LUISS

Dipartimento di Scienze Politiche

Cattedra: Conflict and Peace Building

Sino-Indian relations within the Fifth Domain:
Competition and challenges in the cyberspace

Prof. Mulas Roberta

RELATORE

Francesco Pagano

CANDIDATO Matr. 000862

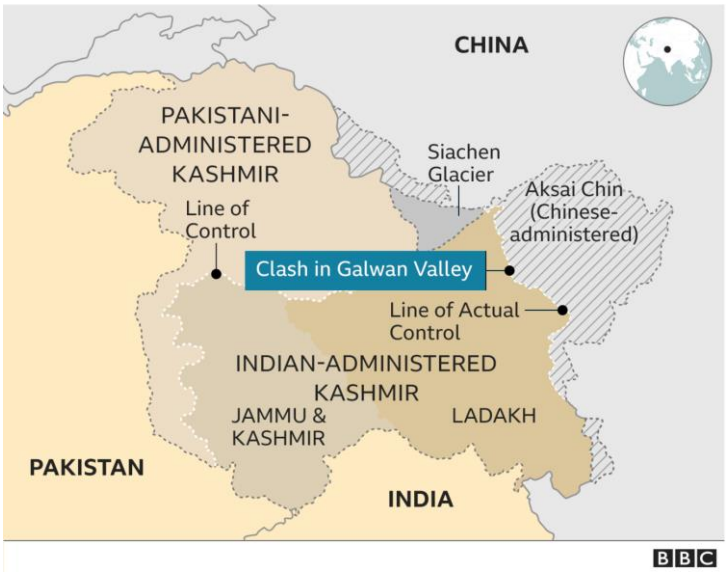
Anno Accademico 2019/2020

Table of Contents

Introduction

The thesis seeks to evaluate an analysis of the cyber competition taking place between China and India through a reflection of the modern swinging Sino-Indian relations affecting the Indo-Pacific region. It is fundamental to evaluate a comprehensive overview of the contemporary relations of China and India, being both emerging world powers with ambitions of regional hegemony[1] (wielding peerless power and influencing the Indo-Pacific region), in order to comprehend the new challenges triggered by the digital age. Both the states grew rapidly in the last twenty years, challenging themselves in a long-term rivalry for regional hegemony over Asia by exercising influence on internal policies of other Asian states.[2] Regional hegemony has been a changing dynamic in the 2000s. On one hand, China is continuously rising its influence across South Asia through different strategies such as flexing its muscle over Bhutanese border, signing free trade agreements with states such as Maldives and Nepal and acquiring strategic assets such as the Hambantota port in Sri Lanka. On the other hand, such moves result of great concerns for India, which finds Chinese rising influence as a growing alarm. In fact, India benefited since its independence a dominant position in South Asia through: leveraging its own bilateral relations with Asian states, unilateral political influence, one-sided economic arrangements and coercion through military interventions, like it happened in Sri Lanka, Maldives and Bhutan.[3] Indian dominance over the region resulted a *fait accompli* mainly due to the non-involvement of other major powers.[4]

Dynamics of hegemony began to change with the growing Chinese economic power and declining of Sino-Indian relations. In fact, China's ambition is to expand its hegemony in South Asia, even at the cost of deteriorating the relationship with India. It is therefore necessary to analyze Sino-Indian relations and the new challenges to come, especially in the light of the latest 2020 China–India skirmishes, which are part of an ongoing military standoff between the two Asian giants. The latest events occurring in 2020 shape the tensions going on between China and India - both the states have engaged in deadly skirmishes along the borders. Thousands of Chinese and Indian troops have been in a standoff in the Ladakh region high in the Himalayas since early May and after a de-escalation on June 6, the mutual withdrawal of troops from the Galwan Valley trasnformed into new skirmishes.[5] The latest skirmishes result in a severe apprehension since there has been no deaths or shots fired along their borders since 1975. There is a chance that the latest clashes can progressively deteriorate the relationship between the two states, fueling instability at the borders, marking insecurity at the Asian regional level and establishing the typical security dilemma[6]'s unpredictability.



[1] In international relations, regional hegemony is the hegemony (political, economic, or military predominance, control or influence) of one independently powerful state, known as the regional hegemon over other neighboring countries..
[2] Joshua Ball, Global Security Review, Asian Hegemony: Ongoing Tensions between China and India, 2019
[3] Sandeep Bhardwaj, University of Nottingham Asia Research Institute, India and the mantle of regional hegemon, 2018
[4] Ibid.
[5] Alyssa Ayres, The China-India Border Dispute: What to Know, Council on Foreign Relations, 2020
[6] Security dilemma in political science is a situation in which actions taken by a state to increase its own security cause reactions from other states, which in turn lead to a decrease rather than an increase in the original state's security.

To present a structural vision of the bilateral relationship of the two regional powers, this thesis will carry out an analysis framing historically the origins and the evolution of Sino-Indian relations, focusing particularly on the events of the 20th and 21st century. The first chapter will explore the history of Sino-Indian diplomatic relations to comprehend the function of the modern and future challenges altering the state of relations between the two Asian states. The linear description of the history shaping relations between China and India aims to carry out a detailed research of the main factors affecting the stability and the balance on which these bilateral relations are based from the 50s to modern day. The description will highlight critical points of destabilization within the bilateral relations, especially through the role of: Sino-Indian boundary issues, the Tibetan sovereignty debate between the two states, the nuclear dimension as a factor of instability in the Indo-Pacific region and the asymmetrical perception of threat, marking the fragility of a possible cooperation between the two Asian states.

Considering the latest events fuelling the deterioration, the thesis will outline a debate on the fifth-dimension[7]'s confrontations occurring on cyberspace between the two states. Indeed, through a theoretical approach, the second chapter will outline the common ground linking the modern cyber confrontation occurring nowadays, originating from the above mentioned historical and ''physical'' causes of dispute and consequently affecting the stability of the whole Asian region. The chapter will evolve from a theoretical debate on cyberspace and cybersecurity's implications within international relations, especially from a Neorealist's perspective of international security studies. In particular, it will trace different features of the cyber dimension of international relations affecting the Sino-Indian stability, like the attribution conundrum and the lack of a structural governance regulating the new battlefield of cyberspace. Through the lenses of Neorealism, the chapter will trace the conditions establishing a security dilemma in the emerging theatre of computer networks and information technology.

The third chapter will outline a wide-ranging debate, through the above theoretical analysis, enclosed within the fragmentations of the Sino-Indian relations. Different cyber projections will possibly ensure a condition of dispute within cyberspace, triggering possible escalations and making computer networks and technology possible factors of destabilization for large geopolitical disputes. The chapter will on one hand, specifically examine China's belligerent doctrine framed in cyberspace through an analysis of its cyber capabilities, organizational mechanisms, large cyber-attack campaigns and the advantage of a strategic use of cyber domains to ensure national security objectives. On the other hand, it will delineate the implications of Chinese's cyber posture towards India's national security. Comprehensive analysis on the implications of cyberspace within international relations is duty bound in a modern and digital world enclosed by modern and digital future-oriented challenges - ''*the strategic landscape has changed forever.*''[8]

[7] Domains of warfare are land, sea, air, space and cyberspace being the 5th

[8] Brig. Gurmeet Kanwa, Acupuncture Warfare: China's Cyberwar Doctrine and Implications for India, Indian Defence Review, 2017

1. Historical Framework

1.1. History of Sino-Indian Diplomatic Relations

The first chapter of this thesis will bring to light a linear historical description of the Sino-Indian relations. To deal with present and future challenges, understanding the bilateral relations between the two states is fundamental, especially to comprehend the ongoing breaking points that hamper a common ground for cooperation in good faith. The chapter will particularly carry out an exploration of the 20th and 21st century affairs between India and China. However, it is culturally important to understand how both the states did not only share traces of contemporary history, but also shared an ancient history of the oldest civilizations[9] which have co-existed for millennial.

Ancient history has delivered us ground breaking works such as Stewart Gordon's book "*When Asia Was the World, Traveling Merchants, Scholars, Warriors, and Monks Who Created the; Riches of the East*" a long and outstanding description of Asia's ancient diplomatic relations. Around 500-600 B.C, Ancient China did not find any interest in opening towards the Western World[10]: after the fall of the Roman Empire, Europe was neither considered a point of prosperity for the Chinese, and nor the Eastern Roman Empire, which lasted longer. Chinese cultural superiority at the time was so elevated that missions in external lands would have taken place only to further strengthen different sources of power. Indeed, the Chinese Empire found its West in the neighbouring Asia, especially in India. Chinese literature, such as the popular legendary figure *Sun Wukong* from the 16th-century Chinese novel *''Journey to the West''* dealing with the first waves of travel from China to India. Also known is the history of the Buddhist Monk Xuanzang who travelled around India around 618-632 A.D *(Anno Domini)*. Such outstanding excursions, from an ancient perspective, gave birth to the some of the first foreign and intracontinental relations, such as trade. At the same time, it gave birth to the first industrial espionage activities[11] – on his return to China, Xuanzang took back Indian's production procedures to produce cane sugar and techniques for vinifying grapes.

The earliest formulas of international political economy could be found in such relations for what concerns trade. At the time, also in relation to Xuanzang's journey across the ancient (and contemporary due to the clear resurgence through the Belt and Road Initiative) Silk Road, we know that Chinese silk has been one of the most important means of payment and transaction. Chinese Silk was seen, accepted and sought after as modern cash money; nomadic people from regions of India and other states such as modern Uzbekistan, Turkmenistan and Afghanistan bought Chinese Silk in exchange of other goods. It seems like China of that time had the role of modern United States of America in the last decades: Chinese Silk had the function of the modern dollar, able to control a universally accepted means of payment around the world.[12] To close this little ancient parenthesis: after Xuanzang's discoveries, China undertook a long chain of diplomatic missions (around fifty in just a century) towards India. Such an old parenthesis is not of secondary importance as it draws the most ancient roots of the two twin engines of global economy, outlining the cultural proximity and interest.

Contemporary relations began from a common starting point: a late independence obtained from both States. People's Republic of China (PRC) and India gained their independence in 1949 and 1947, respectively, starting their patterns of growth in the region with similar visions. The first phase of their relations indeed began with a mutual recognition of sincere cooperation confirmed from a common vision. In both cases, the two states emerged from different but both bloody colonial imperial domination, which matured in a creation of a new and brighter future within the Asian Region.

[9] Zhiqun Zhu, China-India Relations in the 21st Century: A Critical Inquiry, *Indian Journal of Asian Affairs* Vol. 24, No. 1/2, , 2011
[10] Federico Rampini, Oriente e Occidente: Massa e individuo, Feltrinelli, 2020
[11] Ibid,
[12] Ibid. p. 40-42.

n

On 30 December 1949, India became the first non-socialist nation to recognize PRC.[13]Immediately afterwards, a first diplomatic relationship was established. The first phase of such a bilateral relation has been scheduled as the era of *''Hindi Chini Bhai Bhai''*[14] (Indians and Chinese are brothers) because of such a close view towards regional, national, economic and cultural affairs. In fact, similar visions at the beginning could be traced due to the sharing of similar characteristics such as huge agrarian populations, a thick presence of widespread poverty throughout the land, accompanied by a high rate of social and economic inequality structured because of the common weak economy characterised by underdeveloped industrial sectors. At the same time, both states shared multi-ethnic, multi-cultural societies with a complex colonial inherited border issues to solve with neighbouring states.

The bonhomie of the 50's was characterised by a series of frequent diplomatic visits between representatives, initiated by the famous first meeting between the Prime Minister Zhou Enlai visiting India in 1954.[15] What was prevalent and shared was also the strategic vision of both states on regional affairs. Indeed, in different international occasions, New Delhi's mediatory and third-state role favoured China's vision on several strategic assets. For example, Beijing was supported in the Korean War by Indian's obstruction towards UN resolutions labelling China as the aggressor. At the same time, the first Indian Prime Minister Jawaharlal Nehru internationally called for China's membership within the United Nations and simultaneously accepted Beijing's sovereignty over the region of Tibet. Such a region was strategic for the Sino-Indian bilateral relationship. In 1954, Nehru and Zhou Enlai signed in Beijing the Sino-Indian Agreement on Trade and Intercourse between Tibet and India, introducing what became the milestone of such a friendly bilateral relation – the ''*Panchsheel''*[16] Treaty.

[13] Zhang Li, China-India Relations: Strategic Engagement and Challenges, Center for Asian Studies, 2010
[14] Tien-sze Fang, Asymmetrical Threat Perceptions in India-China Relations. OXFORD, 2014
[15] Pandit Jawaharlal Nehru, India's first Prime Minister, along with the then Chinese leadership had coined the Hindi Chini Bhai Bhai term in the early 50s. It became a slogan coined in order to create goodwill cooperation and Indo-China alliance.
[16] Panchsheel Treaty: Non-interference in others internal affairs and respect for each other's territorial unity integrity and sovereignty (from Sanskrit, *panch*: five, *sheel*: virtues), which was signed at Peking on 28 April 1954, *United Nations Treaty Series*, vol. 299, United Nations, pp. 57-81

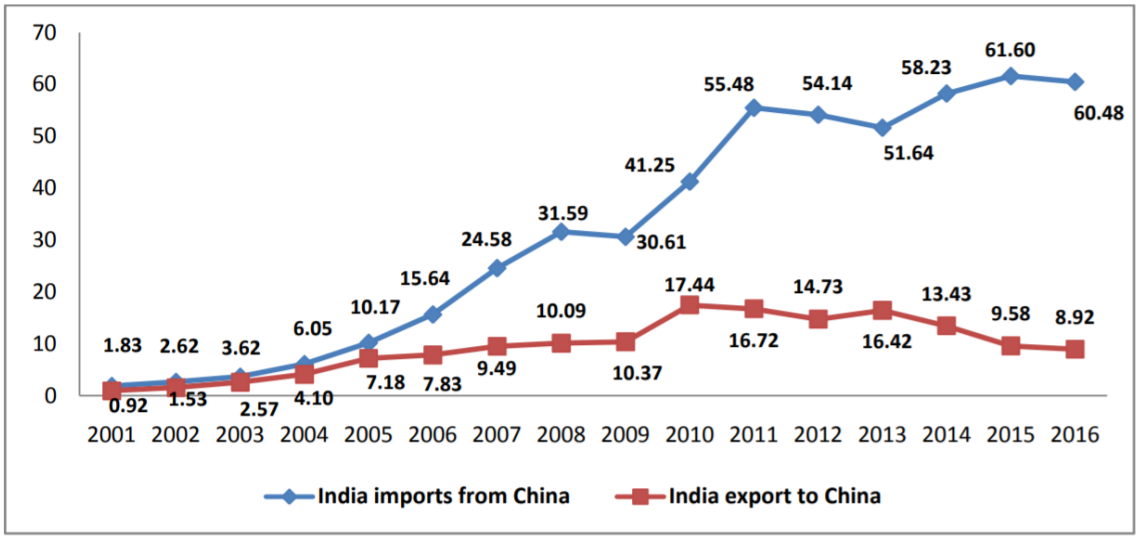
The ‘’*Panchsheel’’* Treaty (in Hindi), also known as the ‘’Five Principles of Co-existence’’ represented the peak of an optimistic perspective on the bilateral relations of the two Asian states. The agreement covered five different principles: mutual respect for each other’s territorial sovereignty and integrity, non-aggression, non-interference in internal affairs, equality and mutual benefit of cooperation and peaceful coexistence in the region of Asia. Indeed, cooperation and goodwill in the 50’s were factual in several occasions. In 1954, Nuhru welcomed China’s inclusion in the Genève Conference to declare globally the recognition of China as a new Asian nation. Simultaneously, a Sino-Indian trade agreement was signed between Nehru and Zhou Enlai to establish locally Sino-Indian Friendship Associations, to promote on the ground of sincere spirit of collaboration and partnership. In 1955, the two states decided to project themselves globally into the African Continent with Nehru and Zhou Enlai promoting convivial and beneficial ties with the Asian-African conference hosted at Bandung, in Indonesia, in order to promote a converged growth of all those states that suffered from colonial heritage and history.

However, what seemed one of the best honeymoons throughout Asia, quickly deteriorated by the end of the 50’s due to the infringement of the ‘*’Panchsheel’’* philosophy. Border disputes and different perspectives on its rationale culminated in a deterioration of relations especially after Tibet’s spiritual head Dalai Lama’s escape to India in 1959. The Sino-Indian border dispute evolved into a short, brief but decisive war in 1962. Borders became an unstable factor, which affected the common sense of cooperation between the two States and a setback in diplomatic relations. The grievances produced by the border clash resulted in a fragmentation of the bilateral relations, which lasted, from 1962 until the 80’s. However, from 1976 Beijing and New Delhi resumed a low-profile dialogue through a fresh start of diplomatic missions, ambassadorial relations, and bilateral cooperation to find out a shared and acceptable answer related to the boundary issue. Normalization of the relationship was launched through a ‘’look forward’’ policy[17] of cooperation and coordination. Nevertheless, the first nuclear tests conducted by India would become a new factor of concern for China and therefore a reason of diplomatic confrontation between the two States, who saw their relations going back again into a ‘tailspin’.[18]

Indeed, relations between China and India can be understood as a perpetual pendulum swinging from ‘’bhai bhai moments’’ to complex periods of rapid, descendent and twisting relations. Infact the two Asian states have cooperated to expand contacts and increase cooperation throughout many different fields such as border issues, combating against terrorism in Asia and the vital role of trade. Indeed, the economic relation between the states is considered one of the most significant bilateral relation in the contemporary global economic scenario marking China as India’s largest trading partner, whereas India is within the top ten of China’s trading partner.[19] The figures below present divers economic indicators describing the Sino-Indian economic relation. On the political front, high-level interaction meetings throughout contemporary history have played a vital role[20], such as the ‘’2006 Year of China-India Friendship and Cooperation’’[21] and other vital and summits and visits which took place throughout 2010-2020 decade. However, the degree and intensity of partnership has always been challenged by the thin line dividing cooperation from competition, especially on issues relating to aspirations such as the global economy (especially trade frictions), security throughout the hotspots of the Asian region, energy security and other factors driving each other’s interests divergently.

