International Journal of Political Science (IJPS)
Volume 7, Issue 1, 2021, PP 25-33
ISSN 2454-9452
https://doi.org/10.20431/2454-9452.0701003
www.arcjournals.org

Internet, Cyber Attacks, Rare Earths: Sino-Russian Confrontation with the West

Eirini Sotiriou*

PhD Candidate, Department of Political Science and International Relations, University of the Peloponnese, Greece

***Corresponding Author:** **Eirini Sotiriou,** *PhD Candidate, Department of Political Science and International Relations, University of the Peloponnese, Greece*

Abstract: *The rising tide of technology, digital oppression, the complete questioning of human rights and freedoms compose the new image of the future. The triumphant advent of 5th generation technology takes place, with estimated connectivity speeds of up to 20 Gigabits per second. Artificial intelligence, the development of smart devices in combination with cloud technologies (cloud computing) penetrate into every aspect of our daily lives. The Internet of Things is an integral part of our lives.*

At the same time, the United States is promoting an open and commercial Internet, China is building the Great Wall, and Russia is shutting down its World Wide Web. Cyberspace is the new field of conflict. Rare earths, led by China, are the key to geopolitical developments. What emerges is the promise of technology in the 21st century not to turn into a curse and technology to serve man and not to become a tyrant.

Keywords: *Internet, Cyberattacks, Rare Earths, Sino-Russian Confrontation with the West*

1. INTRODUCTION

In this day and age, a reality is taking shape where the role and action of state and non-state actors, interdependent relations at the economic, social and political level, integration phenomena and new threats, co-shape the international system (Cheila & Ziogas 2017). For nearly five decades (Macedonia 2019) , the Internet has grown and spread widely around the world under US leadership (Shen 2016 :319), beginning with the military (Tai 2006 :85). For many years, American social media companies have been accused of "exporting" US culture and politics to the rest of the world (O' Brien 2019). (Primary ICANN (Fang 2018: 434, Arsene 2016 :26) distribution of addresses on the internet under American umbrella until recently). ICANN is a nonprofit company based in California, which was accountable to the U.S. Department of Commerce. This entity is responsible, inter alia, for the operation of the Domain Name System (DNS), privacy, intellectual property and cyber security issues (Liaropoulos 2015:192). It plays a crucial role in the stability and security of the Internet as well as in the fair distribution of resources (Arsene 2016:30).

The loss of U.S. leadership online could be a symptom of the greater U.S. abdication of global leadership in countries such as China and Russia, which are expanding their spheres of influence in Africa and the Middle East, just as the U.S. is leaving these regions (Uchill 2019).

The central question that arises is to examine the different ways of approaching the internet from the perspective of the China- Russia confrontation with the West. Cyber –attacks as a new field of competition and the possession of rare earths as a cause of contention for the future deserve our attention.

Stations of our tracking will be-in the midst of the 4th Industrial Revolution and its rapid consequences-the internet, cyber-attacks, rare-earths as a challenge for tomorrow and the geopolitical balances (or their absence) that are taking shape.

2. INTERNET

Internet, Cyberspace basic icons of a new mythology, with unparalleled fascination for new technical miracles, that transforms every society (Bakardjieva 2005 :1). The Internet is a record of a large volume of free software and information resources, placed on the network by individual developers,

enthusiasts and entire collectives with the aim of interacting with the entire Internet community. It is the fourth means of communication, after the press, the (radio) broadcasts, the television and provides the effective power, all the time, relatively inexpensive, direct and convenient. The Internet, which has been described as a double-edged sword (Stoycheff & Nisbet 2016) is a vast treasure trove of knowledge, information and materials, which is the symbol of electronic resources (Genieva 1997 :382). The Internet quickly became a transformative force around the world, forever changing the economic, social and political landscape of the world. Ability to overcome social distances and barriers, vision for a global village (Bakardjieva 2005 :43). The broader problem of "post-truth" that emerges in various forms of fake news, hoaxes, trolling should concern us (Mikelis 2018 :18-19). Web governance emerges as leading issue for 21st century global governance (Nocetti 2015 :112). The battle for 5G is shifting from trade to geopolitics (Veratis 2020), as this technology is considered the next "tool" of dominance.

