Comparative Analysis of Cyber Intelligence: the Italian case

Alessia Boi [1]

[1] *Center for Cybersecurity and International Relations Studies*

Abstract

A complex operational domain as cyberspace, forces us to assess which strategy is better to implement in order to preserve and protect national interests. For many analysts, the best solution seems to be ANDM, that is "the National Multidimensional Approach to Crisis Management", which appears to be applicable to any type of complex operational situation that requires the combined use of national resources and / or of the International Community.

This paper therefore aims to assess whether the multidimensional approach is really the key to implement an effective and effective strategy in cyber space. The approach will be evaluated through a comparative analysis with the strategy, instead, applied by the People's Republic of China, selected also for its diametrically opposite political and strategic situation, obviously such analysis could concern as many state realities as Russia, India, Israel and as many others, but for the purposes of analysis in this case and for the synthetic need, the comparison with the Chinese reality has been considered comprehensive.

Keywords

Cyber Intelligence, Italy, China, NATO, MNE7

1. Introduction

Threats in cyberspace represent a challenge to the stability, prosperity and security of all nations. The cyber environment has implications in both the physical and informational domains, as it is "transversal"[1] to traditional operating domains (terrestrial, maritime, air and space), directly influencing the general and operational planning as well as conduct of operations. When made explicit in the form of attacks, these implications can be aimed at governmental, economic and financial structures, companies, and critical infrastructures. On the other hand, the perpetrators of the attacks may originate from state entities, terrorists, criminal groups, or individuals aiming at information collection.

Hence the need to develop, in the field of national defense, suitable capabilities to "connect" conflicts beyond normal physical boundaries, compressing the space-time dimension through a complex interaction between the traditional and the information environments of the cyber space.

A complex operational domain as cyberspace, forces us to assess which strategy is better to implement in order to preserve and protect national interests. For many analysts[2], the best solution seems to be ANDM, that is "the National Multidimensional Approach to Crisis Management"[3], which appears to be applicable to any type of complex operational situation that requires the combined use of national resources and / or of the International Community.

This paper therefore aims to assess whether the multidimensional approach is really the key to implement an effective and effective strategy in cyber space. The approach will be evaluated through a comparative analysis with the strategy, instead, applied by the People's Republic of China, selected also for its diametrically opposite political and strategic situation, obviously such analysis could concern as many state realities as Russia, India, Israel and as many others, but for the purposes of analysis in this case and for the synthetic need, the comparison with the Chinese reality has been considered comprehensive.

ITASEC 2021, Italy
EMAIL: alessia.boi@consorzio-cini.it (A. 1);
ORCID: 000-0002-2675-9360 (A. 1);
© 2020 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-2940/paper22.pdf

2. Italian Governance and Strategy

With the beginning of the new century, in cyberspace there have been numerous phenomena of geopolitical importance and an exponential growth of crisis areas, attributable to the contemporary global interconnection. This situation has therefore forced the adaptation of its legislative systems to adequately address the new threats.

In a more and more interconnected society, marked by the advent of technology, intelligence also becomes the main mean for the acquisition of precious information. For this reason, many States have re-evaluated the use of intelligence techniques for the acquisition of advantages in the cyber space and a new branch of the subject has been created: The Cyber Intelligence.

In this scenario, Italy has provided for the legislative update, through law no. 124 issued in 2007 "Information system for the security of the Republic and new discipline of State secret" (Sistema d'informazione per la sicurezza della Repubblica e nuova disciplina del segreto di Stato). This law, introduced in order to respond to the changed social-national and political-international contexts and to the new economic, energy and cyber challenges, represents a significant turning point in the history of our Services, since it defines and frames the tasks, criteria and principles that regulate the functions of national intelligence, with newfound consistency and accuracy.

This legislative text that does not establish a single Service but creates the Department of Information and Security (DIS) an informative and analytical hub, superordinate to two new structures: Agency for Information and External Security (AISE) and Agency for Information and Internal Security (AISI).

Within the legislative framework, a further turning point within the Italian information structure was the regulation of cyber matters which, until then, had only been mentioned but never organically organized with clear directives. The National Plan for Cyber Protection and Cyber Security is drawn up through the Prime Ministerial Decree of 31 March 2017[4], proposing the following objectives:

- Strengthening the defense capabilities of National Critical Infrastructures and of the actors of strategic importance for the country system;
- Improvement, according to an integrated approach, of the technological, operational and analytical skills of the institutional actors involved;
- Encouragement of cooperation between national institutions and companies ;
- Promotion and dissemination of the culture of cyber security;
- Strengthening of international cooperation in the field of cyber security;
- Strengthening of capacity to combat illegal activities and online content.