[17] Maxwell, Neville, Settlements and Disputes: China's Approach to Territorial Issues"(PDF). *Economic and Political Weekly*. 41, 2006.
[18] Tien-sze Fang, Asymmetrical Threat Perceptions in India-China Relations. OXFORD, 2014
[19] Phd research bureau phd chamber of commerce and industry India – China Trade Relationship: The Trade Giants of Past, Present and Future, 2018
[20] Zhang Li, China-India Relations: Strategic Engagement and Challenges, Center for Asian Studies, 2010
[21] David M. Malone and Rohan Mukherjee, India and China: Conflict and Cooperation, Survival Global Politics and Strategy Journal, 2010

India – China Trade at a Glance (*USD Billion*)



Source: PHD Research Bureau; Compiled from Trade Map Database

India – China Trade Statistics

	2001	2006	2011	2016
India's imports from China (USD billion)	**1.83**	**15.64**	**55.48**	**60.48**
CAGR (%)	-	53.6%	28.8%	1.7%
Share in India's total imports	3.6%	8.8%	12.0%	17.0%
India's exports to China (USD billion)	**0.92**	**7.83**	**16.72**	**8.92**
CAGR (%)	-	53.4%	16.4%	-11.8%
Share in China's total imports	0.4%	1.0%	1.0%	0.6%

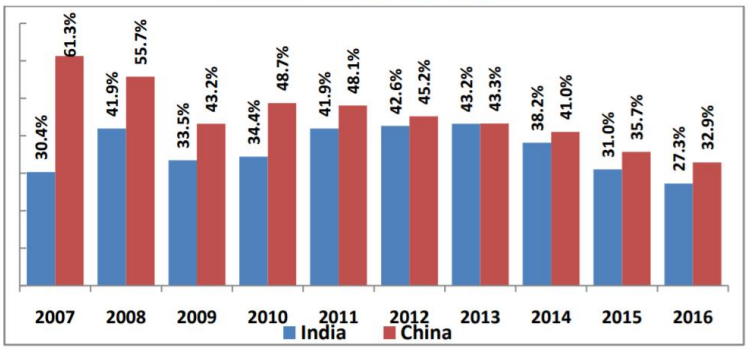
Source: PHD Research Bureau; Compiled from Trade Map Database

India – China Trade at a Glance (April – October 2017)

USD Million	Apr-17	May-17	Jun-17	Jul-17	Aug-17	Sep-17	Oct-17
India's exports to China	**978.46**	**751.37**	**754.56**	**793.64**	**908.29**	**1036.95**	**1224.6**
Growth (Y-o-Y)	40.08%	3.69%	20.85%	31.85%	60.08%	38.21%	72.13%
India's imports from China	**5904.12**	**5942.42**	**6237.88**	**6026.38**	**6489.53**	**6939.07**	**5907.76**
Growth (Y-o-Y)	64.75%	28.80%	16.67%	19.46%	20.55%	29.72%	4.22%

Source: PHD Research Bureau; Compiled from Ministry of Commerce and Industry

Trade-to-GDP ratio at a Glance



Source: PHD Research Bureau; Compiled from World Bank Database and Trade Map Database

Economic relation does not reflect however the altering status of political relation of the two Asian states. Indeed, tailspin's phases tracing favouring confrontation can result in standoffs such as the high altitude clash between the two nuclear powers like the above mentioned 2020 India-China skirmishes along the Sino-Indian borders, with the deaths of at least 20 Indian soldiers. In the next paragraph, we will briefly try to understand the different sources of historical confrontation between the two Asian states tracing different points of interest and friction within the Sino-Indian modern relations.

1.2. Sources of disputes and enmity

This paragraph will briefly analyse some of the main factors destabilizing the relationship between India and Cina throughout contemporary history. The Sino-Indian border issue has been a ceaseless factor of destabilization throughout modern history. The border covers a physical distance of 2,000 km extended through the boundary between Kashmir, Tibet and Xinjiang (western sector), Tibet-Kashmir-Himachal Pradesh border's intersection to to Nepal-Tibet-Uttar Pradesh conjunctions (middle sector) and the confluence of China-India-Bhutan to China-India-Myanmar border. However, according to Indian suggestions, the border is about 4,057 km as it should also include the Tibet-Sikkim border and a fragment of land between Xinjiang and Pakistan-controlled Kashmir.[22]

23

At the basis of the territorial dispute there is a divergent interest towards the strategic use of the disputed border. The dispute indeed concerns the construction of infrastructure, roads, airports and railways, which could facilitate the sending of reinforcements in case of an escalation of the dispute, such as the 2020 skirmishes. Infact, armed confrontation for the supremacy of the Himalayan region, also disputed by Pakistan, which controls Azad Kashmir with the political and military support of China, is dictated by the interest in carrying on the 'China-Pakistan Economic Corridor' between Xinjiang and the port of Gwadar on the Arab Sea, the flagship of the New Silk Road.[24]

[22] Tien-sze Fang, Asymmetrical Threat Perceptions in India-China Relations. OXFORD, 2014 – P.124
[23] Indian, Pakistani and Chinese border disputes: Fantasy frontiers**,** TheEconomist 2012
[24] Nicola Missaglia, ISPI Research Fellow, India Desk, India e Cina: cime tempestose, 2020

The border dispute has produced two different attitudes towards such an historical phenomenon. India is is apprehensive towards the threats produced by the lack of a peaceful solution at the borders, while China is propitious towards the *status quo* condition produced by the lack of a resolution. What also remains different is the different perception of legacy towards boundaries: for example, India believes the western border was delimited in 1842 by agreements signed by the authorities of Kashmir and Tibet, while the eastern border demarcated by the McMahon Line[25] established at the Simla Conference in 1913-1914. China believes such agreements to be a commodity of the British imperialist policies. Therefore, the legitimacy of such an historic agreement does not come from the Chinese central government. At the base of such phenomena we see two different perspectives: a Chinese expansionist theory, with the philosophy to seek revenge for the historical suffering caused by the imperialist phase of its history.[26] Simultaneously, India experienced Chinese' expansionist and containment policies. Indeed, ''China's threat'' syndrome was born first in India[27], before reaching the west, throughout the 60's.

28

Throughout the territorial dispute, the role of Tibet is of considerable importance. Since 1954, New Delhi officially endorsed Tibet as a legitimate part of China – however, it remains a factor of distrust in Sino-Indian relations. Indeed, Tibet became a strategic leverage for New Delhi due to its support towards exiled Tibetans (moving in India). The strategic status of Tibet began with the exile of the Tibetan leader, Dalai Lama, thousands of supporters, and the Tibetan government. The support offered to the Dalai Lama by the Indian state is a mean to refuse Beijing's expansionist policies in the region. However, by not interfering directly within the region of Tibet India results coherent with the principles of the ''*Panchsheel''* Treaty as it does not explicitly violate the principles of mutual respect for each other's territorial sovereignty, integrity, non- and non-interference in Chinese internal affairs.

[25] '' The McMahon Line is the demarcation line between Tibet and the North-east region of India proposed by British colonial administrator Sir Henry McMahon at the 1914 Simla Convention signed between British and Tibetan representatives. It is currently the generally recognized boundary between China and India, although its legal status is disputed by the Chinese government.'' Claude Arpi, Tibet: The Lost Frontier, 2008
[26] Zheng Yongnian 1998:5
[27] Wang 1997: 7-9
[28] Indian, Pakistani and Chinese border disputes: Fantasy frontiers**,** TheEconomist 2012

[29]

Tibet is a factor fueling in the Sino-Indian relations the territorial disputes, border tensions and water feuds.[30] However, Tibet became a variable in Beijing's relations with countries like India, Nepal and Bhutan that traditionally did not have a common border with China, but only afterwards annexation of Tibet by China. New Delhi operates on the Tibet issue through a bivalent strategy: oscillating between non-interference and therefore not supporting its independence publicly. Such a move allows the Tibetan government and its followers to operate within India. The synthesis laying at the base of such policy is that India is perpetually concerned about possible threats to its security, after the 1962 war. When the military (and economic) capabilities are inferior, states need to build new capabilities such as soft power's forms of coercion: and the Tibet issue remains important strategic leverage for New Delhi and therefore destabilizing factor affecting China-India relations. However, China's hydro-engineering projects in Tibet highlight the strategic importance of the region for both countries, especially when water becomes the source of the conflict.[31]

The Tibetan territory dispute is characterised on one hand by Tibetan supporting the independence of the region before the peaceful liberation of Tibet. The mentioned liberation refers to the annexation (in Western opinion) of Tibet by the People's Republic of China by which it gained control of the region. On the other hand, China declaring its sovereignty over the region since China's Yuan Dynasty (1271-1368). However, leaving aside the strategic dialogues over the region, why is sovereignty over Tibet (Tibet Autonomous Region) so important for the PRC? A synthesis can be traced at President of People's Republic of China Jiang Zemin's statement at the Fourth Tibetan Work Forum in Renmin Ribao stating that Tibet's importance laid at the base of China's grand western development strategy, social stability, national unity, unification and security of motherland and for China's national image.[32] The power gap between the two Asian states, different ambitions to expand over the region of Asia, different foreign policies and also different misperceptions of threat, forge the issue of Tibet still as a hot spot in Sino-Indian relations.

[29] Laura Canali, Limes Maps
[30] Brahma Chellaney, Why Tibet remains the core issue in China-India relations, Forbes, 2014
[31] Ibid.
[32] Tien-sze Fang, Asymmetrical Threat Perceptions in India-China Relations. OXFORD, 2014 – PG. 61

A vital factor of destabilization in the history of Sino-Indian relations has been the nuclear power evolution and projection of India and China. What characterises the bilateral relations is ''the asymmetry in terms of motives for nuclearization and the perceived nuclear threat''.[33] The policy which have guided China towards nuclear deterrence has never emerged against India, rather was directed towards US, USSR and their global bipolar engagement typical of the Cold War period. However, the situation has always been different from New Delhi's perspective. Indeed, the main sources of Indian's anxiety towards Chinese nuclear posture were: Chinese nuclear capability to blackmail and/or coerce India, China's stance towards nuclear proliferation due to its assistance to Pakistan and Chinese diplomatic and political status (and negotiation posture) as an Asian nuclear power.[34]

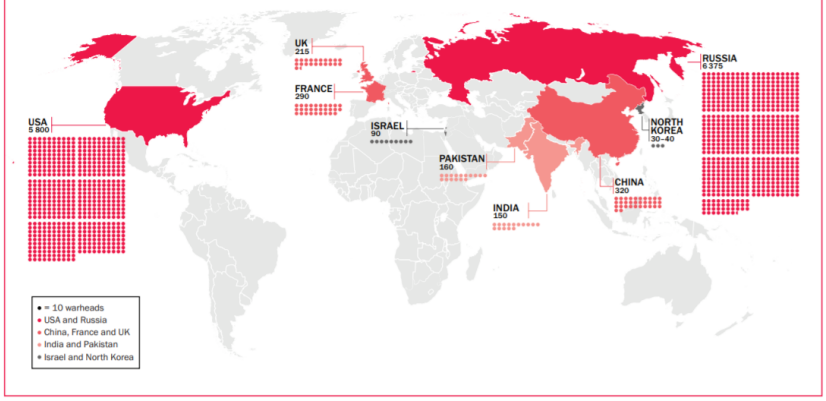
The starting point of the nuclear destabilization factor of Sino-Indian relations is to be found in 1964, when China exploded its first atomic bomb. In fact, India's nuclear evolution strategy and programme finds as its natural opponent (and stimulus) China's nuclear development, being the strongest nuclear power within the Asian region. India's nuclear history begins before being defeated by China in 1962. In the 50's, India started a civilian nuclear programme and in the 70's tested its first nuclear devices through the Peaceful Nuclear Explosion[35] surprising other States. India found itself in a sort of nuclear limbo characterised by two main alternatives: being a non-nuclear state or being a nuclear weapons state. The latter prevailed causing structural changes within Sino-Indian military and diplomatic relations, due to Beijing being alerted. And later ''India's retaliation posture has evolved towards survivable second-strike forces – survivability''.[36] The two national nuclear evolutions caused the conditions of security dilemma driven by a rush towards increasing the 'great power status', through national nuclear development programmes.

According to SIPRI Yearbook 2020, nuclear states having minor nuclear arsenals are focusing on developing, or at least declaring the intention of deploying a new weapon system. Such a matter, on one hand, sees the China in the middle of an important expansion and modernization of its nuclear arsenal. However, despite the speculation that China's program shifting from a strategy of minimum deterrence to one of limited deterrence, "it is fairly safe to say that Chinese capabilities come nowhere near the level required by the concept of limited deterrence."[37] What has been considered a threat since the 1980s by the nuclear community is Chinese missile-related exports (e.g. supplied Pakistan with 34 DF-11 short-range missiles in 1992).[38] While on the other hand, India is trying to increase the size of its nuclear arsenal.[39] India has a largely indigenous nuclear power programme and is committed to growing its nuclear power capacity as part of its massive infrastructure development programme through an ambitious targets to grow nuclear capacity.[40]

''Chinese President Xi Jinping and Indian Prime Minister Narendra Modi are both political strongmen who project muscular security policies and under their leadership, Beijing and New Delhi are improving their nuclear arsenals and conventional military capabilities.''[41] Such technical and political developments could generate a new nuclear deterrence paradigm in Southern Asia if relations between the two states take a more belligerent turn.''[42] Is such a trend vicious for Sino-Indian relations?

[33] John Garver, 2001
[34] Wu and Song 1998
[35] ''Nuclear explosions carried out for non-military purposes, such as the construction of harbors or canals. PNEs are technically indistinguishable from nuclear explosions of a military nature. Article V of the Non-Proliferation Treaty (NPT) allows for PNEs.'', Comprehensive Nuclear-Test-Ban Treaty Organization
[36] Narang, 2014
[37] NTI Building a Safer World, China, 2015
[38] NTI Building a Safer World, China, 2020
[39] SIPRI Yearbook 2020
[40] World Nuclear Association, Nuclear Power in India, 2020
[41] Toby Dalton, At a Crossroads? China-India Nuclear Relations After the Border Clash, Carnegie Endowment for International Peace, 2020
[42] Ibid.

GLOBAL NUCLEAR WEAPON STOCKPILES, 2019



Note: The boundaries used in this map do not imply any endorsement or acceptance by SIPRI.

WORLD NUCLEAR FORCES, 2019

Country	Deployed warheads	Other warheads	Total inventory
USA	1 750	4 050	5 800
Russia	1 570	4 805	6 375
UK	120	95	215
France	280	10	290
China	–	320	320
India	–	150	150
Pakistan	–	160	160
Israel	–	90	90
North Korea	–	[30–40]	[30–40]
Total	**3 720**	**9 680**	**13 400**

43

The 15th June 2020 military conflict over disputed territory in the Himalayas shook Sino-Indian relations. The clash in the Galwan Valley along their shared border is the heaviest military confrontation the two nuclear powers have faced in fifty years. A report by the Stockholm International Peace Research Insitute states that India has the third biggest defense budget at $71.1 billion, while China's defense budget is more than three times that of India at $261 billion.[44]

Army

Particulars	India	China
Tanks	4,292	3,500
Armored vehicles	8,686	33,000
Self-propelled artillery	235	3,800
Field artillery	4,060	3,600
Rocket projectors	266	2,650

Source: Global Firepower

Air power

Particulars	India	China
Combat aircraft	538	1,232
Dedicated attack aircrafts	172	371
Special mission planes	77	111
Helicopters	722	911
Helos	23	281

Source: Global Firepower

[43] SIPRI Yearbook 2020
[44] Rounak Jain, India vs Chine defense budget and equipment comparison, Business Insider, 2020

Naval power

Particulars	India	China
Aircraft carriers	1	2
Submarines	16	74
Destroyers	10	36
Frigates	13	52
Corvettes	19	50
Mine warfare	3	29
Coastal patrol	139	220

Source: Global Firepower

‘’Indian security analysts pay great attention to China’s nuclear policy and capabilities while Chinese analysts maintain a dismissive attitude about the relevance of nuclear weapons within the bilateral relations. The different attitude stems from a widely held view that India’s indigenous military technologies are significantly behind China’s and that China will continue widening the gulf between the two countries’ conventional and nuclear capabilities.’’[45] However, Chinese analysts tend to understimate the long-term destabilizing implications of this growing gap which may lead India to feel pressure expand its nuclear arsenal, and this could further threaten the fragile stability between India and Pakistan.[46] China tends to underestimate the role Beijing may have in shaping New Delhi’s threat perception and nuclear strategy.[47]

The fragility over the Sino-Indian relations in general can be understood in terms of mutual expectations and perceptions of threat, destabilizing the dimension of cooperation. Misperception, perceptions of centralization, overestimating one’s importance as influence and target, the influence of desire and fears on perception, and cognitive dissonance[48] are all factors which have further deteriorated the earliest sincere spirit of cooperation between the two states. Deprivation produced by the perception of threat, through an expectation of harm to assets or values[49], leads to possible competition in different areas such as the military and the economy. Such a fragility comes from an historical enmity[50] leading to malevolence and amplifying perceptions of threats.[51]

Misperception of threat leads to countermeasures against possible threats. Sino-Indian relations are characterised by balancing countermeasures: on one hand, increasing strength, reducing personal vulnerabilities[52] internal balancing[53]. On the other hand, allying with states sharing the same concerns[54] such as the Sino-Pakistani military cooperation to externally balance[55] India in the Kashmiri issue. A solution for such a fragility could have been conducted confidence-building measures to reduce military intent and therefore capabilities.[56] However, the reality is that states with higher perception of threat try to change the *status quo* (basically India has been the latter throughout the 20th century), while states with a lower perception of threat will try to ensure the *status quo*, like China.

[45] Toby Dalton, At a Crossroads? China-India Nuclear Relations After the Border Clash, Carnegie Endowment for International Peace, 2020.
[46] Ibid.
[47] Ibid.
[48] Robert Jervis 1976, Asymmetrical Threat Perceptions in India-China Relations. OXFORD. Tien-sze Fang. 2014
[49] Baldwin 1971: 71-8, Ibid.
[50] David Singer 1958: 93 Ibid.
[51] Buzan 1998: 59 – Ibid.
[52] Buzan 1998 – Ibid.
[53] ‘’Internal balancing: According to the balance of power theory, states, motivated primarily by their desire for survival and security, will develop and implement military capabilities and hard power mechanisms in order to constrain the most powerful and rising state that can prove a potential threat’’, Kenneth N. Waltz, "Realism and International Politics" (New York: Routledge, 2008), 137
[54] Buzan 1998 – Ibid.
[55] External balancing: condition under which states come together and form an alliance to balance and gain more leverage over a dominant or rising power. Stephen G. Brooks and William C. Wohlforth, "World out of Balance" (Princeton: Princeton University Press, 2008)
[56] Krepon 1998 – Ibid.

Misperception of threat also impacted the different influence projections in the Asian region. However, reducing such a perception is necessary and fundamental for the regional security and the economic growth of both the states. Indeed, it is fundamental to keep in mind that both China and India have turned South Asia into an area of rivalry and enmity. Since the 60's, China retained its influence within the region through different approaches (economic partnerships and military collaboration) with Pakistan countering New Delhi. On the other side, relations between India, Japan and the ASEAN states (Association of Southeast Asian Nations) countering Beijing, seems like a perpetual threat in China's risk assessment. Indeed, India's 'Look East' policy[57] engaging the ASEAN states, Taiwan, South Korea and Japan created turned into a new opportunity of competition, and not cooperation.

The two states have nevertheless found reasons to cooperate geographic proximity for example has been an important opportunity of cooperation by enlarging huge markets demanded by both large populations[58], fuelling bilateral trade. At the same time, such a proximity was an opportunity of cooperation in regards of illegal cross-border activities, drug trafficking and cross-border crimes. Special attention has been posed on anti-terrorism cooperation[59] to combat Islamic militancy emerging from Afghanistan and Central Asia since the late 1980s. Such a phase of regional collaboration evolved in India joining as an observer status the Shanghai Cooperation Organization (SCO), and afterwards China being accepted in 2005 as an observer State at the South Asian Association for Regional Cooperation (SAARC), the organization fuelling economic and political cooperation throughout South Asia.

The opening chapter introduced the historical evolution of Sino-Indian relations. particularly, by exploring the evolution of the latter throughout the 20th and 21th century. The first section touched different historical points, starting from a historical bracket dealing with the cultural civilization proximity. It later analysed the progression from the *Hindi Chini Bhai Bhai* era, to the deterioration by the end of the 50's, to the 2020 skirmishes at the border lately in order to point out the altered state of the relations between the two Asian states. In order to understand the relations' fragility, the second section investigated on several main factors of destabilization: the Sino-Indian border issue, the importance of Tibet, the nuclear history and strategy of the two Asian states and the implications of asymmetrical perceptions of threat. The historical analysis of the twisting relations serves to understand the points of rupture between the two states, to carry on with the upcoming topic in regards of the modern challenge of cyber competition between China and India.