3. CYBERSPACE

Global sector within the information environment, whose particular and unique character is framed by the use of electronic and electromagnetic spectrum for the creation, storage, conversion, exchange and exploitation of information through independent and interconnected networks, using information communication technologies, in accordance with Daniel Kuehl's definition. Cyberspace, as a term created and spread by William Gibson, has achieved the status of a major intellectual trend, as computerization and Internet connectivity become deeply rooted in every aspect of human life (Tai 2006 :xxii). Cyberspace is a growing digital network that connects social, business and military networks around the world (Liaropoulos 2013:5) . Cyberspace is the fifth battlefield, after the ocean, earth, space and sky (Fang 2018:423). Krasner's typology of domination- Domestic, Interdependence, International Law and Westphalian- contributes to the demystification of the myth that cyberspace is invulnerable to state domination (Liaropoulos 2013 :22). Cybersecurity a common challenge (Fang 2018 :177) and a national security issue (Liaropoulos 2015: 189). Cyberattack is an aggressive act against network computer systems or infrastructure. Our confidence in automation focuses on individual failure points that can have dramatic consequences if they are directed to power stations, communications networks, transport and other utilities (Acs 2016 :11) . Authoritarian governments seek to create a "psychological wall" that paints the Internet as a frightening world full of political threats (Stoycheff & Nisbet 2016).

The global spread of information and communication technologies (ICT) that have driven the Internet over the past decade has intensified the global information revolution and governments have struggled to cope with the economic, social, cultural and political consequences of this revolution (Tai 2006 :81). Cybersecurity requires discipline, the practice of preventing and mitigating attacks on computer systems and networks.

4. GREAT WALL OF PROTECTION

A censorship and filtering service, designed to prevent the circulation of information that authorities consider politically dangerous without affecting non-sensitive information, requiring huge financial, human and technological resources to maintain it (Puddington 2017 :7).

According to the "Spectator Index" , Google search, Gmail, Yahoo, Facebook (Iosifidis & Wheeler 2016 :176), YouTube, Wikipedia, Twitter, Netflix, Instagram, WhatsApp and Dropbox, as well as the websites BBC, The New York Times and the Economist (French 2019) have "no place" in the Chinese internet. This is a powerful digital surveillance architecture (Polyakova & Meserole 2019). The Great Firewall or On Line Great Wall of China (Kathimerini 2019), as part of the Golden Shield Project is the most advanced surveillance system in the world (Ziccardi 2012:247). The goal is to "make the internet clean and bright," according to Xi Jinping (Puddington 2017 :19). The Chinese President promoted the idea of "cyber sovereignty" (Fang 2018 :173, Li 2019) asking other countries to respect China's internet governance practices. Censorship is a matter of national security for the Chinese state (French 2019). Beijing has been rocked by the role social media (Liaropoulos 2013 :7) played in the Arab Spring and Green Revolution of 2009 in Iran and has therefore completely blocked access to Facebook.

Another possible reason for the ban is the riots (SecNews 2014) that broke out in July of the same year between Muslim Uighurs and Chinese Han in the western Xinjiang region (Zucchi 2019). The social revolutions that took place in Iran, Tunisia, Egypt and other countries revealed that social media and social networks can act as a force multiplier for political action (Liaropoulos 2013 :5).

5. TECHNICAL EXCLUSION METHODS

Keyword (Xu & Mao & Halderman 2011 :134), which prevents access to or block search, removal of prohibited results from search engines, occupation, by those who wish to regulate a particular behavior and have targeted a specified site, have direct access and full jurisdiction for web content hosts form the canvas of relevant techniques (Ziccardi 2012 :201). The most insidious method of censorship is self-censorship.

CASE OF CHINA: Block IP Address, Redirect.