In the National Cyber Security Plan is reviewed the role of the Nucleus for Cyber Security (NSC) as a support structure of the President and of the Interministerial Committee for the Security of the Republic (CISR), with purpose of foresee and respond to any crisis situations and, in the event of an accident, it must provide for the activation of the alert procedures. The operating logic of the NSC is characterized by various activities, including:

- operational planning in response to situations of cyber crisis;
- evaluating and promoting information sharing procedures;
- carry out international exercises concerning simulations of cyber events.
- national reference point for relations with the UN, NATO, the EU, other international organizations and other states.

It is important to emphasize the relevance of this latter functionality, in order to establish solid international cooperation and collaboration, because not only does it coordinate exercises from abroad, but from abroad it can also receive reports of relevant cyber events and issue alarms to administrations and private operators.

The Italian cyber security strategy does not end in 2017, infact a text to which we cannot fail to refer is the implementing decree of the NIS Directive[5], which has been applied to the Italian context through the Legislative Decree 65/2018[6] on the basis of the 2016 European Directive, which required for each European state to develop a national cyber security strategy, foreseeing:

- a governance system with a national authority that must ensure the implementation of the legislation;
- define priorities and objectives;
- implement monitoring and prevention activities;
- support research and development in the technology sector;

In the Italian system, still today no independent or additional authorities to the government structure have been created, representing one of the weaknesses of the Italian national cyber strategy, indeed the entire governance structure was placed under the control of the Executive power and the single point of contact is identified at the top of our information services, within the DIS.

3. China, NATO and United States of America: Comparing Models

A recurring theme in the discussion and the great weakness of the Italian Cyber National Strategy appears to be the need for a greater multidimensionality of strategy in the cyber context and greater collaboration between the various institutional and non-institutional substrates, not-favored in the Italian context also for the lack of an independent structure dedicated exclusively to cyber domain.

The need of this cooperation appears to be shared by most of the state realities in the world and appears complex to most of them to implement. It could therefore be said that the achievement of an optimal harmony of the "process" of integration of the various actors, is almost utopian. But despite this, there are some examples in the world of a beginning, albeit feeble, of a process of cooperation, as in the case of India, China and Russia.

Specifically, this paper will try to define through guidelines, the structures and principles that support and regulate China's great "Intelligence" machine. Although it may seem pretentious to take China as an example, for a country like Italy, which is diametrically opposed in principles and structure, it may be useful to understand the profound differences, not to align ourselves with their system but to try to integrate some of their aspects in our modus operandi.

3.1 Chinese Information System

The culture of security in China has very ancient origins, founded on the principles of Confucius and Sun Tzu, espionage is elevated to a system; in fact, every citizen is obliged to keep not only the secrecy relating to its functions, but is also urged to collect information that, in his opinion, is contrary to the collective and party interests. For this reason, the Secret Services of Beijing, for us westerners, are a puzzle both on a theoretical and operational level, despite the organizational structure we know.

There is no idea how the government can manage billions of pieces of information provided by billions of sources distributed around the world. It is not clear how a system of overlapping jurisdiction works between internal and external security, police and secret services, party and state, private and public [7].

What is clear, however, is that the general direction of the entire process is in the hands of the Communist Party. Given that, in terms of number and specific skills, all the intelligence organizations of the People's Republic of China are difficult to identify and quantify, we can however try to outline the structures of strategic importance.

The Chinese secret service has thirty sections that report to the Central Committee of the Chinese Communist Party, thirteen of these play a role of espionage and counterintelligence, directed by the Ministry of State Security (MSS). The main areas of action dealt with by these institutions have been for over half a century after the establishment of the People's Republic, the safeguarding of political power, internal order against separatism, territorial sovereignty, military threat from the outside and export of the revolution. But after the reformist invitation of Deng Xiao Ping to take advantage of the

free market, activities of hunting for business, resources, money, technology and vulnerabilities have also been added.