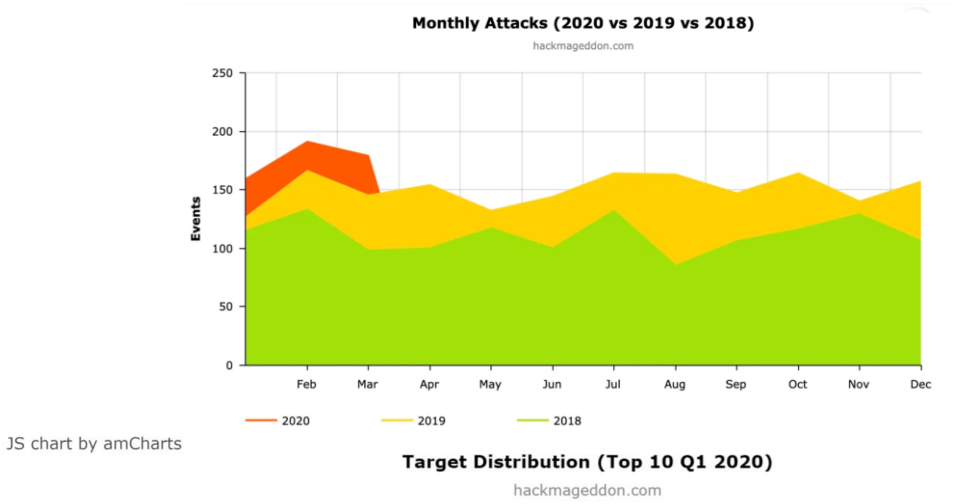
[57] ''India's Look East policy is an effort to cultivate extensive economic and strategic relations with the nations of Southeast Asia to bolster its standing as a regional power and a counterweight to the strategic influence of China.Initiated in 1991, it marked a strategic shift in India's perspective of the world.'', Thongkholal Haokip, "India's Look East Policy: Its Evolution and Approach," *South Asian Survey*, Vol. 18, No. 2, 2011

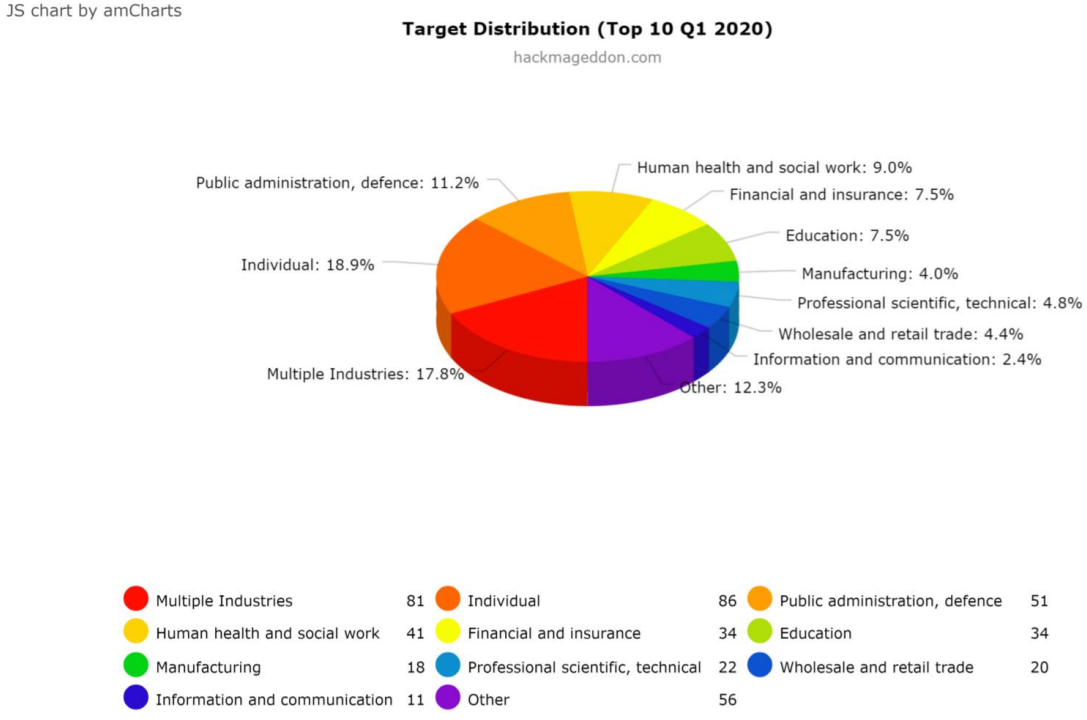
[58] Xinhua 1996 – Ibid.

[59] Xinhua 2002 – Ibid.

2. Cyberwarfare

‘’Chinese hackers attempted attack on Indian cyberspace more than 40,300 times in a week post-Galwan clash.’’[60] The mentioned headline has alerted on June 2020 the public of new confrontations between China and India but this time taking place on cyberspace. Indeed, attacks on National Information Technology infrastructure have increased in recent years (especially in 2020 due to national lockdowns imposed in the wake of Covid-19 pandemic[61] by governments and the consecutive rise of social distancing[62] and digital devices’ usage such as smart working[63]) becoming a new threat for national security and therefore a subject matter for academic scholars. In fact, to better understand such a modern type of conflict played on cyberspace, but originating from ‘’physical’’ causes of dispute, we shall open a theoretical parenthesis in the next paragraph, to better understand and contextualize cyber security within the field of international relations. Below some statistics infographics are shown representing the increasing trend in 2020 monthly attacks, target distribution and motivations by target.[64]





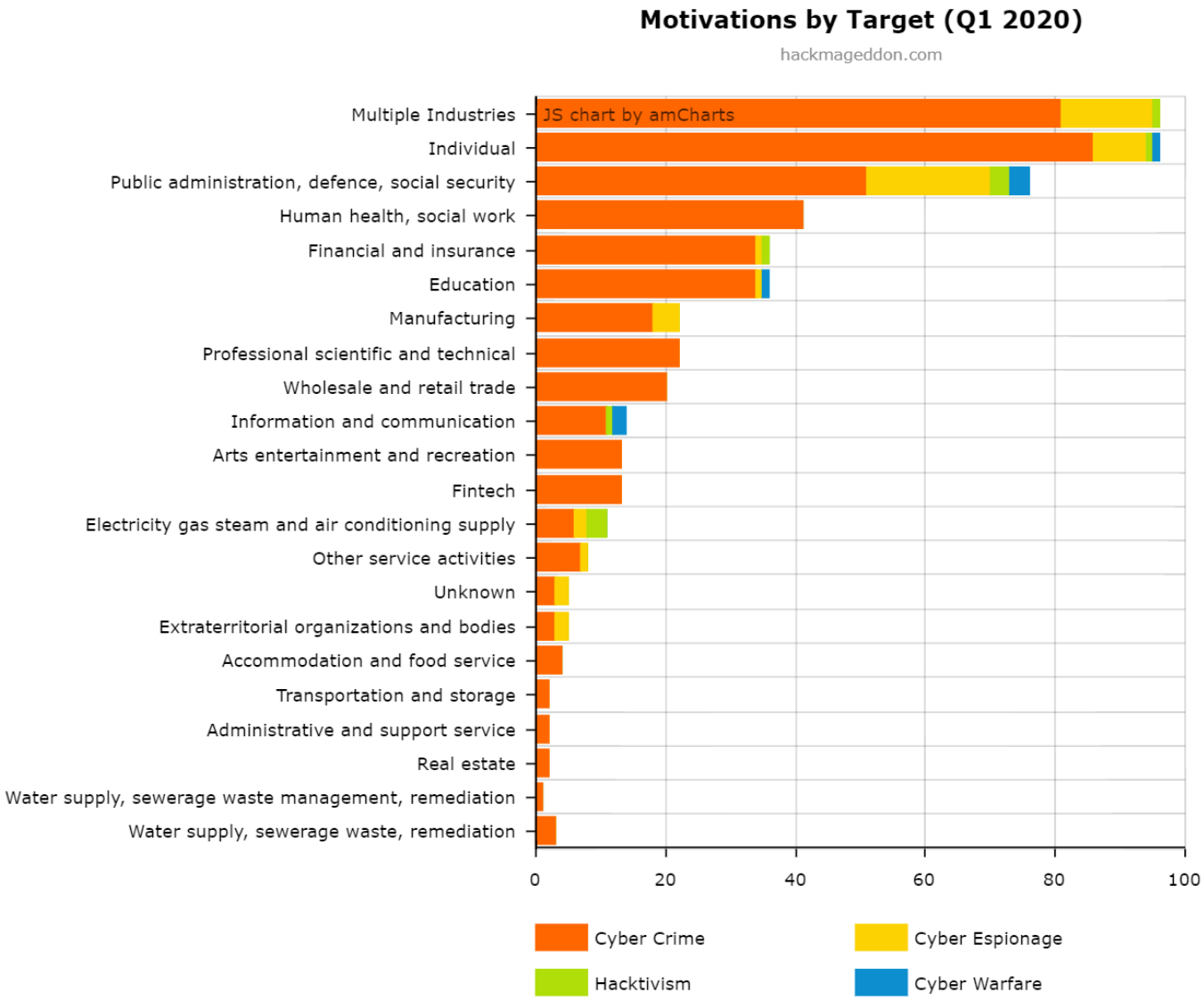
[60] Timesnownews Article, June 2020 https://www.timesnownews.com/india/article/chinese-hackers-attempted-attack-on-indian-cyberspace-more-than-40300-times-in-a-week-post-galwan-clash/610315

[61] ‘’The COVID-19 pandemic, also known as the coronavirus pandemic, is a pandemic of corona virus 2019 (COVID-19) caused by severe respiratory syndrome coronavirus (SARS-CoV-2)’’, "Naming the coronavirus disease (COVID-19) and the virus that causes it", World Health Organization

[62] In public health, social distancing, also called physical distancing, is a set of non-pharmaceutical interventions or measures intended to prevent the spread of a contagious disease by maintaining a physical distance between people and reducing the number of times people come into close contact with each other.

[63] The agile work (or smart working) is a mode of execution of the employment relationship characterized by the absence of time or space constraints and an organization by phases, cycles and objectives, established by agreement between employee and employer; a mode that helps the worker to reconcile life and work time and, at the same time, promote the growth of its productivity, Italian Ministry of Labour and Social Policies.

[64] Hackmageddon, Information Security Timelines and Statistics, 2020


Motivations by Target (Q1 2020)
hackmageddon.com
JS chart by amCharts
Multiple Industries
Individual
Public administration, defence, social security
Human health, social work
Financial and insurance
Education
Manufacturing
Professional scientific and technical
Wholesale and retail trade
Information and communication
Arts entertainment and recreation
Fintech
Electricity gas steam and air conditioning supply
Other service activities
Unknown
Extraterritorial organizations and bodies
Accommodation and food service
Transportation and storage
Administrative and support service
Real estate
Water supply, sewerage waste management, remediation
Water supply, sewerage waste, remediation
0
20
40
60
80
100
Cyber Crime
Cyber Espionage
Hacktivism
Cyber Warfare

2.1. Cyberspace and Cybersecurity within International Relations

Tracing a definition of cyberspace is dutiful since domains of global security have recently shifted from physical spaces towards cyber playing fields. In fact, the cyberspace has become the realm of intelligence and military states' activities, also shaping foreign policy, through cyber-attacks and intrusions. However, dealing with a precise definition of cyberspace and its possible implications is not easy: ''cyberspace is not about being a new technology, rather a technology-enabled domain for humans and machines to live and interact, a hypostatic abstraction[65], a political reality.''[66] ''The concept of cybernetic risk is closely associated with that of "cybernetic space" or cyberspace, a term born in science fiction in the eighties of the last century and then cleared first in military and then in general terms. It indicates the global domain resulting from the interconnection of all those networks, heterogeneous and interdependent, made of information processing systems and communication infrastructures. This domain, although commonly perceived as a sort of immaterial dimension, is now unanimously recognized as an objective and concrete reality, even subject to the legitimate sovereignty of states, even if still in the absence of specific regulations or international agreements and even a shared definition of its very nature.''[67]

For such an assumption, cyberspace can be considered as a game changer that added an extra layer of complexity to international relations, one which we are dangerously unprepared to cope with which confronts us with a man-made domain in continuous technological evolution and of which citizens only partially understand the cultural, political and military disruptive implications.[68] However, following the National Academy of Science' definition of cyberspace, it refers to ''the artifacts based or dependent on computing and communications technology; the information that these artifacts use, store, handle, or process; the interconnections among these various elements'.[69] What remains difficult is not only to conceptualize the idea of cyberspace, but rather to understand the implications the latter can have in international relations and on the international security environment through its potential impact.

In order to shed light on the power cyberspace may have in influencing global politics, focusing on its historical implications on international relations is fundamental. Most important cases to explicate new challenges in the political sphere were the cyber-attacks launched in Estonia in 2007 and probably the most important known as Stuxnet case. First uncovered in 2010, Stuxnet was a malicious cyber worm used, ''probably'', by United States and Israel as the first weaponized malware to sabotage Iran's nuclear programme, causing the nuclear centrifuges to spin out of control while producing signals that operations were normal.[70]

''Probably'' refers to the difficulty in attributing the nature and origins of the attack. Probability is a key variable of cyberspace. In fact, the ability to hold responsibility for cyber operations, intrusions, or attacks, is quite difficult due to the attribution problem (state and non-state) misleading the disguising any type of involvement. Related to the attribution conundrum, Thomas Rid, an important political scientist known for his studies on risks of information technology in conflict studies, states that '' the attribution problem in digital forensic is always a question of what evidence did you get, but there is still this 'attribution is impossible' knee jerk reaction that occasionally pops up.''[71] In fact, the attribution conundrum heavily relies not only on technical data but also on intelligence activities. The attribution conundrum remains a core issue of cyberspace, primarily when dealing with the concept of self-defence in conflicts. In fact, the Senior Research Scholar and Military Personnel Jason Healey states that the 'whodunit' approach may be completely weak and dangerous: adopting a 'spectrum of responsibility' may better trace potential responses

[65] Hypostatic abstraction in mathematical logic, also known as hypostasis or subjectal abstraction, is a formal operation that transforms a predicate into a relation. New media, digital media, Internet, cyberspace-techniques of mass symmetrical communication-have created a particular interactive informational space in which information plays the most important role, influencing the shape of social life.
[66] W. Gibson, "A consensual hallucination experienced daily by billions of legitimate operators", *Neuromancer*, 1984
[67] Corrado Giustozzi, Cos'è il "rischio cyber" e perché ce ne dobbiamo preoccupare, ISPI, 2019
[68] F. Rugge, "An 'Axis' Reloaded?", in Idem (ed.), *Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace*, ISPI Report, 2018.
[69] National Academy of Science 2014:8
[70] Broad et al. 2011
[71] Thomas Rid - Newman 2016

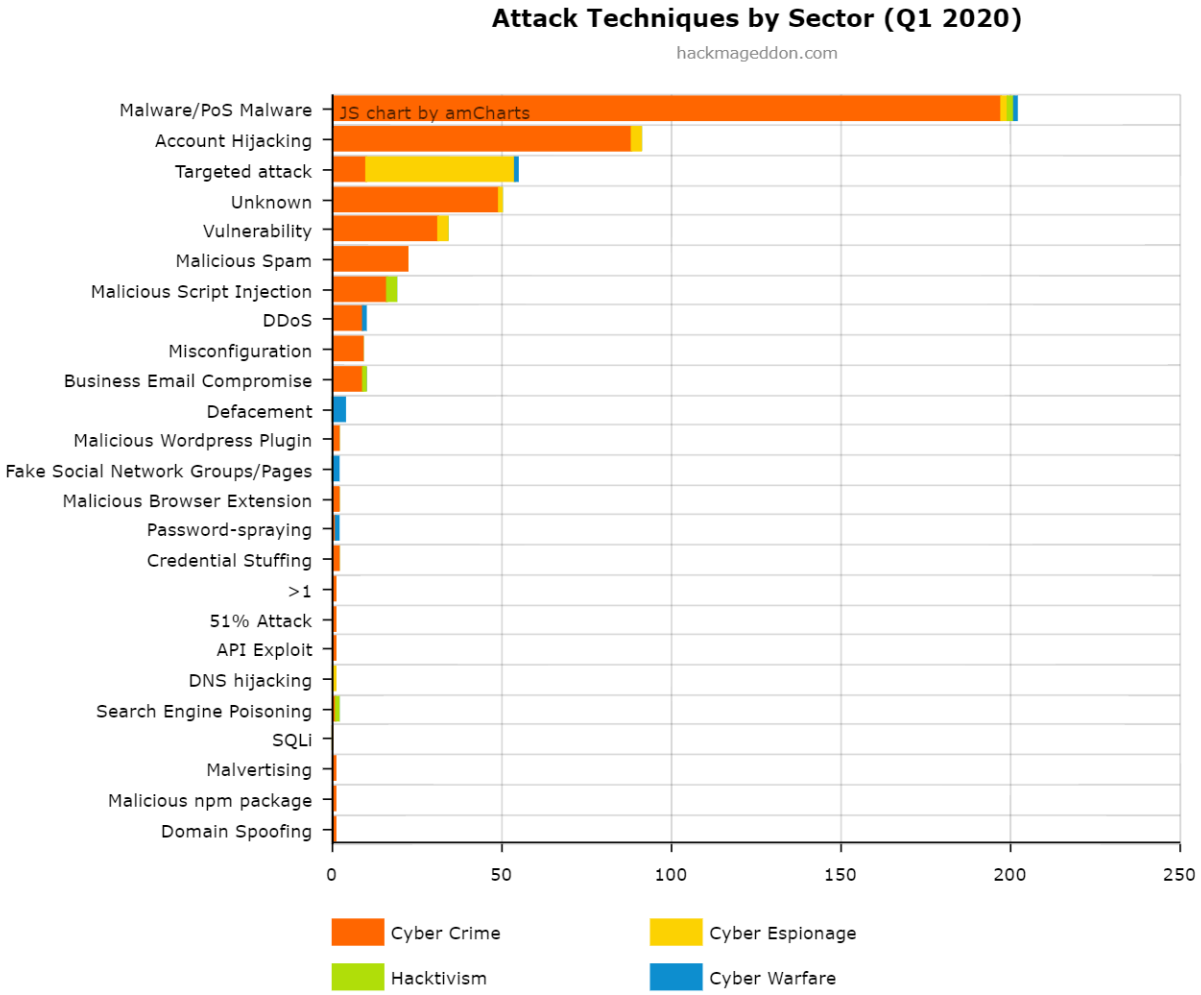
to cyber operations.