5.1. Internet Manipulation

5.1.1. Methods of Control of the Internet from the Party

The government uses the fear of punishment or its threat (Nathan 2018) to guide behavior. The flood refers to the regime's attempts to stifle critical thinking in a storm of pro-government messages or confusing news leading to an ocean of contradictions, in the hope that the average citizen will not pursue the truth further. The most worrying tactic is friction over access to or dissemination of information as an increase in costs, either in time or in money (Weber 2019:3). Its quintessence is the delay of the loading rods, instead of the total ban.

5.2. China's Orwellian Social Credit System

In George Orwell's dystopian novel, 1984, the Ministry of Truth moved under a narrative regime, with an account of endless conflicts abroad and treacherous enemies at home (Puddington 2017:7). Orwell and other enemies of totalitarianism sought to describe the danger that propaganda and censorship pose to knowledge, reality, and independent thought.

China's Orwellian Social Credit System constitutes a form of digital totalitarianism (Pelevani 2019) allows the state to gather information about citizens from a variety of sources and use it to justify ratings or rankings based on an individual's true credibility, even in political matters. The invisible "Big Brother" monitors digital fingerprints in cyberspace (Tai 2006 :98). The citizen could receive a bad grade by reporting to the government, participating in protests or circulating banned ideas on social media (Puddington 2017:58).

5.2.1. Assessment to "Social Credit System"

Citizens with a good "Social Credit" rating benefit from a range of perks, including travel apps abroad, energy discount accounts and fewer frequent checks. "Social Credit" penalties include individuals or companies that are considered "unreliable" can be excluded from state-sponsored benefits, such as non-prepaid apartment rentals or banned air and train tickets.

5.3. Position of the Chinese Leadership

"If trust is lost in one place, restrictions are imposed everywhere. Those who are considered unreliable will not be able to take a step." The internet and advanced face recognition technology with countless cameras control individual behavior (Eckert 2019), "enriching" the blacklist of dissidents.

China already has a spy program that competes with the Stasi (Kendall –Taylor & Frantz & Wright 2020), East Germany's state security service, which may have been one of the most widely used secret police in the world. It was famous for its ability to monitor individuals and control information flows, using repression to maintain control. Led by China, today's digital empires utilize technology, the Internet, social media, and artificial intelligence to transcend long-term imperial survival tactics.

6. ANTILOGUE IN THE WEST

It's already in use thanks to Silicon Valley. In China, they formalize and systematize what is already happening in the West.

6.1. Runet the Autonomous Network Of Russia

The Russian-controlled home internet (Rondeaux 2019) is identified with the official version of the "great firewall" and is aimed at state control of cyberspace. Its philosophy is to cut off Russia's connections to the World Wide Web and replace them with its own controlled "home internet," which could spark internal reactions. Runet, Russia's autonomous Internet, aims to repel attacks from abroad by reviving the "iron curtain on the internet" (Mounter 2019) to protect its national security (Pallin 2017:18) as a nuclear power (Rondeaux 2019).

The memory of the "encircled by imperialist forces" Soviet Union (Fakiolas 1998:78), according to the country's leadership is tangible (Napoleon's invasion, foreign invasion shortly after the October Revolution and the German invasion in the 1940s). The first truly invasive move aimed at controlling the Internet was in 2000. The Federal Security Service (FSB) began forcing Internet service providers (ISPs) to install monitoring equipment, known as SORM (Ognyanova 2015 :17). In 2012, the Russian state-owned Douma passed a bill that became known as the "Internet Blacklist Act." It blocked websites containing extremist material, child pornography, information related to illicit drug use, suicide techniques and other sensitive topics. The country plans to create its own Wikipedia and politicians have passed a bill banning the sale of smartphones that do not have preinstalled Russian software (Wakefield 2019).