As previously mentioned, this quite logical and rational institutional framework is accompanied by the non-institutional and almost spontaneous framework, which makes the Chinese Secret Services unique in their kind. “Watching each other is a duty. Spying on foreigners is patriotic". [8]

The duty of collaboration, inserted in the Chinese Constitution, which itself assigns security and information tasks to all citizens. In this perspective, Chinese citizens are an integral part of the information production chain. It is easy to understand the difficult process of collecting and analyzing the countless reports a day provided by millions of sources scattered all over the world.

The solution to this problem, it’s still unknown and for many years western analysts have hypothesized through the "mosaic metaphor" that the bodies responsible for this function combined all this information to arrive at a single and complete one. The mosaic theory, to date, however, appears to be non-exhaustive, as it does not explain how a system of overlaps between police, secret services, party, state and citizens can work. Furthermore, we do not know what the criteria and procedures are adopted by the various agencies to process and disseminate information, if and where the analyzes and the merging of this strategic information take place. What is clear, however, is that the Party is at the head of the political and security management.

Once this complex phenomenon of cooperation has been described, the application in the field of Cyber Intelligence, in which China plays a key role worldwide, is easier to understand. The cyberspace environment facilitates the immediate sharing of materials by millions and millions of users, who are very often granted. In this difficult environment the role of "node" between the institutions and the various militias is most likely played by telecommunications companies, which also represent a source of technical expertise from which the Chinese army can draw. Chinese telecommunications companies are not technically part of the government apparatus, nor are they officially classified as state enterprises, however, there are indications that major Chinese telecommunications companies can effectively act as delegates of the People’s Republic of China and play a supporting role in promoting China’s strategic interests abroad.And although it does not appear that the companies in question are currently in charge of conducting offensive attacks, they certainly play a key role in the transmission of sensitive information.

To date, China has not expressed any desire to militarize Western cyber confrontation, but despite this, its defensive aggressive policy in the West is perceived as a military threat rather than merely cyber. This is why the strategy declared by the United States, which is similar to that of NATO, announces the militarization of cyber space and an offensive war against the critical infrastructures of China and Russia, paraphrased by computer defense.

3.2 Improving Cyber strategy: NATO and USA

The policy in question was created by NATO in 2011 to highlight the main five missions to be implemented in cyberspace, missions that logically need to be integrated with the iconic Article 5 that defines the three "core tasks", fundamental tasks, for the Alliance: collective defence, crisis management, and cooperative security.

- Strategic Initiatives 1: organize and equip cyberspace so as to draw all the benefits of its potential;
- Strategic Initiatives 2: use new operational concepts to protect defence networks and systems;
- Strategic Initiatives 3: participate with other government agencies and private individuals in the creation of a unified strategy;
- Strategic Initiatives 4: building strong relations with allies and international partners;
- Strategic Initiatives 5: Leverage national ingenuity to build exceptional cyber strength and accelerate technological innovation.

The existence of these objectives enriched by the fundamental precepts means that nowadays an armed attack against one or more of the member countries of the Atlantic Alliance, conducted in or

through cyberspace, is considered as a direct attack against all member countries. Therefore, should a cyber-attack materialize, each of the Allies in the exercise of the right of self-defense, individual or collective, must assist the party or parties attacked by undertaking immediately, individually and in agreement with the other parties, the action deem as necessary, including the use of armed force, to restore and maintain security in the North Atlantic region.

The need to clarify the objectives and regulate the conduct in cyberspace by major international organizations arises mainly as a result of the attack that still appears to be the most important in the history of cyber operations in Europe, the attack on Estonia in 2007. In the spring of 2007, Estonia was the victim of a 22-day cyber-attack, through a massive wave of Ddos cyberattacks, blocking the information systems of banks, government institutions, and national media, which plunged Estonia into 22 days of complete blackout.

To this an unprepared NATO did not know how to react and did not appeal to article 5, the allied countries simply sent their best experts to Tallinn to stem the problem and look for the source of these innumerable attacks. From the beginning it was quite clear who was responsible for this attack, but in spite of this an official accusation was never formulated, not to increase the tension but also for the scarce useful data that hackers had left. 2007, however, was a wake-up call, helping Estonians and NATO to implement their cybersecurity standards. Estonia has now become the most digitalized state in the European Union, where 90% of banking transactions are carried out via the Internet, political consultations are carried out online, and 100% of the public administration is equipped with computer. Not surprisingly, the name of the state is often ironically deformed in "E-stonia".