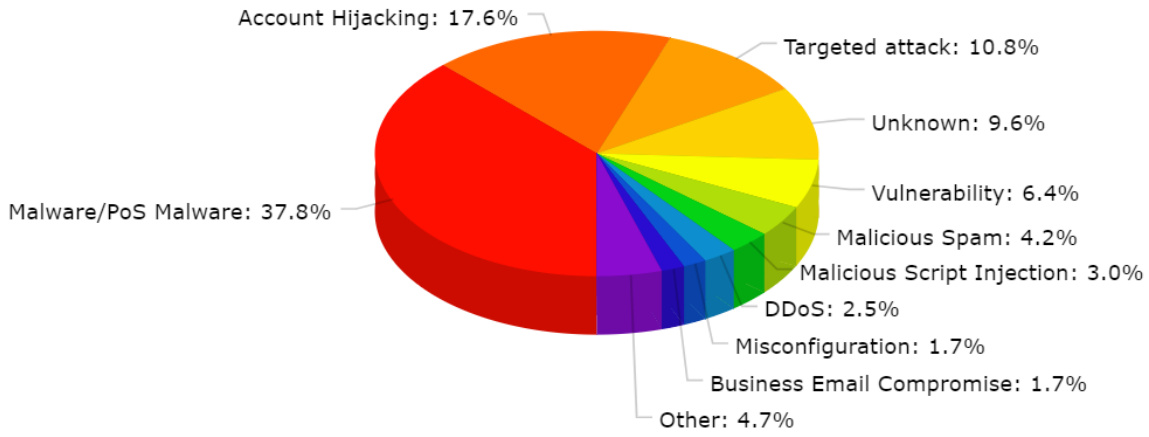
Going back to the importance of cyber power, cybersecurity and their impacts within the international security theatre, the American political scientist Joseph Nye declares ‘’defined behaviourally, cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. Power based on information resources is not new; cyber power is. There are dozens of definitions of cyberspace but generally “cyber” is a prefix standing for electronic and computer related activities. By one definition: “cyberspace is an operational domain framed by use of electronics to …exploit information via interconnected systems and their associated infra structure.”[72] Power depends on context, and cyber power depends on the resources that characterize the domain of cyberspace.[73] This includes the Internet of networked computers, but also intranets, cellular technologies, fibre optic cables and space-based communications. Cyber power can be used to produce preferred outcomes within cyberspace, or it can use cyber instruments to produce preferred outcome in other domains outside cyberspace’’.[74]

Cyber power is given by the capability of a state or a non-state actor to conduct cyber operation, even known as ‘computer network operations’, which can be divided in computer network attacks, computer network exploitation and computer network defence. The first two mentioned, may be described as ‘’the use of deliberate actions and operations – perhaps over an extended period of time – to alter, disrupt, deceive, degrade or destroy adversary computer system networks or the information and (or) programs resident in or transiting these systems or networks’’.[75] Complexity is to be found in the subtle difference between attacks and exploitation. In fact, according to the Senior Research Scholar in cyber policy and security Dr. Herbert Lin, cyber exploitation is non-destructive and its main goal is to obtain information that would otherwise be kept confidential.[76] An important feature of the exploiting nature of such activities, is its minimal disturbance to the target and the presence on the targeted network or system.[77]

An important detail to stress is the variety of attack techinques targetting different sectors. On one hand, cyber espionage has become a feature of the digital age. Indeed, the first actors to penetrate cyberspace have been states’ intelligence services. Intelligence through computer network exploitation seek to capture sensible data to give strategic advantage to government, especially in relation to foreign relations. Originally, states were the exclusive actors to control technological resources to operate domestically and internationally. Technologization of international relations, however, have moved differently from nuclearization: the different availability of resources have given the chance to non-state actors and business enterprises to become actors within cyberspace. On the other hand, attacks can be framed within cyber crime, hacktivism and cyberwarfare and can be launched through different methods like: malware[78], account hijacking[79], malicious spam[80] and denial-of-service attack (DoS).[81] The charts below show a statistic of 2020’s attack distribution and attack techniques by sector.[82]

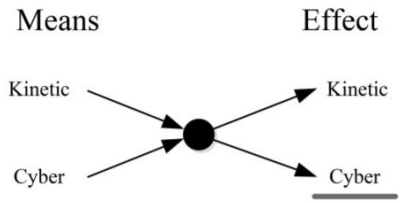
[72] Kuehl, 2009
[73] Joseph S. Nye, Cyber Power, Harvard Kennedy School, 2010
[74] Joseph S. Nye 2011a: 123
[75] Dr. Herbert Lin – 2010: 63
[76] Ibid.
[77] Ibid.
[78] ‘’Malware (a portmanteau for malicious software) is any software intentionally designed to cause damage to a computer, server, client, or computer network’’, Microsoft.
[79] ‘’Account hijacking is a process through which an individual’s email account, computer account or any other account associated with a computing device or service is stolen or hijacked by a hacker. It is a type of identity theft in which the hacker uses the stolen account information to carry out malicious or unauthorized activity’’, Techopedia
[80] "Spam is any kind of unwanted, unsolicited digital communication, often an email, that gets sent out in bulk’’, Malwarebytes
[81] In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled’’, Understanding Denial-of-Service Attacks
[82] Hackmageddon, Information Security Timelines and Statistics, 2020





Malware/PoS Malware	200	Account Hijacking	93	Targeted attack	57
Unknown	51	Vulnerability	34	Malicious Spam	22
Malicious Script Injection	16	DDoS	13	Misconfiguration	9
Business Email Compromise	9	Other	25		

Cyber operations can be labelled in offensive cyber operations (OCO)[83], defensive cyber operations (DCO)[84], and DODIN[85] operations. While conventional attacks are easy to estimate due to the damage caused by such weapons is often explicit, cyber operations have both conceptual and practical challenges to evaluate possible damages and collateral damage.[86] Conceptually, ‘’the lack of agreement about what constitutes “harm,” specifically surrounds the question of whether mere breaches of the confidentiality, integrity or availability of data without any physical effects should constitute “damage” for the purposes of collateral damage estimations.’’[87] Practically, ‘’ the outcomes of cyber operations can be much more uncertain than physical operations, and evidence of whether any damage has occurred at all may be unavailable since harms that originate in code may be latent or transient.’’[88] For example, a software vulnerability exploited by an adversary could be used to install a software program in order to cause the adversary’s power station to overload and later be physically destroyed. A conventional bomb, or cyber attack, may have similar implications on physical effects. For example, in 2003 the U.S. military physically destroyed communication systems in Iraq through a cyber attack campaign, disabling satellite and other communications equipment that provided service to Iraqi military forces and civilians in Iraq and neighboring countries.[89]



This section of the thesis focused on the concept of cyberspace and cyber security, framed within the context of international relations. To give a comprehensive view of states’ modern and digital threats, it analysed the concept of cyber power, cyber capabilities, and cyber operations, in order to move the following section of the work.

[83] ‘’Cyberspace activities intended to project power dodin (i.e. cause an effect) “in and through cyberspace’’, Dictionary of military and associated terms, 2017
[84] ‘’Defensive cyber activities taken in response to an adversary’s actions (such as an attack, or imminent threat)’’,
[85] ‘’DODIN operations are those typically known as cyber security efforts that protect one’s computer network and information from compromise’’, Dictionary of military and associated terms, 2017
[86] ‘’Unintended harm to a computer or information system that is not the target of a lawful cyber operation.47 Where “harm” is defined as either a) the deletion, manipulation, or alteration of computer code governing the operation of hardware or software that is not specifically intended by the party conducting a lawfully-authorized operation, or b) the compromise of the integrity or availability of a computer network or data, or exfiltration of data, that is not specifically intended by the party conducting a lawfully-authorized operation.’’, Understanding Cyber Collateral Damage - Journal Of National Security Law & Policy
[87] Sasha Romanosky & Zachary Goldman, Understanding Cyber Collateral Damage, 2017
[88] Ibid.
[89] John Markoff and Thom Shanker, Halted ’03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk, N.Y. TIMES, 2009

2.2. Assessment of international norms regulating the cyberspace and cybersecurity

The Internet is a complex system. Its impacts within international relations also. Internet is a decentralized structure whose functioning depends on a series of technical protocols, laws, and international regulations.[90] On whole regulated from a multistakeholder and multilateral approach coordinated by governments, citizens, and other social parts. But why does the Internet and especially the cyberspace in terms of cybersecurity need a set of strict regulations? The main answer refers to the exposure to cyber threats, especially in an age characterised by digital infrastructures, digital markets and the dependence on connectivity.[91] The dependence on connectivity through cyberspace and the Internet, through digital diplomacy, influenced international relations. For example, the three main impacts have been: ''first, it multiplies and amplifies the number of voices and interests involved in international policy-making, complicating international decision-making and reducing the exclusive control of states in the process; second, it accelerates and frees the dissemination of information, accurate or not, about any issue or event which can impact on its consequences and handling; third, it enables traditional diplomatic services to be delivered faster and more costeffectively, both to ones' own citizens and government, and to those of other countries.''[92]

The capability and implications posed by the danger of cyber threats may be even greater (and statistically more plausible to happen) than a war or skirmishes between states. Nevertheless, developing a jurisdiction governing cyber activities has been and still is a quite difficult pattern. Professor Martha Finnemore argues that ''a complex and technical problem like cyber security might not obviously lend itself to simple norms, but that is the challenge''.[93] But is there a rule of law within cyberspace and internet? And if it is there, could it be at risk? Efforts have been made by United Nations Group of Experts, but with little success. An important effort is the Budapest Convention on Cybercrime, which entered into force in 2004. The Convention is the first international treaty focusing ''on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security''[94], in order to pursue an appropriate legislation to increase international cooperation and pursuit customary criminal procedures. However, since the Convention was endorsed by the Council of Europe, it remained a regional effort which was projected also to the non-members of Council of Europe: China and India were not present. [95]

An important and comprehensive source of legal norms to apply international law about cyber norms is the Tallinn Manual, which was assessed in two different versions (1.0 and 2.0). The *Tallinn Manual on the International Law Applicable to Cyber Operations* (2013) originates in 2009 within NATO[96]'s framework. NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), being an international military organisation established in Tallinn (Estonia), requested an international group of experts, comprising leading legal scholars, to produce a manual on the law governing cyber warfare, following the footsteps of earlier efforts. Defining cyberwarfare is not so simple. Former Special Advisor to President Bush on Cybersecurity, R. Clarke defines cyberwarfare as ''actions by a nation-state to penetrate another nation's computer or networks for the purpose of causing damage or disruption''[97]. The definition given by R. Clarke is important not for its own sake, rather it separates cyberwarfare from cybercriminals. Being domains of states' property, and not criminals, understanding the implications of cyberspace within international relations is fundamental to understand the transformation of conflict between states and the new challenges. The origin of such a

[90] Andrea Calderaro, Overcoming Fragmentation in Cyber Diplomacy: The Promise of Cyber Capacity Building, ISPI, 2020
[91] Ibid.
[92] Nicholas Westcott, Digital Diplomacy: The Impact of the Internet on International Relations, Oxford Internet Institute, 2008
[93] Martha Finnemore (2011: 93)
[94] Council of Europe Portal – Details of Treaty No. 185 Convention on Cybercrime
[95] Chart of signatures and ratifications of Treaty 185: Members of Council of Europe: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Republic of Maldova, Russian Federation, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom;
Non-Members of Council of Europe: Argentina, Australia, Benin, Brazil, Burkina Faso, Cabo Verde, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ghana, Guatemala, Israel, Japan, Mauritius, Mexico, Morocco, Niger, Nigeria, Panama, Paraguay, Peru, Philippines, Senegal, South Africa, Sri Lanka, Tonga, Tunisia, United States of America
[96] North Atlantic Alliance is an intergovernmental military alliance between 30 North American and European countries. The organization implements the North Atlantic Treaty that was signed on 4 April 1949
[97] Richard Clarke and Knake, Cyber War, p.6

product directly came from the attention the NATO's alliance legal community drew on cyber operations, especially in the 90's, specifically focusing on cyber operations (e.g. case of Estonia 2007[98]) and cyber incidents (i.e. the Stuxnet case.)[99] Therefore, states' challenges became to find a guideline to comprehend the international law's applicability over cyberspace and cyberoperations, being offensive or defensive in nature. The manual, by not being a Treaty, scrutinizes the international law governing 'cyber warfare', ranging from full application of the law of armed conflict along the lines of the pronouncements of the International Court of Justice being to application guided by the Permanent Court of International Justice on permission of acts generally not forbidden in international law.[100] The main pillar of the Tallinn's guide is that cyber warfare is bounded by existing norms of international law and by the prohibition on the use of force also applicable to cyber operations, with a special attention on the laws of armed conflict (LOAC) and international humanitarian law (Geneve Conventions).

Indeed, the manual deals in laws of armed conflict must be applied to the cyber domain and cyberspace: concepts and procedures of the *jus ad bellum* (right to war) and *jus in bello* (conduct of war). Indeed, the translatlantic community was towards the concept of customary international law applied to cyberspace.[101] ''The development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete''[102], and therefore ''long-standing international norms guiding State behaviour – in times of peace and conflict – also applying in cyberspace''.[103] The most important guidelines are: the prohibition on the use of force in international law is also applicable to cyber operations, the basis as to whether a cyber operation rises to the level of an act of war is if it causes harm to individuals or damage to property equivalent to a use of force; the actual impact of the cyber operation is critical as a cyber operation resulting in inconvenience and minor disruptions are not considered to be an act of war or a use of force and States are responsible for cyber-attacks even if they are conducted by a non-state entity within their borders if the state is aware of them or these groups act under their direction.[104] Indeed, for example, the manual focus on cyber-to-cyber operations, such as a cyber-attack against a state's critical infrastructure[105] or targeting enemy command and control systems.[106] However, the Tallinn Manual leaves aside a variety of cyber domain features such as cyber espionage, theft of intellectual property and the rest of criminal activities occurring in cyberspace (activities not covered by international law on the use of force and armed conflicts) which may pose serious threats to states' national security, corporations, citizens and international security.

To cover such a missing gap, *Tallinn 2.0* was published in 2017 to address those cyber activities falling beneath the threshold of war.[107] Tallinn 2.0 broadened the commission of experts, by including members from non-western world (China, Japan, Thailand, and Belarus) and substantive expertise in space law, human rights, and international communications law. The updated manual deals with those malicious cyber activities involving major cyber breaches, which may lead to armed conflict between states. The goal of the project again does not seek to create a real jurisdiction governing cyberspace but ''to reflect the law as it existed at the point of the Manual's adoption by the two International Groups of Experts in June 2016. In is not a 'best

[98] Rain Ottis ''In the spring of 2007 Estonia fell under a cyber attack campaign lasting a total of 22 days. The attacks were part of a wider political conflict between Estonia and Russia over the relocation of a Soviet-era monument in Tallinn'', Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective Cooperative Cyber Defence Centre of Excellence

[99] ''Stuxnet is a malicious computer worm, first uncovered in 2010, thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran. Although neither country has openly admitted responsibility, the worm is widely understood to be a cyberweapon built jointly by the United States and Israel.'', The Secret History of the Push to Strike Iran, The New York Times Magazine, 2019

[100] Tallinn Manual on the International Law Applicable to Cyber Operations: Principle of Lotus Case at 18.

[101] Gary Brown, The Customary International Law of Cyberspace, 2012

[102] Tallinn Manual on the International Law Applicable to Cyber Operations

[103] White House Cyber Strategy

[104] Security Studies: An Introduction, Paul D. Williams and Matt McDonald – Cybersecurity, Rhea Siers

[105] ''Critical infrastructure encompasses those systems and assets so vital to a country that interruption or destruction would have a debilitating impact on national security, economic security, and/or national public health, safety or collective morale. Critical infrastructure protection entails all the activities, including prevention/mitigation, preparedness, response and recovery, directed at enhancing the resilience of people, systems and physical infrastructure associated with the operations of those critical infrastructure sectors and their provision of essential goods and services. Examples of critical infrastructure sectors are: Banking & Finance, Chemical & Hazardous Materials, Defense Industrial Base, Emergency Services, Energy, Food & Agriculture, Information Technology, Postal & Shipping, Public Health and Healthcare, Telecommunications, Transportation, Water'', US Department of State Archive

[106] Tallinn Manual on the International Law Applicable to Cyber Operations

[107] Paul D. Williams and Matt McDonald, Security Studies: An Introduction, (Rhea Siers, Cybersecurity)

practices' guide, it does not represent 'progressive development of the law'. Tallinn Manual 2.0 is intended as an objective restatement of the *lex lata.*''[108] It covers a full spectrum of international law applicable to cyber operations ranging from peacetime legal regimes to the law of armed conflict, covering a wide array of international law principles and regimes that regulate events in cyberspace.[109] It focuses on fields such as the principle of sovereignty, various bases for the exercise of jurisdiction, the law of state responsibility and numerous regimes of international law like human rights law, air and space law, the law of the sea, and diplomatic and consular law.[110]

However, the manual, with its 154 rules, has unearthed the difficulty of a clear evaluation of norms. For example, rule 32 states that ''peacetime cyber espionage by States does not per se violate international law''. However, Michael Schmitt, a leading American international law scholar in international humanitarian law and use of force, argues that ''the method by which cyber espionage is carried out may violate principles of international law''. Indeed, consensus on different matters was hard to find; for example, the manual states that ''its participants were incapable of achieving consensus as to whether remote cyber espionage reaching a particular threshold of severity violates international law''.[111] The Tallinn's experiences exemplify the difficult but possible connection between legal norms, technology and different ethical calibres; international law reminds us how difficult may result to bind states under common practices. In such a reality, shifting states' operations from physical to digital and cyber space, may complicate things because of different variables such as the attribution conundrum and an unfounded search on a concrete and binding set of norms governing the cyberspace. However, it seems like a share of states are moving in the right direction through efforts such as the Paris Call for Trust and Security in Cyberspace, through the adoption of customized rules assessed at the bilateral level (e.g. China-Russia cybersecurity agreement), regional level (African Union Convention on Cyber Security and Personal Data Protection) and globally (Digital Geneva Convention)[112] – demonstrating how decisive is states' behaviour.

[108] Introduction to the Tallinn Manual 2.0
[109] CCDCOR, Tallinn Manual 2.0 https://ccdcoe.org/research/tallinn-manual/
[110] Ibid.
[111] Michael Schmitt n.d: 170
[112] Council on Foreign Relations – Net Politics and Digital and Cyberspace Policy Program

2.3. Theoretical Framework: Security Dilemma in the Cyber Age

The emerging cyber security field exhibits a resurgence of realist-influenced perspectives with a focus on security and competition in explaining international cyber politics.[113] Neorealism, a broad theory of international relations, describes the international system being anarchic in nature and pursued by powers' competition by states. The assumption of not having a global government, or at least an efficient global governance, makes the international system a world in which states must provide security by themselves. Most of the time, such a feeling of mistrust does not develop a genuine diplomatic channel as it is for Sino-Chinese relations.

The low degree of cooperation, coordinated with systematic divergent interests, ensures what is called in the neorealist language as the security dilemma. The term was first used in 1951 by John Herz in his work ''Political Realism and Political Idealism''. The dilemma originates from the condition in which two states might choose to go to war due to the sense of uncertainty towards the other state's intention, rather than of a real conflict. According to Robert Jervis, the scholar incorporating the condition of security dilemma within the neorealist framework, the dilemma is the condition in which ''many of the means by which a state tries to increase its security decrease the security of the others''.[114] The neorealist scholar Chrarles L. Glaser says that the security dilemma exists when "a state's efforts to increase its security would have the unintended effect of reducing its adversary's security." However, as we mentioned in the first side of his work, an important variable affecting the relations between states, including China and India, is the asymmetrical perception of threats. On this topic, the scholar Montgomery defines the security dilemma as "the situation where one state's attempts to increase its security appear threatening to others and provoke an unnecessary conflict."[115]

The security dilemma does not technically create conflicts, but instead modifies states' attitude in increasing defensive and offensive capabilities to ensure safety from external threats. Arms racing, maintaining proficient militaries, diplomatic tensions and sometimes war is the output of ''the best defence is a good offence'' theory. However, as Charles Glaser argues, enhancing security and capabilities to seek security, may project external and internal threats: the first, projection of threat to other states, and the latter projects internally within the state by heavy financial resources which could be used for other purposes, such as inclusive economic reforms.[116] The degree of the dilemma is highly influenced by military technology[117]; for example, even the augmentation of defensive technologies (e.g. missile defence systems) can throw off the balance of relative security between states.[118] Such an increase in the degree of security dilemma, is highly fuelled by the asymmetrical perceptions of threats.