6.2. "Russia Big Brother" - "Digital Westphalia"

Internet and telecommunications service providers are obliged to keep the data in their files due to fears of espionage, ideological diversion, control of strategic technologies, distribution of harmful viruses (Genieva 1997 :388). Proper government planning will reduce the relative cost of implementing it. Private intelligence can only be obtained by the intelligence services and law enforcement agencies with the approval of the judiciary, according to Putin. Concern over the return to the country of 4,500 Russian citizens joined in the Islamic State. In addition, any foreign company using personal data of Russian nationals outside the territory must transfer its servers to the territory of the Russian Federation, otherwise access to this type of source of information will be denied (Iosifidis & Wheeler 2016 :188). An obvious trend is the fight against tools to circumvent Internet censorship, such as virtual private networks, VPNs (Soldatov 2017:53).

6.3. The Russian Expenditure on the Internet

In Estonia, April-May 2007, Moscow's anger erupted when it decided to move the Bronze Soldier (Monument in honor of the fallen of the Red Army in World War II) (Liaropoulos 2013 :20). "Russia" attacked temporarily turning off Estonia's internet, a particularly fierce blow to the world's most internet-dependent economy. Distributed Denial of Service , DDoS, (Veratis 2015) attack focuses on government offices and financial institutions, blocking communications. In attacks with this technique, a large number (an 'army') of electronically infected PCs or systems attack other PCs, networks or systems. Russia has claimed that the attacks were carried out by "cyber-patriots" and were not conducted under the guidance of the Russian government. Similar movements in Lithuania, Georgia, Kyrgyzstan, Kazakhstan, Ukraine (New post 2017). Meanwhile, the use of the Internet is encouraged as a way of spreading government propaganda and disinformation (Iosifidis & Wheeler 2016 :188).

6.3.1. Internet: Digital Cold War

Attacks from both sides to interfere in elections, accusing Russia of involvement in the US elections in 2016. Claim returned by the Russian leader for American involvement in the elections in 2000 and 2012, with the participation of American diplomats and foreign NGOs (Stone 2019:265). Digital Armageddon, cyber war, possible electronic Pearl Harbor (Tai 2006 :93), avoiding "Internet Frankestain" (Nocetti 2015 :118) constant fear of the future. A "Cyber hotline" between the US and Russia was launched as a confidence-building measure as a need for immediate crisis management, June 2013.

6.4. Attack on Russia Bank System

Preparing a Botnet attack (Veratis 2015) by twenty countries targeting Russia's banking system against five to six large banks (Stone 2019:269) for destabilizing the banking system. The word "Botnet" was coined by "roBOT NETwork". An internet bot is a program that performs automated tasks over the internet. Also called web bot, web robot, WWW robot or just bot. Bots are very often used by hackers to coordinate and carry out cyber attacks on servers or for other purposes. Recommendation to citizens for calm and non-withdrawal of their deposits, without attributing responsibility to the US, as evidence is missing. Distributed denial of service, DDoS (distributed denial of service) attacks.

6.5. Cyber Attacks

Cyberspace, cybersecurity, cybercrime, cyberwarfare: About half a million cyber attacks are made every minute (Acs 2016:13). The "war landscape" is not adorned with weapons or bombs, but takes

place via a keyboard. The dimension of cyber warfare, along with social media and virtual realms, offer very economical tools of attack (Mavraganis 2019). The risk is equivalent to the 9/11 terrorist attacks, as it can paralyze the state (Liaropoulos 2013 :23) if it touches on key areas, such as critical infrastructure and national security systems. Cyber-attacks, which include hybrid threats, include attacks on the water and electricity system, the banking system, critical infrastructure, public institutions, local and central authorities, and national security systems. Cyber warfare tools may include espionage, assault, and manipulation (Konstantopoulos 2020 :12).

6.6. Snowden Accusations

Surveillance by the US National Security Agency, according to the testimony of Edward Snowden (Fang 2018 :418), PRISM Scandal (Arsene 2016:138). First on the watch list is his homeland, second is Russia. Reform-oriented complaints by Congress have been positive, while mass surveillance has been deemed illegal by the courts (Stone 2019 :78). Implanting malware (Astanastas 2015) in Japan on civilian infrastructure (Stone 2019 :266), e.g. railway stations, power plants in case the Land of the Rising Sun changes camp, according to his complaints. Malware: the word is complex and comes from malicious software, i.e. in Greek "malware". This includes any software that "runs" on a computer (or mobile device, e.g. smartphone, tablet) and has "bad intentions".