Then this episode on a further evolutionary phase of the approach of the Atlantic Alliance to this domain, the creation of the CCDCOE, or the Center of Cooperative Excellence for Computer Defense of NATO, appears fundamental. The CCDCOE, located in Tallinn, established at the initiative of Estonia along with six other nations Germany, Italy, Latvia, Lithuania, the Slovak Republic and Spain on 14 May 2008.

Unfortunately, having gone under heavy scrutiny, there has been a further step forward in cyberspace by international organizations that have created a new center ready to collaborate with the CCDCOE described by the NATO Secretary-General, Jens Stoltenberg, in his closing speech at the Defense Ministers' meeting in November 2017. From the words of the Secretary General, in fact, it is very clearly understood that NATO has decided to embrace the possibility of using cyber weapons in its military operations and to do so by creating a Cyber Operations Center in which all Allied capabilities can be channeled, to integrate the cyber capabilities of countries belonging to the block.

In the new Cyber Operations Center, the cyber capabilities provided by the Allied Countries will be under the complete command and control of the State that has made them available so that the traditional reticence of the States to share even simple information on the real cyber capabilities developed, which may be significant in a possible conflict.

But despite the intent of militarization by NATO and the aggressive defense of China described above, the most encouraging fact of this confrontation between China and the United States is that, at least for the time being, those that will surely be the two great world powers competing between now and the next few years, seem to prefer the cyber defensive aspects and not the offensive ones that in this case could lead to a dramatic conflict in the open field.30

Among Western actors that recognize a central role for cyber intelligence, the United States of America also stands out. In 2015, they founded a new federal agency within the Office of the Director of National Intelligence (ODNI); this new body is known as the Cyber Threat Intelligence Integration Center (CTIIC) the newest of four multi-agency centers. In fact, along the lines of the Chinese model, the multi-factor approach can be found in the new US government structure, whereby the agency will be a fusion center between other existing federal agencies and the private sector to act in real time against cyber-attacks.

It was established in 2015 on the initiative of President Barack Obama, who appointed the former Director of National Intelligence to establish the CTIIC. The normative text legitimizing the creation of this structure is a Presidential Memorandum[9], in which five responsibilities can be extrapolated that are assigned to the CTIIC:

- Provide integrated all-source analysis of intelligence related to foreign cyber threats or to cyber incidents affecting US national interests.

- Support the National Cybersecurity and Communications Integration Center, the National Cyber Investigative Joint Task Force, U.S. Cyber Command, and other relevant United States Government cyber centers by providing access to intelligence necessary to carry out their respective missions.
- Oversee development and implementation of intelligence-sharing capabilities to enhance shared situational awareness of intelligence related to foreign cyber threats and incidents.
- Ensure that indicators of malicious cyber activity and, as appropriate, related threat reporting contained in intelligence channels are downgraded to the lowest classification possible for distribution to both US Government and US private sector entities.
- Facilitate and support interagency efforts to develop and implement coordinated plans to counter foreign cyber threats to US national interests using all instruments of national power, including diplomatic, economic, military, intelligence, homeland security, and law enforcement activities.

In order to achieve these objectives, the Center has been divided into three sections:

1. Building Awareness: according to this role, the CTIIC engages with other cyber centers and information and analysis providers, helping them to understand the potential significance of threats. It builds an analysis of threat activity and makes it accessible to non-cyber specialists who need to take it into account in their daily activities. CTIIC's work generates a greater understanding of the big picture and trends;
2. Integrating Analysis: the CTIIC works with cyber and non-IT experts to initiate cyber threat analysis and examine adversary strategies in a geopolitical context. The CTIIC will integrate trend and event analysis to identify cyber gaps, and to support federal agencies in developing operations to mitigate adversary threat capabilities;
3. Identifying Opportunities: the CTIIC supports whole-of-government decision-making. The CTIIC provides analysis of opportunities and helps to develop effective response and intervention measures.

The CTIIT is a best practice of a support and coordination structure, whereby the center will not collect information on its own but will analyze the information already collected on the basis of existing authorities and work to fill in the gaps[10].

4. The multinational approach to the cyber context: MNE7

Among the Chinese intelligence targets, Italy is not yet a strategic military target, except as a mere component of the Atlantic blockade. But its economic and industrial complex has been a goal for a long time now.

