonomous way.

The dependence on Western technologies and their software is considered as the biggest security breach by the PRC, which focuses on greater sovereignty in order to defend its own country from possible attacks by its international competitors.

To confirm this vision, China is adopting a very effective plan. It helps develop the poorest and developing countries, asking them in return for helping them in this fight.

[15] Cit. W. Howlet, op. cit., p. 82.

[16] W. Howlet, op. cit., p. 83.

[17] F. Kaplan, “Dark Territory the Secret History of CyberWar”, Ed. Simon and Schuster, 2016, pp. 114-115

[18] D. Palmer, “Cyberattacks from China: Less numerous but more effective”, zdnet, 21-06-2016, http://www.zdnet.com/article/cyber-attacks-from-china-less-numerous-but-more-effective/.

With the European countries instead argues that Washington uses its domain on the web to control its allies.

And to the accusations made by the United States to want to make the internet a new prison, respond that the goal is not to introduce the concept of control by the government of the web, but to force America to share their power with the rest of the world[19].

However, Beijing's pressures and restrictions on the data flow are getting heavier and since February 2018 the government has forced Chinese TELCOs to apply more stringent controls in order to block VPN[20] services, which allow the more experienced to bypass the Great Firewall controls[21].

3.2 Cybersecurity

In China, between tens and hundreds of thousands of cyber-attacks are recorded each month, most of them from the US, as stated by China's National Computer Network Emergency Response Technical Team and Coordination Center (CNCERT / CC).

This makes the topic of cybersecurity[22] fundamental to the country and its political and economic integrity[23].

Precisely for this reason, Beijing is not only concerned with safeguarding the defense of its infrastructural apparatus, but also with controlling the contents that pass on the network.

Most of the investments in cybersecurity are directed to the construction of infrastructures for censorship and surveillance.

This makes us understand that control is focused on issues such as terrorism, separatism, and extremism.

On the other hand, from a technical point of view, on the direction of the government, it was decided to use as much as possible Chinese products and services in the workplace and to control widespread Western goods that do not yet have a suitable replacement. Any company, such as Microsoft, simply has to let the source code of its products be examined to make sure they are used by the PRC offices. These checks are performed by the China Information Technology Security Evaluation Center (CNITSE)[24].

[19] N. Nagelhus Schia & L. Gjesvik, "China's cyber sovereignty", Norwegian Institute of International Affairs, Policy Brief 2/2017.

[20] A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet, http://searchnetworking.techtarget.com/definition/virtual-private-network.

[21] A. Nepori, "In nome della Cyber-Sovranità, la Cina bloccherà ogni accesso al Web libero", La Stampa, 12-07-2017, http://www.lastampa.it/2017/07/12/tecnologia/news/in-nome-della-cybersovranit-la-cina-blocher-ogni-accesso-al-web-libero-EXKbngNWsJFbMntcIKswxN/pagina.html.

[22] The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this, https://en.oxforddictionaries.com/definition/cybersecurity.

[23] J.R.Lindsay, T.M.Cheung, D.S.Reveron, "China and Cybersecurity", Oxford University Press, 2015, p. 3.

[24] J.R.Lindsay, T.M.Cheung, D.S.Reveron, op. cit., pp. 6-15

But in addition to what are mere precautions taken by the government, we try to observe and understand broadly their strategy in this area.

In 2003 the State Network and Information Security Coordination Small Group (SNISCSG) was born, whose purpose is to develop new information technologies and use them to improve national security. He published Document 27 on the implementation of some cybersecurity policies based on the principle of "active defense"[25] to protect critical infrastructures, to improve the monitoring of the entire Chinese network and to encourage the use of cryptography.

Although the document was essential to understand the points to be taken into consideration, however, the dissolution of the SNISCSG in 2008 made the work disorganized and therefore difficult to implement. But notwithstanding this was reactivated in 2009, the ways in which it operates are still unknown, since its works are kept secret.