6.7. Stuxnet

A complex computer virus - the worm (Veratis 2015)- appeared in June 2010. Software worms work in a way that resembles that of viruses, because they are transmitted from PC to PC. But unlike viruses, software 'worms' have the ability to travel without the help of people, taking advantage of the data transfer and movement of files within the network. They reproduce themselves within the system, freeing up the available memory. Ability to increase pressure inside nuclear reactors, while not arousing suspicion. Differentiating the speed of the centrifugal forces, resulting in their destruction in Iran. Generated from code can lead to power outages. It is alleged that Israel and the United States were involved in the creation of the digital bomb (Pavlikkas 2019).

7. Answer To The Challenge

United Nations Human Rights Council Resolution of 5 July 2012, entitled "The promotion, protection and enjoyment of human rights on the Internet", which upholds the freedom of the Internet as a fundamental human right. Condemns Internet outages by national governments, e.g. Turkey, India (Stoycheff & Nisbet 2016).

The NATO Center for Excellence in Cooperative Cyber Defense in Tallinn, Estonia has set up Rapid Reaction Cyber teams (Hellenic National Defence General Staff 2015). The Cooperative Cyber Defense Center of Excellence is the certified NATO body involved in research, training and capacity building in the field of Cyber Defense. A cyber attack is capable of triggering Article 5 on Collective Security.

7.1. Five Security Pillars in Cyberspace

Cyber security is founded on the following five pillars: Training and awareness, Planning and preparing for a possible cyber attack, detecting and repairing damage, sharing experience and collaboration, ethics and certification in terms of mentality and motivation. There may exist "white" (Acs 2016 :58) hat hackers, developers who hack systems to test their capabilities and report vulnerabilities to the authorities for correction and "black" hat hackers, developers who hack systems to test their services in order to exploit vulnerabilities for personal or financial benefit.

8. Rare Earth

Critical parameter is the possession and exploitation of rare earths elements, which are required for hundreds of modern applications, such as mobile phones, laptops. Utilized in defense technology and green energy. Rare earths refer to the 15 minerals of the lanthanide series, in combination with the chemically similar yttrium and occasionally scandium (Chen & Zheng 2019:1). China controls approximately 97% of the global rare earth market (Hurst 2010:3). Until 1970, California had the upper hand.

Unique treasure: The biggest concern of the international community is the lifting of the restriction or no further reduction of China's export rates, after the crisis that broke out in 2010, near the Spratly

Islands (Council on Foreign Relations). Rare earths will be the cause of 21st century wars (Mpoukouvala 2017).

9. HOFSTEDE CULTURAL DIMENSIONS THEORY

It was developed on the occasion of a series of surveys conducted by Geert Hofstede among IBM employees located in a variety of countries. Each people is governed by special characteristics in the culture, which is summarized in 6 points dimensions (Business Mentor).

Power Distance Index (PDI): Demonstrates the degree of acceptance of power relations (or not) between members of a society. In countries with a high power index, hierarchical relationships are considered normal, while in countries with a low power index, this is not easily accepted. In Chinese society, inequalities between people are acceptable and hierarchy is fully respected (Hofstede Insights 2021). In Russia, there is a strong centralized administration from top to bottom. The uniqueness of people implies their inequality in the degree of power and is linked to the degree of acceptance of discrimination.

Individualism (IDV) versus collectivism: Indicates the degree to which a society is organized into groups. In China, the collectivist culture prevails, with an emphasis on the group. In collective societies, people belong to "formations" that care for them in exchange for their faith. Russia is governed by a team spirit, as relations are vital to obtaining information and successful negotiations (Hofstede Insights 2021). In the US, individual orientation is more pronounced and hierarchy is created for ease of access.