According to the neorealist school of thought, the condition of security dilemma can be found too in the emerging theatre of cyberspace. Security dilemma in the cyber age, and in the cyberspace, is a condition which is also linked to different variables of cybersecurity. For example, the attribution conundrum is an important issue framed within a conflict: when the ability to identify the source of the attack is low, the degree of anarchy in the system can increase. Verifiability, which is the ability to confirm compliance to international agreement, is also one of those factors destabilizing the cyber world. An important grey area marking the cyber security dilemma is cyber espionage which is a category of cyber operations which seek to spy other states for political, economic, and military purposes, to gain information. What is important to understand is that cyber espionage is part or a component of cyber warfare but does not comply with the definition of cyberwarfare. It is not an act of war, but according to national sensibility, it may receive typical wartime attentions.

[113] Anthony Craig and Brandon Valeriano, Realism and Cyber Conflict: Security in the Digital Age, E-International Relations, 2018
[114] Jervis, "Cooperation Under the Security Dilemma," p. 160.
[115] Montgomery, "Breaking Out of the Security Dilemma," p. 151.
[116] Charles Glaser, "The Security Dilemma Revisited," World Politics, Vol. 50, No. 1 (October 1997), pp. 174-175.
[117] Robert Jervis, "Cooperation Under the Security Dilemma," World Politics, Vol. 30, No. 2 (January 1978), p. 194; Charles Glaser, "Realists as Optimists: Cooperation as Self-Help," International Security, Vol. 19, No. 3 (Winter 1994/1995), p. 62.
[118] Ken Booth and Nicholas Wheeler, The Security Dilemma: Fear, Cooperation and Trust in World Politics (New York: Palgrave, 2008), p. 51.

For such a reason, cybersecurity became quite linked for what concerns national security, becoming the defensive side of the cyberwarfare (for example, digital infrastructures' – civilian and military – security.[119] R. Clarke states that ''nation-states are preparing for, and have already engaged in, cyberwarfare.''[120]An example close to European attention occurred with Russians' Distributed denial-of-service[121] (DDOS) attacks launched to the Georgian government during the 2008 Russo-Georgian War; and even though the Russian Federation stated that the cyberoperations were led by cybercriminals many experts and scholars managed to trace the origins of the attacks from the Russian intelligence community.[122] '' The attackers in the Georgian incidents "showed considerable restraint"; potential and more severe consequences could have been triggered from financial costs[123] linked to the servers of a national stock exchange (e.g. 2009 DDOS attacks to New York stock exchange).

The second chapter encompasses the concept of cyberspace, which is playing a major role in modern international states relations. It gave several definitions of cyberspace, to have an extensive view of what is cyberspace and what are its implications on global politics. The section also analysed the concept of cyber power, attribution conundrum and other vulnerabilities states may face in cyber challenges. To face vulnerabilities of the cyber domain, it mentioned the variety of cyber opeations, and particularly in the second paragraph the complex governance and establishment of norms involving the cyberspace in states relations. Right after, it focuses on the the concept of security dilemma, being triggered by the modern challenges of a digital and cyber world, through a realist-influenced perspectives, in order to prepare the ground for the following chapter concerning Sino-Indian relations influenced by the cyberspace.

[119] Theohary, "Information Operations, Cyberwarfare, and Cybersecurity, pp. 20-22.
[120] Clarke and Knake, Cyber War, pp. 30-31.
[121] N. 75 definition
[122] Clarke and Knake, Cyber War, pp. 17-20.
[123] Telis Demos, "Cyber- Attack Raises SEC Questions," Financial Times, February 9, 2011.

3. Sino-Indian Cyber Confrontation

This chapter will discuss specifically the confrontation going on between India and China on cyberspace, to understand the possible consequences and implications on their relations. The relationship has degenerated for the above discussed reasons, especially after the 2020 skirmishes at the border. However, in cyberspace, these traditional boundaries disappear, reconnaissance is conducted by people around the world and planning is done by cells of combatants who never meet.[124]

Cyber modern challenges in international relations can be framed within Sino-Indian relations. Maharastra Cyber, the Indian states' police cyber wing, have reported around 40,000 cases of cyberoperations traced in China (Chengdu, the capital city of China's Sichuan province) in only five days, including phishing[125] attempts and security audits of the Indian IT system. The attacks are mainly diverging in different sectors of India's ''system-country'', including infrastructures, information and banking.[126] The cybersecurity firm Cyfirma, a leading firm in decoding threats and implementing cybersecurity strategies defending IT infrastructure, OT (operational technology) and applications' organizations, have traced the attacks linked with two Chinese hacking groups.[127] The firm has warned all Indian ministries, media houses and firms about the possible campaign of cyber-attacks. The two groups, Gothic Panda and Stone Panda, are known for a direct affiliation to People's Liberation Army (PLA), the armed forces of the People's Republic of China and founding/ruling political party Chinese Communist Party (CCP). The DDOS attacks ruptured Indian's cyber network while the Internet Protocol Hijack tried to divert the course of traffic through China for surveillance motivation.[128] In the security dilemma condition influencing the balances of the Sino-Indian relations, can such types of operations escalate in military offensive attitudes, like it has happened in the Galwan Valley Clash?

The recent border clashes and skirmishes between India and China, are the product of the historical complicated dispute going on between the two giants. Another product which may be fuelling the increasement in perception of threats between the two states is the different cyber power projection. Indeed, cyber operations, as we have seen, are not clearly labelled as an act of war, but result as a hybrid and multi-dimensional offensive practice. Such operations can have important effects over disrupting missile launches to breaking nuclear deterrence, influencing narratives.[129] Why different cyber power projections? Mainly due to different cyber vulnerabilities given by each state, being different, asymmetrical, and strongly linked with domestic political features. For example, the rigid-socio political hierarchies of the Chinese state may suffer from information warfare[130][131]. While India's vulnerability may be linked to the huge growth of cyber-espionage attacks received. The main problem of such an asymmetrical security dilemma is that, unlike nuclear deterrence, there is no science available to deduce thresholds framed in a possible cyber operations' escalation scenario.

In the early months of 2020, the relationship between China and India has worsened because of several different factors: critics over the Corona Virus spread, Indian's boycotting of Chinese consumption goods and the border skirmishes. A possible escalation may lead China to take advantages of its cyber and organizational capabilities, which will be discussed later. Indeed, an important example, is the phishing cyber activity launched from the Chinese territory over the State Bank of India (SBI), the largest public sector bank

[124] Cyber Warfare, 2nd Edition, O'Reilly

[125] Ramzan, Zulfikar, ''Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication'' , Phishing attacks and countermeasures

[126] NDTV – Maharashtra Cyber police report

[127] TheHindi Business Line – LiveMint Report

[128] E Hacking News: Gothic Panda and Stone Panda: Chinese Hackers that Launched Mass Cyber Attacks on Indian Companies

[129] Pukhraj Singh, HindustanTimes

[130] Information Warfare in its broadest sense is a struggle over the information and communications process, a struggle that began with the advent of human communication and conflict. Over the past few decades, the rapid rise in information and communication technologies and their increasing prevalence in our society has revolutionized the communications process and with it the significance and implications of information warfare. Information warfare is the application of destructive force on a large scale against information assets and systems, against the computers and networks that support the four critical infrastructures (the power grid, communications, financial, and transportation). However, protecting against computer intrusion even on a smaller scale is in the national security interests of the country and is important in the current discussion about information warfare.

[131] Ibid.

in the Indian Sub-Continent.[132] Cyber infrastructure is very important for the regional economy and security, but may turn quickly into a stage of competition and potential conflict, especially because of cyber espionage. As we have mentioned before, the cyber domain can be framed in terms of competition, rather than war. Lack of agreement of norms, and potential to mistake cyber espionage for military action, may produce a cyber competition increasing risks of miscalculation, conflict and escalation during times of interstate tension[133], like it is happening at the moment between China and India. The asymmetrical danger of threat linked to cyberspace is the close connection it gives the states, connections providing new capabilities and assets to share, to own, to influence and to attack. The competition over cyberspace is not only linked to military capabilities, rather includes a stage to share, to own, to influence and to control the structures and markets of global finance and business, and therefore, regional power and leadership.

Referring to Sino-Indian relations, cyber competition and also traditional conflicts are framed within the Asian dimension: ''in this region it encompasses planning for military competition and asymmetric warfare, engagement in economic espionage to gain long-term economic and trade advantages, as well as a new kind of transnational mass political action. '' [134] One one side, ''Chinese leadership is building the most extensive governance regime for cyberspace and information and communications technology (ICT) of any country in the world. Recognizing that technology has advanced more quickly than the government's ability to control it, Beijing has moved to rapidly to construct a policy and regulatory framework spanning cybersecurity, the digital economy, and online media content—all under one mantel.''[135] Also, China gained asymmetric military advantages by using the cyberspace to gain military and economic advantages. At the same time, India, being one of those Asian states exploring military cyber capabilities, is trying to keep up with its competitor.

Cyber competition between the States is characterised by a grey area drawing a complicated boundary between cybercrime, cyber espionage and cyber-attacks. The intricate cyber security dilemma fuels the condition of possible threats of cyberwarfare, while the risk of cyber espionage and cybercrime is under-appreciated.[136] Such a condition deeply contributes in making cyber espionage and cyber space in Asia, and especially between the two Asian giants, a new sources of instability. The use of internet managed to reduce the risks and costs of conducting espionage. Such a condition is especially true for what concerns economic espionage, an activity quite linked to Chinese' cyber foreign policy: stealing technology, researches, confidential business information and intellectual property.[137] The consequences of cyber espionage, and in general cybercrimes, as we mentioned before, is deeply characterised by what we mentioned as the attribution conundrum. On such a concern, such crimes overlap in cyberspace due to the difficult attribution of responsibilities due to the use of proxies – cybercriminals acting on behalf of national governments.

The use of proxies is typical of Chinese traditional foreign policy[138]; in the cyber attacks led by Gothic and Stone Panda after the skirmishes at the borders, it may turn true also for cyber strategies. State-backed cyberattacks have become a common weapon of retaliation for powerful countries that do not want to get into physical wars.[139] On such a manner, two details are important: first, the Article 7 of the 2017's Act on the Chinese intelligence apparatus, which declares that ''any organization, or private citizen must support, assist and cooperate with Chinese intelligence operations in accordance with the law and maintain the latter a secret''. What it really means, is that also Chinese firms across the world must collaborate with the Chinese intelligence's apparatus. Chinese cyber espionage strategy links official programs and activities led by individuals and companies. This ''thousand grains of sand'' strategy encapsulate also businessmen, researchers and scholars to collect information abroad.[140] The second fact, is the Chinese' incredible growth

[132] Naveem Goud, Cybersecurity Insiders
[133] James Lewis: Cyber Competition and Conflict in Indo-Pacific Asia, Lowy Institute MacArthur Security Project
[134] Ibid.
[135] Samm Sacks, China's Emerging Cyber Governance System, Center for International and Strategic Studies
[136] Ibid.
[137] Survey of Chinese-linked Espionage in the United States Since 2000, Center for International and Strategic Studies
[138] Andrew Mumford, Cyber-Warfare as a Mode of Proxy War, Proxy Warfare and the Future of Conflict, 2013
[139] Abhijit Ahaskar, India now faces threat of Chinese cyberattacks, MINT, 2020
[140] Northrop Grumman Corporation, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,

in the markets of technology, mobile service, internet of things and robotics. Such facts strictly scare other states like India and United States of America. From 2017 to 2019, numerous firms have conducted researches on cyber operations traced from Chinese territory. What has emerged, according to FireEye, a public traded cybersecurity company based in California, is that cyber operations coming from firms' intelligence operations, are funded directly from the national government.[141]

Such facts highlight how cyberspace and technology are increasingly becoming factors of destabilization in large geopolitical disputations. What is also underlined in modern Sino-Indian relations is on one hand China featured by an aggressive cyber foreign policy, while on the other hand India under a domestic pressure to respond to China, especially after the border clashes. Indeed, ''India is under tremendous pressure and you heard Prime Minister Narendra Modi's comments about these casualties will not go in vain.''[142] Yuan Jingdong, an associate professor in Asia-Pacific security at the University of Sidney states that both sides recognize the possible risks of an escalation to a larger military confrontation and ''given that both are nuclear armed states, the risk could not be more severe.''[143] Nevertheless, meetings have been conducted after the Galwan Valley clash between the Government of the Republic of India and the Government of the People's Republic of China to ensure Confidence-Building Measures in the military field along the Line of Actual Control in the India-China border areas.[144] Therefore, according to many analysts, the chances of a war between India and China are quite low. ''State-backed cyberattacks have become a common weapon of retaliation for powerful countries that do not want to get into physical wars.''[145] What outlines the next paragraphs is Sino-Indian evolution of dispute in the following years, due to its low possibility of a real conflict, by looking at the cyber escalation happening in such a moment of dispute. This will be framed within cyberwarfare through the analysis of the respcetive Chinese and Indian cyber capabilities and vulnerabilities.

[141] Kelli Vanderlee, Report: FireEye Cyber Security Analyst, 18/11/19
[142] Jingdong Yuan, University of Sydney, CNBC's Squawk Box Asia
[143] Ibid.
[144] Filippo Santelli, Patto tra India e Cina per ridurre le tensioni sul confine himalayano: "Entrambi vogliamo la pace", Repubblica, 2020 / India, China defence ministers meet amid rising border tensions, Al-Jazeera, 2020
[145] Abhijit Ahaskar, India now faces threat of Chinese cyberattacks, MINT, 2020

3.1. China: belligerent cyber doctrine

This section of the thesis discusses China's cyber capabilities, state organization in regards of cyber strategies and non-state cyber attacks conducted from Chinese territory. Before going into the chapter, it is important to remember that in the recent years, China grew exponentially becoming a global power. A fundamental aspect, linked to cyberspace and to cyber capabilities, is that China, according to different sources, structured such growth by relying on an unsustainable formula of debt, subsidies, cronyism and, very important, intellectual property theft.[146] Media have been reporting numerous time about China violating numerous times the illicit access to proprietary information such as research and development data.[147] Chinese access to sensitive information has a wide syllabus: in 2009 China seemed to have stolen plans of U.S. fighter jet the F-35[148]; China manged to hack several times Google, Intel, Adobe and the RSA's Secure ID authentication technology, targeting Lockheed Martin, Northrop Grumman and L-3 Communications[149]; on the business and financial dimension, China accessed and hacked Morgan Stanley, the U.S. Chamber of Commerce[150] and numerous Indian banks during the Covid-19 lockdown; on the media dimension, cyberattacks originated from China targeted the New York Times, Wall Street Journal, Washington Post[151]; from a critical infrastructure dimension, the United States Department of Homeland Security reported in 2013 that gas pipeline companies were hacked[152] for possible sabotage from China.[153]

However, as the first part of the thesis lays, cyber conflict or competition most of the time mirrors traditional interstate and intrastate conflicts – and Sino-Indian relations seem to be the new case. Cyberspace and its analytical environment give states a degree of deniability, while keeping the military, intelligence, and tactical level into secrecy. In such a scenario, China, acting as the elephant in the room, is at the moment the noisiest threat actor in cyberspace due to: huge population, an structured expanding economy globally and a lack of good mitigation strategies on the part of the target.[154] China is home to bureaucratic hacker groups being the cyber threat actor, and acting on behalf of the State. An important example of Chinese non-state actor, but working as a state actor, is the ''Comment Crew''[155]: this group is behind a variety of global attacks, such as the Operation Beebus targeting the U.S. aerospace and defence industries.[156] The interesting fact is that, even though China has been considered one of the main actor of cyberspace, the Chinese Communist Party keeps maintaining a cool-heated perspective[157], disapproving its significant role in possible cyberwarfare – fuelling the complexity of the attribution conundrum. However, this remains part of ensuring cyber power.

A state's cyber power comprehensively refers to the capability the State must act and exert influence over cyber issues.[158] Such a power is structurally composed of different dimensions. Internet and information technology (IT) capabilities refer to the degree of the state's technological research, development and innovation capabilities, projecting it to the industry sector; IT industry capabilities, where China possesses the leader industry and corporate giant Huawei producing telecommunications equipment globally; the Internet market capabilities referring to the size and scale of the domestic internet infrastructure, number of internet and computers users, which is deeply observed for surveillance and domestic security; the influence of the internet culture, which is strongly nationalised in China; and the state's ability and capability to defend national and military IT infrastructures from attacks linked to its network deterrence and offensive ability, such as subtracting secrets and preventing national secrets to be taken away. Precisely with regard to Huawei,

[146] The Economist: Xi's new economy, 15/08/2020
[147] Kenneth Geers, Darien Kindlund, World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks, 2014
[148] Gorman, S., Cole, A. & Dreazen, Y. , "Computer Spies Breach Fighter-Jet Project," The Wall Street Journal, 2009
[149] Gross, M.J. , "Enter the Cyber-dragon," Vanity Fair, 2011
[150] Gorman, S. , China Hackers Hit U.S. Chamber," Wall Street Journal, 20133
[151] Perlroth, N. , "Washington Post Joins List of News Media Hacked by the Chinese," and "Wall Street Journal Announces That It, Too, Was Hacked by the Chinese," The New York Times, 2013
[152] Gertz, B. , "Dam! Sensitive Army database of U.S. dams compromised; Chinese hackers suspected," The Washington Times
[153] Clayton, M. , 2013 "Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage," The Christian Science Monitor
[154] Ibid.
[155] Sanger, D., Barboza, D. & Perlroth, N. , "Chinese Army Unit is seen as tied to Hacking against U.S." The New York Times, 2013
[156] Pidathala, V., Kindlund, D. & Haq, T. , "Operation Beebus," FireEye, 2013
[157] Li Zhang, A Chinese perspective on cyber war, International Review of the Red Cross, 2012
[158] Tim Jordan, Cyberpower: The Culture and Politics of Cyberspace and the Internet, Routledge, London/New York, 1999

diplomats have warned India to prevent Huawei's services to build a 5G network[159] into the Indian market. Assuming an hypothetical worst case scenario, where a state, such as PRC, has an interest in doing any damage, the possibility of interrupting or sabotaging the telecommunications network increases.[160] Such possible threats, result in the last decade's states reinforcements of the cyber security apparatus, demonstrating how national security must chase technology. Huawei's links to the Chinese Communist Party is one of those factors making the attribution conundrum an important variable of security dilemma. The logic of banning Huawei and its services, in India, but globally speaking, follows the one of disengagement and containment of China.

An important factor of cyberspace destabilizing Asian relations is the use of domestic internet in advertising nationalist sentiment that may turn in increasing the risk of conflict, as governments feel, for electoral purposes, ''the need to respond to domestic political pressure generated by internet activities.''[161] Such things may have unpredictable consequences for regional stability. For example, a series of fake news spread in the Indian internet and social media[162], fuelling national hate against Chinese for what concerns the skirmishes at the border. This culminated in national boycott of Chinese goods in India, destabilizing bilateral trade and relations. Another consequence was the Indian's move, part of a tit-for-tat retaliation, in banning around sixty Chinese mobile apps (including TikTok and WeChat) for national security concerns, according to the Indian Prime Minister Modhi. Chinese telecommunications and social network companies have been keeping an eye on India's giant market. According to the Indian Minister of Electronics and Information Technology Ravi Shankar Prasad, ''the Chinese apps were stealing and surreptitiously transmitting users' data in an unauthorised manner to servers which have locations outside India''.[163] Such alert is strictly linked with what we have mentioned before, the Chinese National Intelligence Law holding that companies must collaborate for Chinese Intelligence activities; and cybersecurity analysts have previously warned about Chinese apps and telecom companies' possible risks.