However, in 2006 China's 15-year grand strategy (more formally called "The National Program for the Development of Science and Technology in the Medium and Long Term 2006-2020) comes out, which contains the objectives of China for the development of new technologies and increased investment in research and development[26].

The plan is to achieve an investment of 2.5% of GDP in the field of R&D by 2020 but observing the figures for 2015 they were still at 2.1%, which suggests that the goal is still far away[27].

In 2012, however, the State Council's Information Office publishes a new document called "The State Council vigorously promotes informatization development and offers several opinions on conscientiously protecting information security", which continues to point out the disparity between China and the West in the fields of infrastructures, information exchange between the government and industries, and inadequate defense capabilities. Thus, establishing a series of guidelines:

- Securing critical information systems and infrastructures;
- Strengthen the security system of classified information;
- Increase the protection of industrial control systems;
- Safeguarding personal information of Chinese citizens.

The Beijing strategy has always been weak and disorganized at least until 2014, with the establishment of the Central Leading Small Group for Internet Security and Informatization (CLSGISI) that takes care of safeguarding the network as well as

[25] The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy, https://www.thefreedictionary.com/active+defense.

[26] M. Raud, op. cit., pp. 10-12.

[27] Research and development expenditure, The World Bank, https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=CN.

managing information, putting order where there was only chaos before due to the lack of coordination between the numerous offices created by the government[28][29][30].

A further move to increase its cybersecurity was achieved with the entry into force of the Cyber Security Law of the People's Republic of China[31].

Promulgated by the Standing Committee of the National People's Congress on 7 November 2016, it entered into force on the first of June 2017 and among the main features we find:

1. Greater attention to the protection of personal information and individual privacy of citizens;
2. A clearer definition of what the network operators are (network owners, managers, and suppliers[32]) and the security requirements they must meet;
3. Greater protection of critical infrastructures, with particular regard to information infrastructures;
4. A more acute restriction on the transfer of sensitive personal data, which will be kept within the national space;
5. More severe penalties for those who break the law, including the suspension of the activity, their closure or revocation of the license, as well as the payment of a fine up to a maximum of 1 million renminbi.

If on the one hand it improves the security of the country, on the other hand it creates many problems for those companies that have their data collection bases outside China. These, in fact, have moved to ask a postponement in the complete implementation of the law, getting it[33].

3.3 Cyberwar

The cyberwar, that is, the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes[34] it is a type of struggle that is found not only in military conflicts but also within normal political, economic, cultural, scientific and technological competition.

It can be divided into five categories of combat (four offensives and one defensive):

[28] M. Raud, op. cit., pp. 13-15.

[29] T.F.Camponeschi, “Beijing Consensus e Cybersecurity: al via la 3 giorni del World Internet Forum di Wuzhen”, Agenzia Giornalistica Italia, 04-12-2017, https://www.agi.it/blog-italia/agi-china/cina_pechinoworld_internet_forum-3197673/post/2017-12-04/.

[30] A. Spalletta, “La Cina vuole aprire le porte a Internet. Per controllarlo sempre di più”, Agenzia Giornalistica Italia, 04-12-2017, https://www.agi.it/estero/world_internetconferencecina_web-3197168/news/2017-12-04/.

[31] HamChamChina, before: “中华人民共和国网络安全法”, https://cdsglobalcloud.com/wp-content/uploads/2017/02/AmCham-Cybersecurity-Translation.pdf, http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm.

[32] J. Wagner, “China's Cybersecurity Law: What You Need to Know”, The Diplomat, 01-06-2017, https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

[33] “Overview of China’s Cybersecurity Law”, KPMG, February 2017.