"Masculinity" (MAS) against "femininity": Determines the degree to which a society prioritizes "quantity of life" (male) over quality of life (female). China is seen as a male-dominated, success-oriented society at the expense of leisure or family warmth. In Russia there is a devaluation of personal achievements, modesty, unacceptable dominant behavior, with the exception of the professional arena. American society is riddled with competition, success as the winner. Basic principles and values are indicated in the terms "try to be the best they can" and "the winner gets everything", manifesting an arrogance.

The Uncertainty Avoidance Index (UAI): It outlines the degree of tolerance of a society towards "uncertainty and ambiguity". China treats laws and regulations with flexibility, as it is distinguished by an ambiguity, which is also reflected in their language. Uncertainty about the future has led the Russian people to create one of the most complex bureaucracies in the world. In their communication with foreigners they are considered very formal and distant. In the US, the prevailing cultural standard is reflected as a satisfactory degree of acceptance for new ideas, innovative products and a willingness to accept modernity. Not many rules are required and they are less emotionally expressive than other ethnicities. Intense fear has gripped American society since 09/11.

The long-term orientation (LTO) versus the short-term: Indicates the degree to which a society is oriented towards the future or the present. China is governed by a realistic culture and a long-term definition. The truth depends on the historical context, the time. They show flexibility in changing conditions, a strong tendency to save, invest, dedicate and persevere in achieving results. Russia's choice goes hand in hand with China's in this area. Americans are not realistic and practical, they are driven by strong beliefs about thorny issues such as abortion, drug use, euthanasia, and business performance measurement is implemented on a short –term basis.

Indulgence vs. Restraint (IVR): Demonstrates the extent to which members of a society try to control their desires and impulses. China is seen as a restrained society, ruled by cynicism and pessimism, restraint of actions by social norms, and performance is somewhat misjudged. Due to the restrained nature of Russian culture, there is a tendency towards cynicism and pessimism, not an emphasis on leisure and lack of control over the satisfaction of desires, restraint of actions by rules and a view of performance somewhat wrong. In the US, society is characterized as lenient, states wage war on drugs, but drug addiction exists. It forms a prudent society, but a portion of immoral people is not lacking (Hofstede Insights 2021).

10. THUCYDIDE TRAP

When an emerging power threatens to displace a dominant power, the trap of Thucydides emerges (Allison 2020:11 & 16). According to Paul Kennedy, "empires, hegemonic or number one forces

(whichever term one prefers) rarely if ever collapse in a rapid and spectacular way. Instead, they "slip" slowly down, trying to avoid conflicts, bypassing the growing obstacles, making offers, always looking for a flatter and calmer landscape (Tzifakis 2012). In the History of the Peloponnesian War, the rise of Athens and the fear it caused in Sparta is recorded as its cause, a fact that made the war inevitable. According to the study by Professor Graham Allison, twelve rivalries ended in war and four avoided it. In the seventeenth case, a strong and rising China is in conflict with sovereign America. But if China does not limit its ambitions or Washington does not agree to share its lead in the Pacific, then a trade dispute, a cyber attack or an accident at sea could spark a major war (Allison 2020, Back cover). Key requirement is its avoidance.

11. CONCLUSION

If the 20th century was defined by the fight for freedom of information against censorship, the 21st century will be defined by malicious entities, states or companies that abuse the right to freedom of information (Puddington 2017:15). A battle of values and ideas emerges. If these rivalries escalate into a war of the great powers it is perhaps the central issue of the geopolitics of the twenty-first century (Brands 2018:61-114). In an aversion to his speech, former US President John F. Kennedy in his inaugural address after his inauguration on 01/20/1961 had pointed out "In the long history of the world, only a few generations have acquired the role of defending freedom at the time of greatest danger. I do not abdicate this responsibility. I welcome it (Edel 2019) ". The biggest challenge at the gates.

BIBLIOGRAPHY

[1] Acs, 2016, Cybersecurity, Threats, Challenges, Opportunities, p11.