According to the computer scientist Cristopher Ahlberg, chief executive of Recorded Future, a cybersecurity company in Massachusetts, certain attentions on the part of the Indian state are legitimate. ''India's concerns are not overblown, they are valid. China would not be above using these apps for large scale data collection, and it is easy under Chinese law to require companies' collaboration.''[164] ''Chinese mobile app firms and other tech firms are beholden to the Chinese Communist Party under Chinese law; and as extensions of the Chinese state, they pose a national security and sovereignty risk.''[165] This is the reason why in April 2020, Indian government passed legislation requiring government approval for any investments from Chinese entities. According to Nikhil Pahwa, the founder of MediaNama, an organization advocating for a free internet, ''techno-nationalism has been in vogue in India for a while; the government views Indian citizens' data as sovereign, and therefore fears a digital Chinese colonization, and therefore has avoided signing data sharing agreements in the past''.[166]

Nevertheless, being a global leader in the IT environment, it is important to note that China itself faced different internet threats. According to the annual report of the National Computer Network Emergency Response Technical Team Coordination Centre of China, national public networks and critical infrastructure have been attacked in 2012 from United States, Japan and South Korea. Indeed, according to a spokesman from China's Ministry of Defence, People's Liberation Army's military networks suffered around 80,000 attacks per month[167] in the first decade of the 21st century, targeting also Chinese financial institutions. Such

[159] ''In telecommunications, 5G is the fifth generation technology standard for cellular networks, which cellular phone companies began deploying worldwide in 2019, the planned successor to the 4G networks which provide connectivity to most current cellphones.'', de Looper Christian,"What is 5G? The next-generation network explained", 2010
[160] Report: Stefano Zanero, Computer Engineering, Politecnico di Milano, 2019
[161] Nigel Inkster, China in Cyberspace, Nationalism in Chinese cyberspace, Cambridge review of international affairs, 2010
[162] BBC Reality Check
[163] Monday Statement of Ravi Shankar Prasad
[164] The New York Times
[165] Brahma Chellaney, former adviser to India's National Security Council
[166] The New York Times
[167] Li Zhang, A Chinese perspective on cyber war, International Review of the Red Cross, 2012 - Available (only in Chinese) at: http://www.mod.gov.cn/affair/2012-03/29/content_4354898.htm

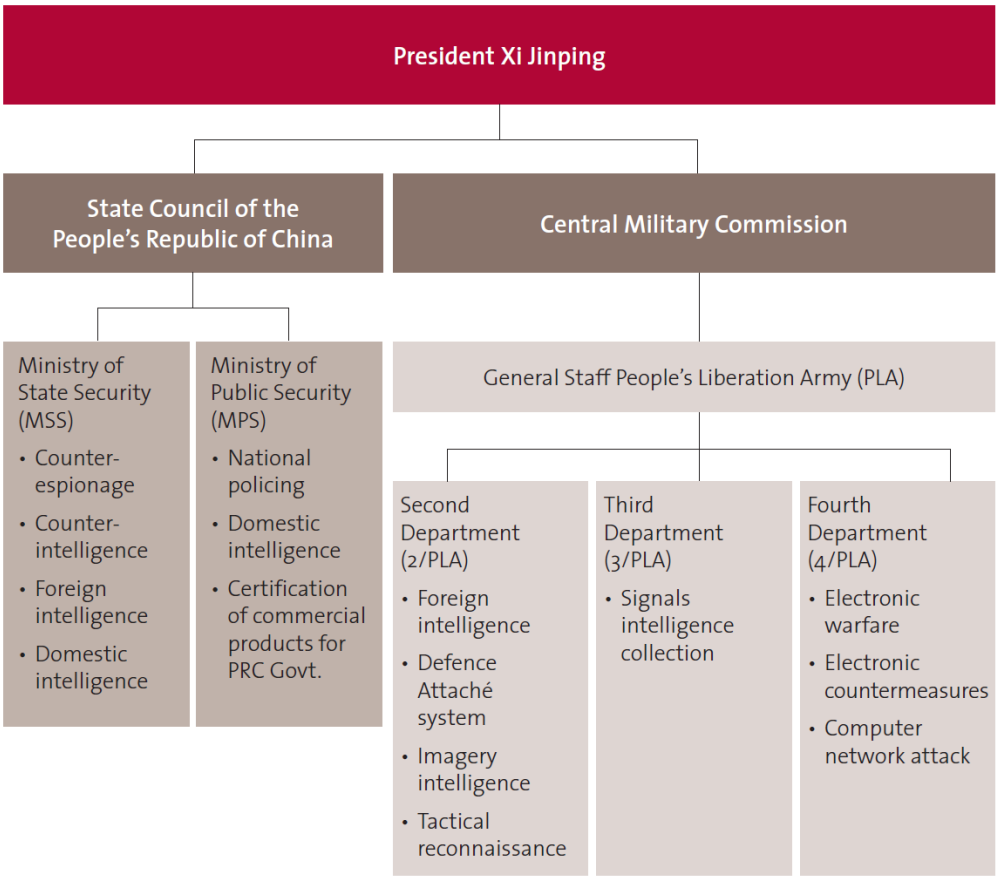
threat fuelled China's own sense of threat and insecurity in the cyberspace, creating the necessity for China to become a global power in cyberspace.

China's origins of asymmetrical technical capabilities is traced back to the Gulf War in 1990-91; indeed, according to Chinese military, the 90's have been marked as the 'the great transformation' of China adapting to the new theatre of cyberspace. The highest point of such a strategic update is to be found in the 1999 publication of Unrestricted Warfare[168][169], laying the foundations of Chinese strategies: taking advantage if weaknesses created by the adversary's superior conventional capabilities through cyber means.[170] Chinese cyber capabilities concerned the use of cyber capabilities in support of military operations and espionage.

In 2013, the People Liberation Army Lieutenant General Qi Jianguo confirmed such program at Chinese Communist Party Central Party School by stating Chinese' perspective: ''cybersecurity concerns national sovereignty as well as the security of economic and social operations, and it concerns the quality of human existence. The West's so called internet freedom is a type of cyber-hegemony; in the information era, seizing and maintaining superiority in cyberspace is more important than seizing command of sea and command of the air were in World War II''.[171] The 2015 Ministry of National Defense paper entitled "China's Military Strategy'', being the first official military document addressing cybersecurity, issued the target of "winning informationized local wars," and defined cyberspace as a "new pillar of economic and social development, and a new domain of national security.'' It continues with "China is confronted with grave security threats to its cyber infrastructure" as "international strategic competition in cyberspace has been turning increasingly fiercer, quite a few countries are developing their cyber military forces."[172]

Nigel Inkster, former director of operations and intelligence for the British Secret Intelligence Service and currently the Director of Transnational Threats and Political Risk at the International Institute for Strategic Studies, declares that Chinese intelligence does not follow a formal central mechanism for assessing and synthesizing intelligence reports for the central government.[173] The curious thing is that, unlike what it may seem, it is not usually typical of authoritarian systems. In fact, both military and civilian intelligence work through different analysis on provincial, regional and international level, with different layer influencing the final product.

[168] Unrestricted Warfare ('warfare beyond bounds') is a book on military strategy written in 1999 by two colonels in the People's Liberation Army. Its primary concern is how a nation such as People's Republic of China can defeat a technologically superior opponent through a variety of means. Rather than focusing on direct military confrontation, this book instead examines a variety of other means. Such means include using International Law (*see Lawfare*) and a variety of economic means to place one's opponent in a bad position and circumvent the need for direct military action.
[169] Tobias Feakin, Enter the Cyber Dragon Understanding Chinese intelligence agencies' cyber capabilities, ASPI Australian Strategic Policy Institute, 2013
[170] Richard A Clarke & Robert K Knake, Cyber War: the next threat to national security and what to do about it, Harper Collins, 2010, 47-51
[171] James Bellacqua & Daniel Hartnett, Article by LTG Qi Jianguo on international security affairs, 2013
[172] Lyu jinghua, What Are China's Cyber Capabilities and Intentions? Carnegie Endowment for International Peace, 2019
[173] Nigel Inkster, ''Chinese Intelligence in the Cyber Age'', Survival, 2013



174

On the civilian level, the organizational structure is composed by the Ministry of State Security (MSS) and Ministry of Public Security (MPS). To obtain the mentioned functions in the chart, both ministries endorsed joint researches such as the project between Zhongxing Telecommunications Corporation and Chongqing University of Posts and Telecommunication[175], creating a melting pot between Chinese military, intelligence activities and the corporate sector of China.[176] On the military level, the structure is composed by the Second Department of the People Liberation Army, the Third Department and the Fourth Department.

According to Larry Wortzel, a Commissioner of the US-China Economic and Security Review Commission[177], network operations conducted by the Chinese State can be traced in two main typologies of operations. The first one consists in exerting domestic control against political dissidents communicating on the web (and sources providing information to international media) by controlling the cyber-domain. The second type of cyber operations refers to intelligence operations to gather economic, political, military or technology intelligence and information in order to foster economic development, stronger negotiating posture, market access, to develop and field weapons system and to save time in technology research and development.[178] However, as we have already mentioned earlier, Chinese cyber-activities are not only conducted by the intelligence agencies: it comprises different communities of hackers, patriotic 'netizens' (citizens attacking for Chinese state's interests and ideals). Such groups can operate in parallel due to their provision of possible deniability of the State and the volume of information they can collect.

[174] Tobias Feakin, Enter the Cyber Dragon Understanding Chinese intelligence agencies' cyber capabilities, ASPI Australian Strategic Policy Institute, 2013
[175] Byran Krekel, Occupying the information high ground: Chinese capabilities for computer network operations and cyber espionage, 2012
[176] Desmond Ball, 'China's cyber warfare capabilities', Security Challenge, 2011
[177] ''The United States-China Economic and Security Review Commission (informally, the US-China Commission) is a congressional commission of the United States government. Created through a congressional mandate in October 2000, it is responsible for monitoring and investigating national security and trade issues between the United States and People's Republic of China'', H.R.5408 - Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001
[178] Larry M. Wortzel, China's approach to cyber operations: implications for the United States, testimony before the Committee on Foreign Affairs, 2010

It is fundamental to understand that cyber-domain became the new theatre for China to project its most important national security objectives and measures: sustaining regime survival, defending national sovereignty and territorial integrity, and establishing China as a regional and national power.[179] China has developed the cyberspace as the ideal tool to reach such long-term goals, being an economical mean to engage multiple and different targets straight away. On such a goal, Chinese cyber operations campaigns aim in strengthening China's core, more than diminishing the enemy. ''Focusing solely on the United States, suspected Chinese cyber espionage actors have targeted a variety of industries such as space[180], infrastructure[181], energy[182], nuclear power[183], technology[184], clean energy[185], biotechnology[186] and healthcare[187], in order to fuel national economic industry growth.''[188] Such industrial policies for the growth of strategic emerging industries encompasses sectors such as new energy, energy conservation and environmental protection, biotechnology, new materials, new IT (broadband networks, Internet security infrastructure, network convergence), high-end equipment manufacturing (aerospace and telecom equipment) and clean energy vehicles.[189] On a regional dimension, such an aggressive competition could address possible regional competitors, in the event of escalation. People Liberation Army managed to ensure doctrinal and organizational reforms, to fuel on the ability of the services to fight jointly, along with cyber support, [190] to meet its strategic aims. Chinese modern capabilities, therefore, also challenge Indian decisionmakers on matters they have not previously decided to confront, such as Chinese strategic influence in South Asia and the Indian Ocean via a large program of security assistance, such as the construction of infrastructure like ports (e.g. Belt and Road Initiative).

''At the very beginning of the cyber age (before the term "cyberspace" even existed) it was evident that reliable technology was going to be crucial in military operations, that Information and Communications Technologies (ICT) networks were inherently unsecure as they may be hacked or malfunction, and that the distinction between what is "cyber" and what is "real" was going to be increasingly difficult to grasp.''[191] This section analyzed Chinese cyber capabilities to our days, to get an idea of how China understood the implications of the cyber age. Through its Sun Tzu's doctrine of ''subduing the enemy without fighting'', Chinese cyber policy structured non-violent but still offensive activities, in peacetime and during hostilities.[192] Information operations (e.g. intelligence operations, command and control operations to disrupt enemy information flow, electronic warfare by seizing the electromagnetic initiative) have been previously labelled as "acupuncture warfare'' in 1997 by the PLA National Defence University publication entitled "On Commanding Warfighting under High-Tech Conditions".[193] Such doctrine has also been labelled as "paralysis warfare"[194] due to its ability to paralyse the enemy by attacking the weak link of his command, control and communication. Therefore, through its "active defence" approach, China is to be considered ''one of the world's greatest cyber power."[195]

[179] Colonel Jayson M. Spade, Information as Power: China's Cyber Power and America's National Security, 2014 Quadrennial Defence Review
[180] John Walcott, "Chinese Espionage Campaign Targets U.S. Space Technology," *Bloomberg*, 18 April 2012
[181] Tom Simmonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant," *Technology Review*, 2 August 2013
[182] Ibid.
[183] Jennifer Liberto, "New Chinese Hacker Group Targets Governments, Nuclear Facilities," *CNN Money*, 4 June 2013
[184] Stew Magnuson, "Stopping the Chinese Hacking Onslaught," *NDIA*, July 2012,
[185] Susan D. Hall, "Chinese Hackers Targeting the Healthcare Industry," *FierceHealthIT*, 20 March 2013.
[186] Nick Paul Taylor, "Chinese Trial Data Hackers Reportedly Active Again," *FierceBioTechIT*, 27 May 2013,
[187] Susan D. Hall, "Chinese Hackers Targeting the Healthcare Industry."
[188] Emilio Iasiello, China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities, ASPI Africa and Francophonie – 4th Quarter 2017
[189] "China's 12th Five-Year Plan: Overview," (Beijing, China: KPMG, March 2011)
[190] [190] Arzan Tarapore, Carnegie India: The Army in Indian Military Strategy: Rethink Doctrine or Risk Irrelevance, August 10, 2020
[191] Fabio Rugge, Cyberspace and the Armed Forces, ISPI, 2018
[192] Office of the Secretary of Defense, *Military and Security Developments*
[193] Barbara Opall-Rome, "PLA Pursues Acupuncture Warfare", Defense News, Springfield, Virginia (USA), March 1, 1999
[194] "China Developing 'Paralysis Warfare", Taipei Times, October 10, 2003
[195] Robert Lemos, Is China the World's Greatest Cyber Power?, Dark Reading, 2020

3.2. India: lack of a strategic evaluation

This section outlines Indian cyber capabilities, dealing with the national state apparatus dealing with cyber challenges, especially in the light of the extraordinary modernization of China's military capabilities which has slowly begun to threaten India not only on land border, but also on new domains like the cyberspace. The modernization of military technologies is drastically reshaping the features of modern conflicts, demanding for evaluations and strategic review processes of national military's organization, training and doctrines. The military should no longer presume the land domain to be the decisive arena of conflict, as it should focus on different domains such as space and cyberspace (independently). Actions in each domain should support and enable forces in another domain, seeking moments of advantage that they can quickly exploit to defeat the enemy's systems.[196] Especially with current fragile geopolitical environment due to Sino-Indian dispute, the digital world has opened new fronts of confrontation, shifting from features such as army and equipment to electrons and malware ready to cause damage. Indeed, most of economies are nowadays vulnerable to cyberspace, such as in the energy sector, telecommunications and military installations. What is important to consider is the fact that '' while disengagement and de-escalation are possible through dialogue and diplomacy in the physical world, the imponderables in a Digital World are very different. Cyber Wars tend to be open ended and potentially endless. Nothing is visible to the naked eye, yet havoc is wreaked in our conscious presence. The impact can be so gigantic that it could cripple Countries.''[197] In a worst-case scenario, the above-mentioned implications, may turn true for what concerns Sino-Indian relations, on a long-term view.[198]

''China economic growth and its military capabilities stemming out of the economic propensity have propelled it towards expanding its strategies in the realm of cyber warfare. As the age of information based warfare dawns, cyber war presumably is all likely to become a key component and feature of any future conflict within Asia.''[199] India therefore must develop counter capabilities in order to ensure its national and citizens' security. Indeed, in recent years, several government and non-reports have debated about cyber intrusions of Chinese activities within India. As we have mentioned above, weighty Indian targets have included ministries, embassies, industrial houses, defence establishments, apart from sensitive government offices.[200] Nevertheless, Indian cyber intrusion investigation reports are not accessible on open domain, while foreign investigators do exist, wherein India is mentioned as one of the victims, with intrusions attributed to China.[201]

The 2010 Joint Report ''Shadows in the Cloud: Investigating Cyber Espionage'' published by the Information Warfare Monitor and Shadowserver Foundation, reported at the time about computer networks of two of India's leading defense magazines (India Strategic and Force), have been hit by Chinese hackers (information about contact details of subscribers and conference participants). During the course of investigation, it was found that beleaguered academic targets included exfiltrated papers on subjects such as the containment of the People's Republic of China, Chinese military exports, Chinese foreign policy on Taiwan and Sino-Indian relations.[202] According to the scholar Monika Chansoria, '' the material prominently signifies that the hackers successfully managed to get their hands on the issues that constitute to be of prime importance to the PRC.''[203] The 2010 report included other attacks such as: attacks against computer networks of the National Security Council Secretariat (NSCS) of India and the Joint Intelligence Committee which is responsible for national security strategic planning; 14 exfiltrated papers included two documents labelled as "secret"; cyber attacks against computer networks at the Indian Embassies in Kabul and Moscow and against the Consulate General of India in Dubai and the High Commission of India in Abuja, Nigeria. About hundred documents, including encrypted diplomatic correspondence, documents marked as

[196] U.S. Army, The U.S. Army in Multi-domain Operations 2028, TRADOC pamphlet no. 525-3-1, December 6, 2018
[197] Manoj Chugh, Guns, Roses and Cyberwarfare, Express Computer, 2020
[198] Ibid.
[199] Dr Monika Chansoria, China's Cyber Wars *India Strategic* also hacked, Centre for Land Warfare Studies (CLAWS), 2010
[200] Ibid.
[201] Brigadier Saurabh Tewari, The United Service Institution of India: China's Cyber Warfare Capabilities, 2019
[202] Dr Monika Chansoria, China's Cyber Wars *India Strategic* also hacked, Centre for Land Warfare Studies (CLAWS), 2010
[203] Ibid.