[34] https://en.oxforddictionaries.com/definition/cyberwar

1. The first of the offensive categories is cyber-intelligence, which consists in the research and processing of sensitive news and data of interest in and on cyberspace to prevent, detect, contain and combat security threats. This activity is carried out by the bodies involved through the search for important files to understand the intentions of their targets. Even through the use of viruses, Trojans and specific software for hacking when it comes to stealing sensitive information otherwise untraceable on the network;
2. Cyber-paralysis: the search for weak points in the network in order to exploit them to create a paralysis of the system. These attacks are very often concentrated on the nodes of the network and can guarantee large damages with very little investment since they are carried out, for the most part, through DDoS[35] attacks;
3. With the evolution of wireless technologies, it has become increasingly important to work on a stronger and safer integration between cyber and electromagnetic space. In cyberwar this has resulted in attacks aimed at the suppression of wireless signals, the electronic components responsible for sending data for these routes and for intercepting information[36];
4. Cyber-psychology also plays a primary role in cyber warfare strategies and consists in the planned use of propaganda and other psychological operations carried out on the Web, with the main purpose of influencing the behavior of hostile groups in order to favor the achievement of national objectives[37];
5. And finally, we have the cyber-defense: it would be to say the whole of the doctrine, the organization and the activities aimed at preventing, detecting, limiting and countering the effects of the attacks carried out in and through the cyberspace to the detriment of one or more of its constituent elements. Essential to combine good offensive tactics with an equally good defensive one, so as to avoid that the "enemy" can hit in turn through one of the methods listed above.

Although we do not have official documents regarding Chinese strategies in the context of the cyber war we can understand on what basis the Chinese government funds its work by observing which are the points they consider most important.

The focus falls on three main points:

- The network as a coadjutor of the economy of the country and its growth;
- Protect the role and command of the Chinese Communist Party;
- Maintain national stability and security.

[35] Abbreviation for distributed denial of service: An occasion when a computer network or website is intentionally prevented from working correctly, by a very large number of users sending data at the same time, https://dictionary.cambridge.org/it/dizionario/inglese/ddos.

[36] J.R.Lindsay, T.M.Cheung, D.S.Reveron, op. cit., pp. 124-130.

[37] Phil Taylor, “Glossary of Relevant Terms & Acronyms PROPAGANDA AND PSYCHOLOGICAL WARFARE STUDIES”, University of Leeds UK, 1987. https://books.google.it/books?id=jDxPBwAAQBAJ&pg=PA18&lpg=PA18&dq=Glossary+of+Relevant+Terms+%26+Acronyms+PROPAGANDA+AND+PSYCHOLOGICAL+WARFARE+STUDIES+University+of+Leeds+UK&source=bl&ots=zlYnHX2PPI&sig=TpUKD1qQ-1_dOccZCOZvUHdtaEU&hl=it&sa=X&ved=0ahUKEwj_hYTQ5__YAhUFVBQKHeNpAgEQ6AEINjAC#v=onepage&q=Glossary%20of%20Relevant%20Terms%20%26%20Acronyms%20PROPAGANDA%20AND%20PSYCHOLOGICAL%20WARFARE%20STUDIES%20University%20of%20Leeds%20UK&f=false.

It is now clear that the objectives of the PRC will most likely be:

1. Improve the competitiveness of Chinese industry by acquiring the secrets of new technologies produced abroad through cyber-espionage;
2. To weaken party opponents and resist foreign pressures and ideologies;
3. Comply with the detachment that there is in military and technological capabilities with the USA.

For the first point, the aim is to end the current period that sees China as a "factory of the world", dependent on low manufacturing and foreign technologies, to make it by 2049 (one-hundredth anniversary of the foundation of the PRC) one of the countries leaders in scientific and technological fields[38].

Here, espionage acquires great value as it is aimed at helping in achieving the objectives set within the five-year plan 2016/2020, which sees China make profound changes in sectors such as innovation, environment, and agriculture, with the further purpose to have a more open and inclusive growth.

In fact, in a report on global threats for the United States in 2015, CrowdStrike (a private intelligence organization in the United States) pointed out that a large part of China's cyber-attacks against the US were directed in those sectors taken into consideration in the five-year plan that would be activated soon after[39].

The second point is instead protected by continuous checks on the accounts or on the sites of people, agencies or institutions capable of influencing the international and internal debate. This is essential in order to protect the party and its ideals from possible threats.

And, if inside the State the work is done by some programs like the "Great Firewall", outside it is carried out through persistent attempts to break through the pages of these subjects.