[2] Allison, Graham, 2020, In the Trajectory of War Can the US and China Avoid the Trap of Thucydides? Scientific Editing by Gofas Andreas, Kairidis Dimitris, Translated by Makropoulou Loukritia, Pedio, Athens, p.11, 16, (In Greek).

[3] Arsène, Séverine, 2016, Global Internet Governance in Chinese Academic Literature, Rebalancing a Hegemonic World Order?, China Perspectives, p26.

[4] Astanastas, Eftychios, 2015, Virus (malware) and Malware (malware) are the same? Safer Internet.gr, https://www. safer-internet.gr/virus-or-malware/, (In Greek).

[5] Bakardjieva, Maria,2005, Internet Society The internet in everyday life, SAGE Publications, London Thousand Oaks New Delhi, p 1.

[6] Brands, H. (2018), "Democracy vs Authoritarianism: How ideology shapes great-power conflict", Survival, 60 (5): 61-114.

[7] Business Mentor, The theory of Hofstede & what it says about the Greeks, https://www.businessmentor.gr/wp-content/uploads/2015/06/hofstede.pdf, (In Greek) .

[8] Cheila, Eirini & Ziogas, Christos, 2017, Which international community are we talking about? Exploring its limits in the cases of the Syrian and Ukrainian crisis, http://www.lecourrierdiplomatique.eu/2017/10/gia-pia-diethni-kinotita-milame/, (In Greek).

[9] Chen, Yufeng & Zheng, Biao, 2019, What Happens after the Rare Earth Crisis A Systematic Literature Review, Section Economic and Business Aspects of Sustainability, p1.

[10] Council on Foreign Relations, China's Maritime Disputes 1895-2020, https://www.cfr.org/timeline/chinas-maritime-disputes.

[11] Edel Charles, 2019, "Democracy Is Fighting For Its Life. Around the world political freedom isn't just slipping away-it's getting dragged down by fervent enemies", Foreign Policy, https://foreignpolicy.com/2019/09/10/democracy-is-fighting-for-its-life/.

[12] Fakiolas, Efstathios, 1998, Continuity and Change in Soviet and Russian Grand Strategy, Mediterranean Quarterly, 9 (2), 76-91, p78.

[13] Fang, Binxing, 2018, China's Declaration of Cyberspace Sovereignty in: Cyberspace Sovereignty. Springer, Singapore. https://doi.org/10.1007/978-981-13-0320-3_6, p173.

[14] French, Howard, 2019, China Is Pursuing Its Own 'Decoupling' From the U.S. Through the Internet ,https://www.worldpoliticsreview.com/articles/28386/china-s-protectionism-online-is-driving-its-own-decoupling-with-the-u-s.

[15] Genieva, Ekaterina, 1997, Legal Aspects of the Internet, The International Information & Library Review, Volume 29, Issues 3–4, p 381–392:382.

[16] Hellenic National Defence General Staff, 2015 Participation of the ED in the NATO Center of Excellence for Cyber Defense in Estonia, 2015, https://geetha.mil.gr/6321-symmetochh-twn-ed-sto-kentro-aristeias-toy-nato-gia-thn-kybernoamyna-sthn-esthonia/.

[17] Hofstede-insights, 2021, What about China?, https://www.hofstede-insights.com/country-comparison/china/.

[18] Hofstede-insights, 2021, What about Russia?, https://www.hofstede-insights.com/country-comparison/russia/.

[19] Hofstede-insights, 2021, What about the USA?, https://www.hofstede-insights.com/country-comparison/the-usa/.

[20] Hurst, Cindy, 2010, China's Rare Earth Elements Industry: What Can the West Learn, Institute for the Analysis of Global Security (IAGS), p3.

[21] Iosifidis P.& Wheeler M, 2016, Russia and China: Autocratic and On-line, in: Public Spheres and Mediated Social Networks in the Western Context and Beyond. Palgrave Global Media Policy and Business. Palgrave Macmillan, London, p12-13.