In this regard, in the half-yearly report of 2013 prepared by the Italian Services, it was clearly indicated how the segments of luxury, industrial automation, capital goods and environmental technologies, are carefully monitored by the diplomatic network-console China. The Italian economic-industrial complex is vulnerable especially if threatened by the Chinese giant.

These observations confirmed that Italian cybersecurity, to date, cannot be viewed in isolation from cyber security at the level of multinational and supranational organizations, in particular the European Union and NATO, with the difference that Italy does not yet have adequate defensive and response capacity. But if we can count on the help of the largest militarized cyber-attacks, in the industrial economic field, it is necessary to manage the threat independently.

Despite the obvious difficulties, there is already an attempt to change the multidimensional/ multinational approach to the cyber problem, this through the activities carried out with the Campaign of experimentation called Multinational Experiment 7 (MNE7). The MNE7 is a recent series of experimentation campaigns in which Italy plays the role of leader of the working group aimed at analyzing the international legal framework applicable to cyberspace.

But despite the unquestionable efforts to integrate interoperability, the position of the Italian defence is for now anchored to the previous organizational structures, not so far suited to new contexts. The

structure regarding cybersecurity, entrusts the President of the Council of Ministers with the absolute leadership to which to ultimately lead the national policy, strategy and "governance"[11] on the cyber environment. Decision on absolute leadership, but in the case of cyber defense is inadequate because of the speed of these attacks, speed that implies an immediate response that due to the complex structure proves impossible to give.

The solution could therefore be a single National Authority on Cyber Defence (CD), which can coordinate and optimize operations, capabilities and responsibilities attested in the various departments. This position of the CD, such as to have a broad and strategic perspective of the problem and sufficient delegation of authority to be able to take "strategic" decisions in case of serious entity.

In the final analysis, to close the Italian strategic and operational framework on cyber, it is necessary to identify in addition to the structure now overcome, the greatest criticality that lies in the preventive aspect of the threat that by its nature involves different types of actors. Forecasting activity must be understood as the timely knowledge of «when, where and how», to allow decision-makers, on various levels, to understand the situation and to be promptly and constantly supported in decision-making processes through a cyber picture.

The secret of the effectiveness of this function, as indeed of all previous operations, lies in the ability to share information, namely the information sharing process. Sharing, similarly feasible through the multidimensional approach, involving partner countries, national institutional actors as well as academia and the private sector. Although the discussion seems to have outlined the multiple adverse elements and the respective possible solutions, which our country adopts in cyberspace, it remains to examine the limits within which Italy can exercise its discretion in the cyber framework, that is, the legislative doctrine.

5. Conclusion

Summing up, the addition of the cyber component to traditional war scenarios, leads to the hypothetical creation of the most asymmetrical war ever seen before. New boundaries, new weapons, new timing, and unknown enemies. We can safely say that to date no State is really ready for such a conflict but certainly there are realities that are aiming all their resources for the achievement of this purpose. In relation to this, the text analyzed the position of China and in part that of its counterpart with respect to NATO.

Approaches in some cases divergent, also depended on the type of power that they are required to represent, in one democratic case and in the other a single-party socialist republic. In China, the Western principle of the division and balance of powers is not the foundation of the institutional political system.

The powers are not divided, they do not balance each other, but instead they are united in a single central node, namely the Party. And it is precisely in this centralization of power that many experts make reside the cause of China’s great success in cyber space, since, as previously explained, it is a space in which every movement occurs with very fast timing and therefore a similar speed in response is required. The answer is that in the case of China it is never slow to arrive because the decision-making power is centralized in very few people, which to us, countries of democratic origin, it is impossible to implement because of the various mandatory steps that ultimately constitute the decision-making process. But despite our non-competitive timing, there is a solution in equating our position with the great undemocratic giants of cyberspace, and it is, as already analyzed, multidimensionality.

Finally, the difficult times that face our horizon should advise everyone to pay particular attention and care to the national information and security system, that it may be enabled to protect our society ever more effectively from the dangers that already exist and from those that will necessarily follow.

Because today, more than in past historical periods, knowing has become an essential fact and who is unable or does not want to do it, becomes irrelevant on the world scene.

All States must therefore continue to invest in research and the improvement of new strategies, new weapons that can be used in this now no longer new environment. Since it is useful to remember that the cyber information activity is still managed by men who have as their ultimate goal the search for the truth and then ultimately, the aspiration to freedom.