‘’restricted’’ and ‘’confidential’’, have been exfiltrated by the attackers. One of the document on “Project Shakti”—the Indian Army’s combat command and control system for the artillery that apparently was targeted and later was recovered.[204] Earlier, in March 2009, former Indian Foreign Secretary and National Security Adviser at the time, Shiv Shankar Menon, admitted that ‘’there had been attempts at hacking into the computers of Indian embassies, in response to media reports of a vast cyber network controlled from China, that targeted governments and private computers in 103 countries, including those of the Indian embassy in Washington.’’[205]

In the last decade, cyber incidents against India have been registered on regular basis; such a fact has been endorsed by the former National Security Advisor (NSA) of India, Narayanan.[206] However, as we have mentioned earlier and above, international firms such as the ‘FireEye’ have reported too of China spying on Indian government and business for more than a decade without India being aware of it. [207] Brigadier Brigadier Saurabh Tewari mentioned a variety of different cybernetic operations traced from Chinese territory against different Indian sector: National Informatics Centre (NIC) servers breached (2009); Ministry of Home Affairs (MHA), Ministry of External Affairs (MEA) intruded (2012)[208]; Northern India Power grid crashed (2012)[209]; Defence Research and Development Organization (2013); Prime Minister’s Office (POMP) website hacked[210]; Bharat Sanchar Nigam Limited (BSNL) website hacked (2014)[211]; Indian Space Research Organisation (ISRO) webpage defaced (2015)[212]; an Indian Air Force Sukhoi 30 fighter aircraft was downed, purportedly by a cyber-attack from China (2013)[213]. Such a register of attacks highlights the necessity for India to understand its vulnerabilities and China’s strategies to undertake and understand possible and effective countermeasures. What is definitely not helping India in securing its digital domain are the following variables: lack of effective cyber security environment, lack of offensive capability, and the vast proliferation of Chinese computer and telecommunication hardware (resulting a vulnerability both on national security and within economic competition)., India became strongly dependent on automated data processing and vast computer networks, fuelling its vulnerabilities to such information warfare techniques occurring in the modern Sino-Indian relations.

Major national infrastructure like telecom, government agencies, financial institutions, railways, air traffic control, banks, stock exchanges and power grids may be the possible targets of an escalation beginning in cyberspace, originating a possible cyber Pearl Harbour. Therefore, an establishment of an inter-ministerial, inter-departmental, inter-Services, multi-agency approach to understand which shall be the strategy to develop effective countermeasures to avoid any possible cyber Pearl Harbour is fundamental, especially due to India’s approach towards electronic and cyber warfare being nowhere as evolved as that of China’s.[214] ‘’The Indian Army and India are yet to fully acknowledge the convergence between cyber warfare and electronic warfare, whether doctrinally, operationally or organizationally: a reason is the inadequate interaction between the Indian Army Training Command (ARTRAC), which is responsible for formulating and updating service doctrine, and all the technical entities, such as the Defense Intelligence Agency (DIA), the Corps of Signals, the Defense Information Assurance and Research Agency (DIARA), and the National Technical Reconnaissance Organization (NTRO).’’[215] However, Indian foreign intelligence and domestic security agencies, the Ministry of Home Affairs, the executive office of the National Security Advisor, and the military intelligence have departments that engage in cyber operations. Nevertheless, India lacks a functional information warfare service to be deployed for specific missions and military goals.[216]

[204] Dr Monika Chansoria, China’s Cyber Wars *India Strategic* also hacked, Centre for Land Warfare Studies (CLAWS), 2010
[205] Ibid.
[206] Sharma Deepak, 2011, China’s Cyber Warfare Capability and India’s Concerns, Institute for Defence Studies and Analyses, New Delhi, 2018
[207] https://entrackr.com/2017/12/fireeye-chinese-hackers-target-india-2018/, Accessed 22 Aug 2018
[208] http://www.indiandefencereview.com/spotlights/acupuncture-warfare-chinas-cyberwar-doctrine-and-implications-for-india/, 2018
[209] https://www.oneindia.com/2012/08/22/china-s-hand-in-india-s-power-blackout-1057676.html, 2018
[210] http://www.thehindu.com/news/national/drdo-website-hacked/article4051758.ece, 2018
[211]https://www.thehindubusinessline.com/info-tech/bsnl-site-hacked/article7386407.ece, 2018
[212] http://www.thehindu.com/news/national/isros-commercial-arm-antrix-website-hacked/article7413823.ece, Accessed 28 Sep 2018
[213] https://www.cybersecurity-insiders.com/china-cyber-attacks-indian-sukhoi-30-jet-fighters/, Accessed 13 Nov 2018
[214] Kartik Bommakanti, Strategic Studies Programme, Indian Army’s approach to electronic & cyber warfare is nowhere as evolved as China’s PLA, The Print, 2019
[215] Ibid.
[216] Ibid.

As a former officer stated: "in order to keep pace with evolutionary changes in tactical doctrine, improvements in army command and control are required. The rapidly changing combat environment will impose severe time pressures on the staff and the commander."[217] India's leader reputation in the global IT industry is somehow denied by the relatively little attention the Indian authorities had paid in introducing cyber technologies in the country's governance system, filling the lack of a prospective information based operations integrated with traditional land warfare military operations through an integrated commands system to combat cyber threats posed by hackers acting out of personal, economic, and political reasons.[218] Below, the chart illustrates the hierarchy[219] of cyber security bodies' working for the state of India. However, ''India has various organisations dealing with cyber issues, but such agencies do not integrate with each other and generally operate independently. There is a need to have a single policy level agency and a single execution level agency, which can coordinate at national level.''[220]

PM OFFICE/CABINET SECY (PMO/CAB SEC)	MINISTERY OF HOME AFFAIRS (MHA)	MINISTRY OF EXTERNAL AFFAIRS (MEA)	MINISTRY OF DEFENCE (MOD)	MINISTRY OF COMMON INFO TECHNOLOGY (MCIT)	NON GOVT ORGANIZATION (NGO)
National Security COuncil (NSC)	National Cyber Corrd Centre (NCCC)	Ambassadors & Ministers	Tri Service Cyber Commad	Department Of Information Technology (DIT)	Cyber Security And Anti Hacking Organisation (CSAHO)
National Technical Research Org (NTRO)	Directorate of Forensic Science (DFS)	Defence Attaches	Army (MI)	Department of Telecom (DoT)	Cyber Society of India (CySI)
National Critical Info Infrastructure Protection Centre (NCIIPC)	National Disaster Mgt Authority (NDMA)	Joint Secretary (IT)	Navy (NI)	Indian Computer Emergency Response Team CERT-IN	Centre of Excellence for Cyber Security Research & Development in India (CECSRDI)
Joint Intelligence	Central Forensic Science Lab (CFSLs)		Air Force (AFI)	Educational Research Network (ERNET)	Cyber Security of India (CSI)

PM OFFICE/CABINET SECY (PMO/CAB SEC)	MINISTERY OF HOME AFFAIRS (MHA)	MINISTRY OF EXTERNAL AFFAIRS (MEA)	MINISTRY OF DEFENCE (MOD)	MINISTRY OF COMMON INFO TECHNOLOGY (MCIT)	NON GOVT ORGANIZATION (NGO)
National Crisis Management Committee (NCMC)	Intelligence Bureau (IB)		Def Info Assurance & Research Agency (DIARA)	Informatics Center (NIC)	National Cyber Security of India (NCS)
Research & Analysis Wing (RAW)			Defence Intelligence Agency (DIA)	Centre for Development of Advanced Computing C-DAC	Cyber Attacks Crisis Management Plan of India (CACMP)
Multi Agency Center			Defence Research Dev Authority (DRDO)	Standardisation, Testing and Quality Certification (STQC)	
National Information Board (NIB)					

[217] Ibid.
[218] Alexey Kupriyanov, India in the Era of Cyber Wars, RIAC, 2019
[219] Dr VK Sraswat, Cyber Security, NITI Aayog, 2017
[220] Brig. Gurmeet Kanwal, China's Emerging Cyberwar Doctrine Issue Vol 24.2, 2012

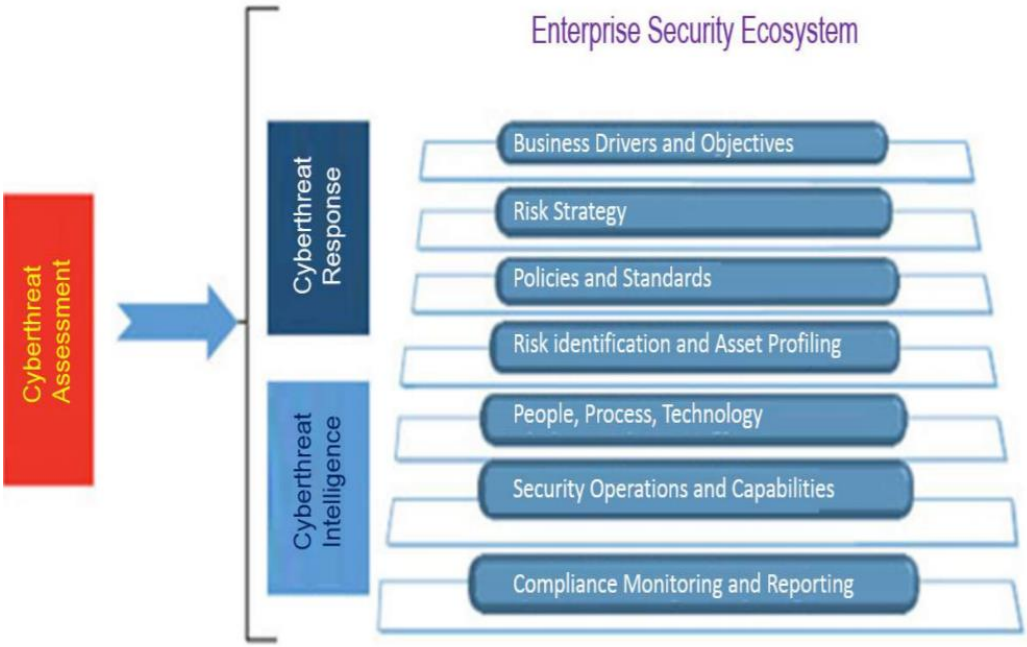
The first serious attempt to respond to challenges in cybersecurity dates to 2012 Munich Security Conference[221] where Indian specialists pushed for:

- Creating their own microprocessors and planning to cut imports of military software, instead of channeling money into domestic R&D (the share of imported military software in India is currently about 70%).[222] About hardware, a number of computers and telecommunication hardware in Indian telecommunication networks, government departments, railway network, power network are of Chinese origin and are infested with virus, worms and trojans due to Chinese espionage campaigns in collecting critical information about Indian networks/systems which may be used to disrupt them at a critical time.''[223] ''China is the major source of silicon integrated microchips (being used in all electronic devices) for all manufacturers across the globe. This increases the possibility of undesired alterations in these integrated circuits which my lead China's intelligence collection and system vulnerability identification, giving PLA a tremendous advantage in a confrontation situation in the bilateral relations.''[224] And security begins and deals with a trustworthy hardware.

- Creating a command and control center to monitor critical infrastructure and eliminate breaches in cybersecurity.[225]

- Creating a National Cyber Security Policy, developed by the Department of Electronics and Information Technology to protect the personal information of India's citizens as well as financial and bank information and data that are of critical significance for state governance and security against theft and cyberattacks.[226]

- Creation of a reliable cyber ecosystem in the country and reliable work among IT systems that were being introduced on a large scale in all economic sectors[227], through a planning of cyberthreat management, like it is shown in the figure below.



228

[221] Elizabeth Radziszewski, India's Response to China's Cyber Attacks, The Diplomat, 2019
[222] Alexey Kupriyanov, India in the Era of Cyber Wars, RIAC, 2019
[223] Brig. Gurmeet Kanwal, China's Emerging Cyberwar Doctrine Issue Vol 24.2, 2012
[224] Ibid.
[225] Alexey Kupriyanov, India in the Era of Cyber Wars, RIAC, 2019
[226] Ibid.
[227] Ibid.
[228] Dr VK Sraswat, Cyber Security, NITI Aayog, 2017

As early as 2018, a report to India's National Security Council Secretariat (NCSC) attributed to China 35% of cyber attacks[229], which had knocked down power grids, nevertheless causing impacts on critical infrastructures. However, the real issue is how '' China's cyber policy against India could undermine the country's conventional power in a future military conflict.''[230] Consider the 2009 incident in which Chinese hackers stole classified intelligence from India's military on missile systems and on India's security situation in its various states: in case of a military escalation, such a collection of information could have been used by the Chinese military not only to exploit systems' weaknesses but also to identify an appropriate window of opportunity to strike when the country is most vulnerable politically. As Elizabeth Radziszewski, an Assistant Professor of Political Science at Rider University, stated in article published on the Diplomat: ''between 2010-2018, China's main goal in targeting India was to gain access to sensitive information from the government and the private sector (over 55 percent of cases), followed by disruption of daily activities as was seen in 2010 when China's use of Stuxnet worm to compromise India's communication satellite led to the loss of TV signal for many. Intrusion with the use of malicious software such as Trojans to enter the target's network or software program has been the most common form of method in cyber attacks during this time. Such intrusions are particularly dangerous. They can remain dormant for a long time only to emerge later.'' The above-mentioned attribution conundrum played its role also on these occasions. Even though the attacks were traced from Chinese territory, the Chinese government denied any responsibility. Recognition of the complexity of threat management has given India the final boost for a modernization of its strategy. Indeed, ''relying on restraint as a strategy becomes even more critical when considering the broader political context in which the attacks take place. Countries that are embedded in a long-term rivalry and that also happen to have other enduring enemies''[231]

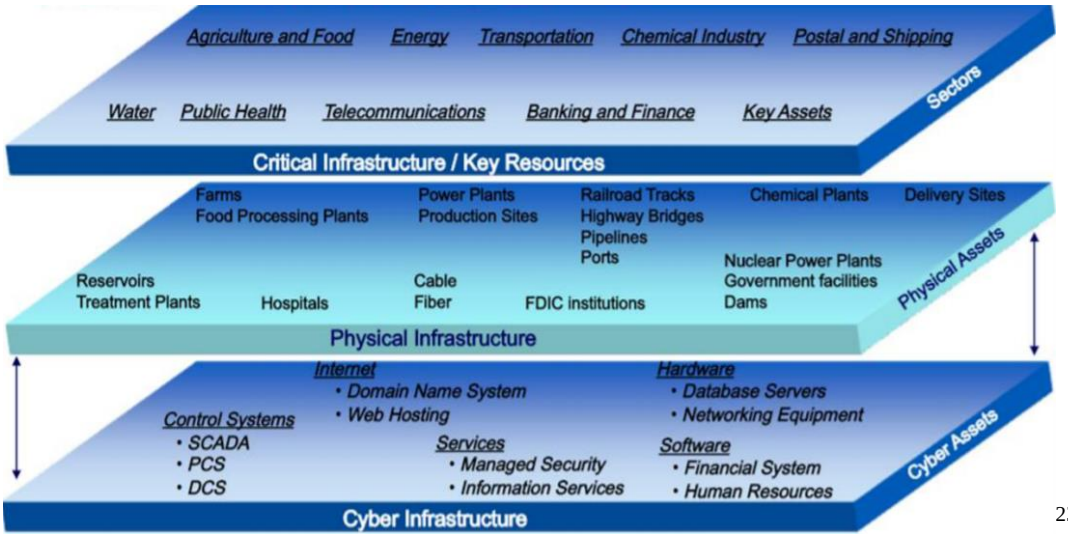
The speech of the Prime Minister Narendra Modi at the Combined Commander's Conference in 2014 summarizes the tones of concern of the above mentioned new challenges: ''We are facing a future where security challenges will be less predictable; situations will evolve and change swiftly; and, technological changes will make responses more difficult to keep pace with. The threats may be known, but the enemy may be invisible. Domination of cyber space will become increasingly important… When we speak of Digital India, we would also like to see a Digital Armed Force.'' Doctrinal response to such new strategic challenges have always been slower than information technologies development, creating the new domain of cyberspace. Since 2018, the Indian government has approved the establishment of a Defense Cyber Agency which is an intermediate step towards a full-fledged cyber command.[232]

In July 2018 India announced the creation of a military agency on cybersecurity called Defense Cyber Agency (DCA) to cooperate with the executive office of the National Security Advisor (established in 2015) to ensure the cybersecurity of the armed forces, the condition of offensive operations in cyberspace and the development of a cyber ops doctrine. However, because of the traditional autonomy of the navy, the air force, and the military, which are reluctant to share operational information with each other and the difficulties of developing their own software, it is hard to evaluate the efficiency of such a program. However, the development of a new cybersecurity strategy for 2020 aims in ensuring the protection of important data given the introduction of 5G technology which, according to Lt. Gen. Rajesh Pant, the National Cyber Security Coordinator on the National Security Council, ''will radically change the state of affairs in this regard.''[233]The Indian authorities have focused on conducting defensive and offensive operations in cyberspace while reducing India's dependence on hardware, software and tools developed aboard, preferring India-made products. Such decisions were made on the base of the new challenges posed by internet and cyberspace, how we mentioned above. At present, India finds as it natural adversaries in cyberspace (and real space) Pakistan and China, with the latter '' conducting large cyber operations against India which have reached such a scale that some analysts characterize them as a full-fledged cyberwar. This war takes on various forms: from hacking Indian networks to providing various rebel groups with hosting services on China's servers; nonetheless, the large-scale cyber

[229] Elizabeth Radziszewski, India's Response to China's Cyber Attacks, The Diplomat, 2019
[230] Ibid.
[231] Elizabeth Radziszewski, India's Response to China's Cyber Attacks, The Diplomat, 2019
[232] Vif task force report, Credible Cyber Deterrence in Armed Forces of India, Vivekananda International Foundation, 2019
[233] Alexey Kupriyanov, India in the Era of Cyber Wars, RIAC, 2019

ops have not prevented Beijing and New Delhi from strengthening their political and military relations.''[234]

Internet penetration is a measure of the extent of reliance on net-enabled services by common citizens, business, critical information infrastructure, military and government. In this domain, it is hard to draw clear boundaries between military and non-military users.[235] Cyber threats may result in serious disruption of government, public and private sector resources and services, striking national security and economy. India is quite vulnerable from this point of view; indeed, it has been amongst the worst affected countries from global cyberattacks. For example, the 2017 WannaCry ransomware attack affected about 48,000 computers, while the 2010 Stuxnet malware attack affected computers in India belonging to critical infrastructure facilities, including power grids and offshore oil rigs of the Oil and Natural Gas Corporation. The Nuclear Power Corporation of India, by its own admission, blocks at least 10 targeted cyberattacks a day.[236] The asymmetric nature of warfare is characterized by the fact that '' cyberattacks can be launched by a much weaker adversary (militarily, technologically and economically), or even by non-state actors at negligible cost. Also, the positioning of 'cyber attacks' in the escalatory ladder of conflicts still remains ambiguous. These could well be situated from the lowest end of the spectrum to upper end strategic conflict levels.''[237] In such a scenario, anonymity plays a vital role with cyberattacks may originate from co-opted servers in countries (such as China), at times without knowledge of such countries (however, culpability and legitimacy of actions remains ambiguous.) As it happened to India, intrusions are often used for 'cyber espionage', to gather military intelligence, industrial espionage or theft of commercial information. Nevertheless, such cyberattacks against particular targets may result in cross-sectoral disruption (intrusion into networks controlling critical civilian infrastructure, power grids, transportation networks and financial systems can have national security and military implications.)[238]



239

This section focused on India's cyber capabilities, highlighting the critical points of national's cyber evolution. The considerations of the paragraph have been made, regarding new challenges posed by cybernetic disputes, among which is the Sino-Indian one, with a positive trend throughout 2020 (as mentioned earlier in the chapter.) What emerged however is that ''India is very vulnerable to cyber interventions for such main reasons: certain strategic deficiencies, absence of a clear-cut policy directive and cyber warfare doctrine, and a cyber power insufficient compared to the threats and its national security needs''.[240]

[234] Ibid.
[235] Vif task force report, Credible Cyber Deterrence in Armed Forces of India, Vivekananda International Foundation, 2019
[236] Ibid.
[237] Ibid.
[238] Ibid.
[239] Dr VK Saraswat Member, Cyber Security, NITI Aayog, 2017
[240] Ibid. p.47

Conclusion

‘’The strategic landscape has changed forever, somewhat like when nuclear weapons first appeared on the scene in 1945.’’ [241] Assessing threats and sources of instability between states’ relations in the pre-digital era needed a more classical and traditional approach. As history debates, ages of the human time are often labelled after its dominant technology: and the transition from machine age, to later atomic age and to now information age was quicker than it seemed. Information Communication Technologies (ICT) are recently shaping world power structure[242], and therefore a new evaluation on the matter is dutiful. Technologies’ implications on a transnational level, and in geopolitical debates, needs a role of conduct and a rule of law which has tendentially been normalized by the practices of international law. The issue on which the thesis wants to stress out the alarm call, is that international law has been slow in reacting to the global and regional ramifications the cyberspace was able to generate. ‘’But in cyberspace the legitimacy of a national law claim is determined not by the internal perspective of the legal system but by the external perspective of cyberspace actors. A law will only have authority in cyberspace if it can convince cyberspace actors that its claim is legitimate. And a legal system which repeatedly makes illegitimate claims thereby weakens its status as a system which adheres to the rule of law.’’[243]

Governing the cyberspace must become a focal point for security analysts since it may give rise to a rapid escalation, generating a what has been labelled as cyberwarfare. Cautiousness is needed above all when the actors are two world nuclear powers attempting to seize regional hegemony over the Indo-Pacific. The rising digital world is able to attribute new opportunities and risks in such scenarios: especially when, in light of the description the thesis highlighted on the structural complexity of relations between China and India, the new challenge translates into a strategic cyber competition in both Asia and the cyberspace. The fifth dimension of warfare, due to its overwhelming effects, has been outpaced the technological development in conventional military weapons space, changing the very character of future wars, and the role of cyber warfare in them.[244]China has made an enormous progress in developing cyber warfare capabilities in terms of policies evaluations, restructuring organisations and raising human expertise in order to deter physically and technologically superior military adversary. In another five to 10 years, China is touted to develop much greater depth and sophistication in its understanding and handling cyber and information operations. With the Indian society becoming increasingly dependent on automated data processing and vast computer networks, New Delhi is well on its path at becoming extremely vulnerable and therefore should contribute to strengthen its cyber power and capabilities.