Finally, as shown in the 2015 White Paper on Chinese Military Strategy, the Chinese People's Liberation Army (PLA) will have to organize itself to face possible scenarios of war against technologically superior nations. This is why attacks by hackers against the US Department of Defense are so common now.

The slightest sensible data collected could mean a great advantage for Beijing, which could thus be able to anticipate US military plans, accelerate the process of Chinese’s defense modernization and prepare itself in a better way against possible American attacks.

So, it would be a war based on the information[40].

[38] A. Segal, “How China is Preparing for Cyberwar”, The Christian Science Monitor, 20-03-2017, https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar.

[39] D. Denning, “How the Chinese cyberthreat has evolved”, The Conversation, 5-10-2017, https://theconversation.com/how-the-chinese-cyberthreat-has-evolved-82469.

[40] A. Segal, cited article.

4. Conclusion

Cyber is increasingly considered as weapons of mass destruction. Nowadays, there is no nation that does not consider the Internet as a new battlefield and is not adequately equipped to face the struggles already underway in this area, or at least it is not starting to worry about having to do it.

A low defense could lead the unsuspecting State to repent of the choice made, since it is not just a matter of thinking of possible and unlikely war scenarios, but also and above all economic, if not even political.

China that steals industrial secrets from the US is just one of many possible examples: Russia blocking a whole nation (Estonia in 2007) or the sending of viruses like Stuxnet into Iranian nuclear management systems by strangers, are a minimal part of a whole series of events that should start to make the whole world worry.

China has understood the threat and it sensed that devising defense and counterattack plans are essential.

1. Increase funds for research and development of new technologies;
2. Forming special departments dedicated to cybersecurity and cyberwar;
3. To have a legislative body that gives the conditions to the State to act on the network;
4. Search for the brightest minds in the field;
5. Combat the absolute dominator of the Web, alias USA.

These are the points where the People's Republic of China is concentrating and in which, in my humble opinion, everyone should work, albeit in the case of the third and fifth points, adapting the work to socio-cultural conditions and alliance relations that each country has.

Bibliography

- W. Howlet, “The Rise of China's Hacking Culture: Defining Chinese Hackers”, California State University - San Bernardino CSUSB ScholarWorks;
- F. Kaplan, “Dark Territory the Secret History of CyberWar”, Ed. Simon and Schuster, 2016;
- J.R.Lindsay, T.M.Cheung, D.S.Reveron, “China and Cybersecurity”, Oxford University Press, 2015;
- N. Nagelhus Schia & L. Gjesvik, “China’s cyber sovereignty”, Norwegian Institute of International Affairs, Policy Brief 2/2017;
- “Overview of China’s Cybersecurity Law”, KPMG, February 2017;
- P. Taylor, “Glossary of Relevant Terms & Acronyms PROPAGANDA AND PSYCHOLOGICAL WARFARE STUDIES”, University of Leeds UK, 1987;