6. References

[1] N. de Felice, C. Ammiraglio, "La strategia della Difesa nel cyberspazio quale contributo alla tutela degli interessi nazionali", nella raccolta "Information Warfare 2011", edited by U. Gori, L. Sergio Germani, F. Angeli.

[2] Multiple Futures Project (ACT-2009), Strategic Trends Program - Out to 2040 (DCDC - GBR).

[3] "Documento di riflessione congiunto Esteri-difesa", Edition December 2010.

[4] Decreto del Presidente del Consiglio dei Ministri 31 marzo 2017, *Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali*, (link)

[5] Network and Information Security, European Directive 1048/2016.

[6] Article 7-8 NIS Directive 1048/2016 - National Strategy on Network and Information Systems Security

[7] Alberto Pagani, Manuale d'Intelligence e Servizi Segreti, Rubbettino 2019, "La Cina".

[8] F.Mini, Information warfare 2011 I servizi d'intelligence cinesi: strategie di spionaggio e influenza nello spazio cibernetico.

[9] February 25, 2015 Presidential Memorandum - Establishment of the Cyber Threat Intelligence Integration Center https://www.dni.gov/files/CTIIC/documents/CTIIC-Presidential-Memorandum.pdf

[10] SCOTT E. JASPERU.S. Cyber Threat Intelligence Sharing Frameworks, International Journal of Intelligence and Counterintelligence, 30: 53–65, 2017

[11] Sicurezza e protezione dei dati: cyber security, object storage, biometria, difesa globale e intelligence per un business always-on / Giuseppe Saccardi, Gaetano Di Blasio, Riccardo Florio; Milano: Reportec, 2015.

BIBLIOGRAPHY

- Antiseri D., Soi A., Intelligence e metodo scientifico, Rubbettino, Soveria Mannelli,2013. Caliguri M., Cyber Intelligence, tra libertà e sicurezza,Roma, Donizelli 2016

- Camera dei deputati, Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa cyber, n°83, settembre 2019

- Eftimiades N., "Chinese Intelligence: Agent Recruitment Methods", Intelligence Watch Report Quarterly, vol.2, n 3, 1995

- Giannuli A., Come funzionano i servizi segreti, Salani Editore, 2009.

- Gori U. e Germani L. S, Information warfare 2011 : la sfida della cyber intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale Milano, F.Angeli, 2012

- Inkster N., Chinese Intelligence in cyber age, Survival, 01 marzo 2013, vol. 55, p 45-66 Keegan J., Intelligence in war. Storia dello spionaggio militare da Napoleone ad al- Qaeda, ed. A. Mondadori, 2004.

- Libro Bianco per la sicurezza internazionale e la difesa, presentato dal ministro Pinotti, 2015.

- Magi G, I 36 stratagemmi. L'arte segreta della strategia cinese per trionfare in ogni campo della vita quotidiana, Il punto d'incontro,2003.

- Mini F., Quel che i cinesi sanno di noi (e noi non di loro),in Limes n°7.

- Mori M., Servizi e segreti, introduzione allo studio dell'intelligence, ed. G Risk, Roma, 2016.

- Pagani A., Manuale di intelligence e servizi segreti, Rubbettino, 2019.

- Rapporto del Clusit sulla sicurezza ICT in Italia, 2019, Security Summit.

- Saccardi, Di Blasio, Florio, Sicurezza e protezione dei dati : cyber security, object storage, biometria, difesa globale e intelligence per un business always-on , Milano ,Reportec, 2015.

- Sbaraglia G., Cyber Security, Kit di sopravvivenza, Goware, 2018.

- Sommella R., L'Italia preda di ladri di tecnologie, Milano Finanza, 14/04/2011.

SITOGRAPHY

https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

https://tecnologia.libero.it/pacemaker-vulnerabilita-protocollo-wireless-pericolo-attacchi-dos

http://www.treccani.it/enciclopedia/sistema-nazionale-delle-informazioni-per-la- sicurezza

http://servizisegreti.com/organizzazione

http://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione.html

https://foreignpolicy.com/2018/03/21/nobody-knows-anything-about-china/

https://www.chinahacker.com

https://www.nato.int/cps/en/natohq/topics_78170

https://ccdcoe.org/about-us/