This thesis has tried to highlight the critical points that characterize the history of Indo-Chinese relations. This was done through a historical and linear analysis of diplomatic relations between India and China, focusing on the breaking points that have contributed to destabilize the latter and the Asian region. This analysis has been followed by a theoretical parenthesis on what cyberspace is, and how it has entered in recent years to play an important role in global politics. This phenomenon is analyzed from a neo-realist perspective to highlight the delicate points that characterize cyberspace and the operations that take place in it, such as the attribution conundrum and the lack of a strict governance regulating belligerent operations in cyberspace.

[241] Brig. Gurmeet Kanwa, Acupuncture Warfare: China’s Cyberwar Doctrine and Implications for India, Indian Defence Review, 2017
[242] P.J. Blount, Reporgramming the World: Cyberspace and the Grography of Global Order, E-International Relations Publishing, 2019
[243] Chris Reed, Why judges need jurisprudence in cyberspace, Volume 38, Issue 2 The Society of Legal Scholars, Cambridge University Press, 2018
[244] Brigadier Saurabh Tewari, The United Service Institution of India: China’s Cyber Warfare Capabilities, 2019

In this regard, the thesis has reported a long series of cyber attacks suffered by the Indian State, often attributed to Chinese territory. Subsequently, the last chapter of the thesis tries to analyze in detail, as difficult as it may be, the various doctrines, state organizational skills and evaluation of policies regarding the use of cyberspace in international relations and cyberwarfare. This thesis wanted to dwell on the theme of cyberspace, because I strongly believe, in line with the vision of many academics, that in the coming years, it will be necessary to structurally discuss the possible future-oriented implications that cyberspace can have in global politics. This consideration is especially important in light of the escalation, fortunately not too severe, that has occurred lately between the two Asian states. The fluctuating tones heard in 2020 by both states are part of a political logic that destabilize the possible broad views of cooperation thought in the past. And assuming a scenario of relations' deterioration between the two Asian states, cyberspace, in light of the analysis carried out in the thesis, could play a major role in becoming a new theatre (the fifth operational domain) of confrontations, even more lethal than the skirmishes at the border. The understanding of cyberspace as a domain requires further maturing and discussing.[245]

''Cyberspace has become much more than an infrastructure that enables weapons and early-warning systems: it is now a domain where power is projected, strategic goals may be achieved without the use of force, and wars will be fought.''[246] Operations conducted in cyberspace become a key element in a country's deterrence posture, and may constitute, in future, in preparation for war. ''How to read, for instance, the malwares that have been found in critical infrastructures around the world, other than weapons ready to be used in case of a conflict?'' In 2016 NATO recognized at a summit that "cyber attacks present a clear challenge to the security of states and could be as harmful to modern societies as a conventional attack" and that cyberspace is a domain of operations. [247] According to the Command Vision for US Cyber Command[248], cyberspace has already been militarized, and disruptive technologies (such as artificial intelligence, autonomous lethal weapons, neurological implants) will eventually accelerate states' abilities to impose costs, in our near future. Nevertheless*, ''technology trust is a good thing, but control is a better one.''*[249]

[245] Gen. Larry D. Welch, Cyberspace – the fifth operational domain, www.ida.org
[246] Fabio Rugge, Cyberspace and the Armed Forces, ISPI, 2018
[247] Warsaw Summit Communiqué, paragraph n.70.
[248] The Command Vision for US Cyber Command, "Achieve and Maintain Cyber Superiority", 2018.
[249] Stéphane Nappo, Vice President Global Chief Information Security Officer, quote

Bibliography

- Adam P. Liff and G. John Ikenberry, Racing toward Tragedy? China's Rise, Military Competition in the Asia Pacific, and the Security Dilemma, *International Security*, Vol. 39, No. 2, Harvard College, and the Massachusetts Institute of Technology

- Alexey Kupriyanov, India in the Era of Cyber Wars, RIAC, 2019

- Anthony Craig and Brandon Valeriano, Realism and Cyber Conflict: Security in the Digital Age, E-International Relations, 2018

- Athina Karatzogianni, Cyber Conflict and Global Politics, Routledge, 2009

- B.M. Jain, India–China relations: issues and emerging trends, Routledge Taylor & Francis Group, 2004

- Brigadier Saurabh Tewari, The United Service Institution of India: China's Cyber Warfare Capabilities, 2019

- Brig. Gurmeet Kanwal, Acupuncture Warfare: China's Cyberwar Doctrine and Implications for India, Indian Defence Review, 2017

- Charles Wolf, Jr., Siddhartha Dalal, China, and India, 2025: A Comparative Assessment, National Defense Research Institute, 2011

- Clarke and Knake, Cyber War, Ecco Pr, 2012

- Colonel Deepak Sharma, China's Cyber Warfare Capability and India's Concerns, Journal of Defence Studies

- Daniel Johanson, Jie Li and Tsunghan Wu, New Perspective on China's Relations with the World, E-International Relations Publishing, 2019

- David M. Malone and Rohan Mukherjee, India and China: Conflict and Cooperation, Survival Global Politics and Strategy Journal, 2010

- Elizabeth Radziszewski, India's Response to China's Cyber Attacks, The Diplomat, 2019

- F. Rugge, "An 'Axis' Reloaded?", in Idem (ed.), *Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace*, ISPI Report, 2018

- F. Rugge, Cyberspace and the Armed Forces, ISPI, 2018

- Federico Rampini, Oriente e Occidente: Massa e individuo, Feltrinelli

- Frank O'donnell, Stabilizing Sino-Indian Security Relations: Managing Strategic Rivalry After Doklam, Carnegie-Tsinghua Center for Global Policy, 2018

- Hackmageddon, Information Security Timelines and Statistics, 2020

- Hongzhou Zhang and Mingjiang Li, Sino-Indian Border Disputes, ISPI, 2013

- James Lewis, Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia, Lowy Institute MacArthur Asia Security Project

- Joseph S. Nye, Cyber Power, Harvard Kennedy School, 2010

- Joshua Ball, Global Security Review, Asian Hegemony: Ongoing Tensions between China and India, 2019

- Keshab Chandra Ratha and Sushanta Kumar Mahapatra, India-China Bilateral Relations: Confrontation and Conciliation, Vision 2020: Sustainable Growth, Economic Development, and Global Competitiveness

- Kseniia Neradko, A Cyber Westphalia: Challenging the Fifth Dimension, Tallinn University of Technology, Bachelor's Thesis, 2018

- Lam Peng Er, Lim Tai Wei, The Rise of China and India: A New Asian Drama, East Asian Institute, 2009

- Lyu jinghua, What Are China's Cyber Capabilities and Intentions? Carnegie Endowment for International Peace, 2019

- Li Zhang, A Chinese perspective on cyber war, International Review of the Red Cross, 2012

- Monika Chansoria, China's Cyber Wars *India Strategic* also hacked, Centre for Land Warfare Studies (CLAWS), 2010

- Nigel Inkster, China in Cyberspace, Nationalism in Chinese cyberspace, Cambridge review of international affairs, 2010

- Nigel Inkster, ''Chinese Intelligence in the Cyber Age'', Survival, 2013

- NTI Building a Safer World (reports on China and India), 2015, 2020

- P. J. Blount, Reprogramming the World: Cyberspace and the Geography of Global Order, E-International Relations Publishing, 2019

- P.J. Blount, Reporgramming the World: Cyberspace and the Geography of Global Order, E-International Relations Publishing, 2019

- R. Lindsay, China, and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain, OXFORD, 2015

- Richard Clarke and Knake, Cyber War

- Rika Isnarti, A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War, Andalas Journal of International Studies| Vol 5 No 2 November Tahun 2016

- Rollie Lal, Understanding China and India: Security Implications for the United States and the World, Praeger Security International, 2006

- Samm Sacks, China's Emerging Cyber Governance System, Center for International and Strategic Studies

- Sasha Romanosky & Zachary Goldman, Understanding Cyber Collateral Damage, 2017

- Survey of Chinese-linked Espionage in the United States Since 2000, Center for International and Strategic Studies

- SIPRI Yearbook 2020

- Theohary, "Information Operations, Cyberwarfare, and Cybersecurity

- Toby Dalton, At a Crossroads? China-India Nuclear Relations After the Border Clash, Carnegie Endowment for International Peace, 2020

- Tien-sze Fang, Asymmetrical Threat Perceptions in India-China Relations, OXFORD, 2014

- Tim Stevens, Cyber Security and the Politics of Time, Cambridge University Press, 2016

- Zhiqun Zhu, China-India Relations in the 21st Century: A Critical Inquiry, *Indian Journal of Asian Affairs* Vol. 24, No. 1/2, , 2011

Abstract

La tesi di laurea "*Sino-Indian relations within the Fifth Domain: competition and challenges in the cyberspace*'' ha lo scopo di descrivere l'attuale, nuovo confronto cibernetico tra India e Cina, postosi all'attenzione della comunità internazionale e dell'opinione pubblica, in quello spazio cibernetico che a livello strategico è attualmente considerato la quinta dimensione del teatro di guerra, dopo terra, mare, cielo e spazio. Ciò, peraltro, si contestualizza nelle recentissime tensioni frontaliere avvenute dopo anni di tregua e attività diplomatiche tese a risolvere l'annosa questione dei contenziosi confinari, sfociati nella guerra del 1962. In particolare, la tesi vuole porre l'accento sul trasferimento del conflitto "classico" tra i due Stati alla citata quinta dimensione e, contestualmente, analizzare l'*escalation* ai confini Indo-Cinese alla luce dell'incremento delle operazioni cibernetiche per capire, attraverso una prospettiva neorealista, se lo spazio cibernetico possa diventare un nuovo teatro di scontro tra India e Cina anche per motivi collegati all'impiego di minori risorse e il raggiungimento di maggiori opportunità. Quanto sopra alla luce del lor comune obiettivo di assurgere a prima potenza regionale in Asia lo spazio cibernetico potrebbe offrire nuove opportunità di scontri, rinunciando ai costi di un conflitto militare ai confini e divenendo il nuovo campo di battaglia dei due paesi egemoni.

La tesi deve necessariamente fare un breve *excursus* sulle relazioni Indo-Cinesi al fine di individuare, successivamente le criticità che hanno contribuito alla destabilizzazione dei loro rapporti. Il primo capitolo delinea le loro relazioni diplomatiche relativamente al ventesimo e ventunesimo secolo. In particolare, la prima sezione esamina i rapporti bilaterali tra India e Cina e di come essi siano passati da una "fase amicale" denominata *Hindi Chini Bhai Bhai* (gli Indiani ed i Cinesi sono fratelli) ad una successiva "fase ostilità", che ha portato, alla fine degli anni 50, ad un rapido deterioramento per le divergenti visioni degli affari regionali. Inoltre, si sofferma sull'importante ruolo del Trattato *Panchsheel* (in hindi) siglato dai due Paesi asiatici nel 1954, sul successivo peggioramento delle relazioni stigmatizzate dalla guerra del '62 e ai successivi, altalenanti rapporti politico-diplomatici sviluppatisi fino agli anni Ottanta. La seconda parte analizza i fattori storici che hanno contribuito a destabilizzare l'armonia tra i due paesi asiatici, fra questi: il citato contenzioso territoriale, la questione Tibetana, la proliferazione nucleare e la percezione asimmetrica delle minacce per rivederli in chiave cibernetica. L'analisi storica dei rapporti tortuosi serve a comprendere i punti di rottura tra i due Stati, per proseguire con l'imminente tema della moderna competizione cibernetica tra Cina e India.

Il secondo capitolo riguarda il concetto di *Cyberspace* analizzandone le implicazioni e i risvolti nelle relazioni internazionali alla luce dell'attuale trend incrementale di operazioni cibernetiche Inoltre si sofferma sulla pluralità delle definizioni di *Cyberspace*, secondo le opinioni di illustri accademici e non del campo come W. Gibson, Corrado Giustozzi e F. Rugge, fino a giungere alla definizione unilaterale del *The National Academy of Sciences*, organizzazione non-governativa *pro bono publico*. La prima sezione del capitolo fa una disamina del citato *cyberspace* e delle sue nuove tecnologie di *persuasion* sulla comunità internazionale e sull'intera società, evidenziando come questa sia di difficile comprensione per tutti inclusi i cosiddetti *decision-maker*. A titolo di esempio, si riportano due casi noti: gli attacchi cibernetici del 2007 ai danni dell'Estonia e quelli del 2010 ai danni dell'Iran. Come dimostrato dal caso *Stuxnet*, il dominio cibernetico evidenzia un forte punto critico assente nelle guerre tradizionali: l'enigma nell'attribuzione degli attacchi, che consente di mascherare l'identità, la posizione dell'avversario e l'attribuzione a ignari terzi soggetti. La sezione, inoltre, tratteggia il concetto di *Cyberpower* di uno stato e il conseguimento dei risultati raggiunti tramite le cosiddette *Computer Network Operations*, evidenziando l'incertezza maggiore delle operazioni informatiche in confronto alle operazioni fisiche. La seconda parte del secondo capitolo analizza l'evoluzione storica di una possibile giurisdizione globale che possa governare la complessità del *Cyberspace* e le *Computer Network Operations* e delle implicazioni che possono avere nelle relazioni internazionali. In particolare, descrive gli sforzi compiuti e gli scarsi risultati ottenuti dalle Nazioni Unite, la Convenzione di Budapest (2004) sulla criminalità informatica ed il *Tallinn Manual*, un insieme di norme giuridiche per l'applicazione del diritto internazionale in materia di *cyber warfare* e di operazioni cibernetiche. Come da titolo, introduce il dibattito affrontato dalla NATO circa l'applicabilità del diritto internazionale al *Cyberspace* proponendo una panoramica sulle problematiche attuali. In prosieguo, attraverso le considerazioni di accademici della scuola neorealista di relazioni internazionali, il capitolo affronta il

concetto di *Security Dilemma* partendo dalla sua definizione originale di John H. Herz (1951), fino ad arrivare ad una dimensione cibernetica dello stato di *Security Dilemma*. Per analizzare quest'ultima, la sezione affronta le implicazioni delle nuove condizioni dettate dallo spazio cibernetico, in modo da concettualizzare le attuali moderne sfide che lo spazio digitale/cibernetico pone agli stati.

I primi capitoli, come detto, rappresentano i presupposti per affrontare il tema della competizione e disputa cibernetica in corso tra India e Cina. Difatti, il terzo e ultimo capitolo affronta la questione del confronto cibernetico tra i due giganti asiatici, partendo dalla recente dichiarazione del *Maharastra Cyber* (Dipartimento Cibernetico della polizia indiana) che riporta una tendenza incrementale di attacchi cibernetici provenienti da territori Cinesi in seguito ai succitati scontri militari del 2020 ai confini Indo-Cinesi. In tale contesto, si sottolinea come la pratica offensiva, ibrida e multidimensionale degli attacchi cibernetici possa influenzare negativamente i complessi rapporti tra India e Cina e come la concorrenza cibernetica attuata anche con mezzi "poco ortodossi" sia attuata per ottenere vantaggi economici e commerciali a medio-lungo termine. In questa sede viene affrontato con specificità il ruolo cibernetico della Cina ne viene analizzata l'evoluzione cibernetica, le dottrine utilizzate, l'organizzazione statale dei dipartimenti cibernetici ed il problematico ruolo degli attori non-statali sul territorio cinese. Difatti, la posizione belligerante della Cina ha un ruolo geopolitico, cercando di consolidare la propria egemonia Asiatica, e strategico, tramite l'accesso ad informazioni sensibili per lo stato Indiano. D'altro canto, concentrandosi sulle capacità informatiche dell'India ed evidenziando i punti critici dell'evoluzione informatica nazionale, come l'assenza di una vera strategia guidata da una singola direzione politica e una potenza cibernetica insufficiente rispetto alle minacce e le esigenze di sicurezza nazionale, l'India ha deciso di mantenere una posizione moderata; tale posizione, come affrontato nella tesi, è dovuta per i sopracitati motivi nazionali, ma anche alle implicazioni teoriche affrontate nel secondo capitolo.

In sintesi, come detto in preambolo, la tesi vuole analizzare gli effetti e le conseguenze che il *cyberspace* e le *Computer Network Operations* potrebbero avere sull'instabile rapporto Sino-Indiano. A tal riguardo, l'elaborato si è dipanato dalla storia delle relazioni tra i due Stati, con particolare riferimento ad un'analisi storica e lineare delle relazioni diplomatiche e criticità relative all'intera regione asiatica, a una breve ricerca teorica sul *Cyberspace* e sulla sua maggiore influenza sulla politica globale, attraverso la "lente" della prospettiva neorealista per delineare l'attuale competizione cibernetica tra i due colossi asiatici e i possibili scenari. In ultima analisi l'elaborato si è concentrato sulla disputa cibernetica tra India e Cina poiché, in linea con la visione di molti accademici, è verosimile che nei prossimi anni questa disputa continuerà e dovrà essere affrontata strutturalmente considerando le possibili implicazioni future che il *cyberspace* ed *internet* possono avere nella politica regionale ed internazionale. Rileva che i toni usati dai *decision-maker* sino-indiani nel 2020, al momento fanno ritenere il perseguimento di una logica politica opposta alle ampie visioni di cooperazione dei primi anni 50. Si ritiene che, nell'ipotesi di uno scenario di deterioramento delle relazioni tra i due Stati asiatici, il *cyberspace* possa giocare un ruolo di scontri, ancora più letale delle schermaglie fisiche di confine. La comprensione del *cyberspace* come dominio di confronto tra stati richiederà ulteriori maturazioni e riflessioni, che in parte, ho deciso di riportare in questa tesi.