Articles

- T.F.Camponeschi, “Beijing Consensus e Cybersecurity: al via la 3 giorni del World Internet Forum di Wuzhen”, Agenzia Giornalistica Italia, 04-12-2017, https://www.agi.it/blog-italia/agi-china/cina_pechinoworld_internet_forum-3197673/post/2017-12-04/;
- D. Denning, “How the Chinese cyberthreat has evolved”, The Conversation, 5-10-2017, https://theconversation.com/how-the-chinese-cyberthreat-has-evolved-82469;
- A. Nepori, “In nome della Cyber-Sovranità, la Cina bloccherà ogni accesso al Web libero”, La Stampa, 12-07-2017, http://www.lastampa.it/2017/07/12/tecnologia/news/in-nome-della-cybersovranit-la-cina-blocche r-ogni-accesso-al-web-libero-EXKbngNWsJFbMntcIKswxN/pagina.html;
- M. Ocorandi, “An Analysis of the Implication of Suharto's resignation for Chinese Indonesians”, Worldwide HuaRen Peace Mission, 28-05-1998, http://www.hartford-hwp.com/archives/54b/083.html;
- D. Palmer, “Cyberattacks from China: Less numerous but more effective”, zdnet, 21-06-2016, http://www.zdnet.com/article/cyber-attacks-from-china-less-numerous-but-more-effective/;
- P. Pan, "Chinese Crack Down On Student Web Sites", The Washington Post, 24-03-2005, http://www.washingtonpost.com/wp-dyn/articles/A61334-2005Mar23.html;
- A. Segal, “How China is Preparing for Cyberwar”, The Christian Science Monitor, 20-03-2017, https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar;
- A. Spalletta, “La Cina vuole aprire le porte a Internet. Per controllarlo sempre di più”, Agenzia Giornalistica Italia, 04-12-2017, https://www.agi.it/estero/world_internetconferencecina_web-3197168/news/2017-12-04/;
- J. Wagner, “China's Cybersecurity Law: What You Need to Know”, The Diplomat, 01-06-2017, https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/;
- Express Web Desk, “What is the Great Firewall of China?”, The Indian Express, 19-07-2017, http://indianexpress.com/article/what-is/what-is-the-great-firewall-of-china-4757848/;

Sitography

- https://en.oxforddictionaries.com/definition/cyberspace;
- https://cnnic.com.cn/IDR/BasicData/index_1.htm;
- http://indianexpress.com/article/what-is/what-is-the-great-firewall-of-china-4757848/;
- https://www.techopedia.com/definition/3743/backdoor;
- http://searchsecurity.techtarget.com/definition/firewall;
- https://www.thefreedictionary.com/proxy;

- http://www.washingtonpost.com/wp-dyn/articles/A61334-2005Mar23.html;
- http://www.hartford-hwp.com/archives/54b/083.html;
- https://dictionary.cambridge.org/it/dizionario/inglese/ddos;
- http://www.zdnet.com/article/cyber-attacks-from-china-less-numerous-but-more-effective/;
- http://searchnetworking.techtarget.com/definition/virtual-private-network;
- http://www.lastampa.it/2017/07/12/tecnologia/news/in-nome-della-cybersovranit-la-cina-bloccher-ogni-accesso-al-web-libero-EXKbngNWsJFbMntcIKswxN/pagina.html;
- https://en.oxforddictionaries.com/definition/cybersecurity;
- https://www.thefreedictionary.com/active+defense;
- https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=CN;
- https://www.agi.it/blog-italia/agi-china/cina_pechinoworld_internet_forum-3197673/post/2017-12-04/;
- https://www.agi.it/estero/world_internetconferencecina_web-3197168/news/2017-12-04/;
- http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm;
- https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/;
- https://books.google.it/books?id=jDxPBwAAQBAJ&pg=PA18&lpg=PA18&dq=Glossary+of+Relevant+Terms+%26+Acronyms+PROPAGANDA+AND+PSYCHOLOGICAL+WARFARE+STUDIES+University+of+Leeds+UK&source=bl&ots=zlYnHX2PPI&sig=TpUKD1qQ-1_dOccZCOZvUHdtaEU&hl=it&sa=X&ved=0ahUKEwj_hYTQ5__YAhUFVBQKHeNpAgEQ6AEINjAC#v=onepage&q=Glossary%20of%20Relevant%20Terms%20%26%20Acronyms%20PROPAGANDA%20AND%20PSYCHOLOGICAL%20WARFARE%20STUDIES%20University%20of%20Leeds%20UK&f=false;
- https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar;

https://theconversation.com/how-the-chinese-cyberthreat-has-evolved-82469.

UNIVERSITÀ DEGLI STUDI FIRENZE
DSPS DIPARTIMENTO DI SCIENZE POLITICHE E SOCIALI
DISEI DIPARTIMENTO DI SCIENZE PER L'ECONOMIA E L'IMPRESA
Centro Interdipartimentale di
Studi Strategici, Internazionali e Imprenditoriali - CSSII

Tutti gli scritti pubblicati dal CSSII sono sotto la responsabilità esclusiva dei singoli autori