[22] Kathimerini, 2019, No known foreign search engine in China, https://www.kathimerini.gr/1006325/article/texnologia/diadiktyo/kamia-gnwsth-3enh-mhxanh-anazhthshs-sthn-kina,2019 (In Greek).

[23] Kendall-Taylor, A.& Frantz, E. & Wright, J. (2020), "The Digital Dictators. How technology strengthens autocracy", Foreign Affairs, https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators.

[24] Konstantopoulos, Ioannis, 2020, Hybrid War and Information, Air Force Review, Issue 118, p. 12, (In Greek).

[25] Li, Jane, 2019, Getting a new mobile number in China will involve a facial-recognition test, Quartz, https://qz.com/1720832/china-introduces-facial-recognition-step-to-get-new-mobile-number/.

[26] Liaropoulos, Andrew, 2015, Cyber-Security A Human-Centric Approach, Proceedings of the 14th European Conference on Cyber Warfare & Security University of Hertfordshire Hatfield, UK, p192.

[27] Liaropoulos, Andrew, 2013, Exercising state sovereignty in cyberspace: An international cyber-order under construction, Journal of Information Warfare, Volume 12, lssue 2 :19-26, p 20.

[28] Liaropoulos, Andrew, 2013, The Challenges of Social Media Intelligence for the Intelligence Community, Journal of Mediterranean and Balkan Intelligence, 1, 1, p5.

[29] Macedonia, 2019, China "strangles" the internet. Promotes actions to create an impenetrable cyber defense system, https://www.makthes.gr/i-kina-straggalizei-to-diadiktyo-188566, (In Greek).

[30] Mavraganis, Costas, 2019, Ioannis Konstantopoulos: The targets of hybrid threats are societies and not armies, https://www.huffingtonpost.gr/entry/ioannes-konstantopoelos-stochoi-ton-evridikon-apeilon-einai-oiin- -kai-ochi-oi-stratoi_gr_5cbee6ffe4b0f7a84a74b9e2? plj, (In Greek).

[31] Mikelis, Kyriakos, 2018, Misinformation and conspiracy theories: The prism of International Relations, University of Macedonia, Institute of International European & Defense Analysis, Working Paper No1 / 18-19, (In Greek).

[32] Mounter, Ulf, Edited by Papadimitriou, Giannis, 2019, Russia wants its own…Internet, https://www.dw.com/el/%CE%B7-%CF%81%CF%89%CF%83%CE%AF%CE%B1-%CE%B8%CE%AD%CE%BB%CE%B5%CE%B9-%CE%B4%CE%B9%CE%BA%CF%8C-%CF%84%CE%B7%CF%82-%CE%AF%CE%BD%CF%84%CE%B5%CF%81%CE%BD%CE%B5% CF%84/a-51084493.

[33] Mpoukouvala, Chrysoula, 2017, The rare earths cause of wars of the 21st century., Aperopia, https://aperopia.fr/09-2017/i-spanies-gaies-aitia-polemon-tou-21ou-aiona/, (In Greek).

[34] Nathan, Andrew, 2018, Capsule Review, Censored: Distraction and Diversion Inside China's Great Firewall by Margaret E. Roberts.

[35] New post, 2017, The Russian invasion of the internet - The chronicle of cyber attacks, New post, https://newpost.gr/kosmos/583201/to-xroniko-twn-rwsikwn-kybernoepithesewn, (In Greek) .

[36] O'Brien Danny, 2019, China's Global Reach: Surveillance and Censorship Beyond the Great Firewall, https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall.

[37] Ognyanova, Katherine, 2015, Careful What You Say: Media Control in Putin's Russia – Implications for Online Content. International Journal of E-Politics, 1(2), p17.

[38] Pallin Vendil, Carolina, 2017, Internet control through ownership the case of Russia, Post-Soviet Affairs, 2017 Vol. 33, No. 1, 16–33, http://dx.doi.org/10.1080/1060586X.2015.1121712, p18.

[39] Pavlikkas, Marinos, 2019, The end of the free internet, https://simerini.sigmalive.com/article/2019/11/17/to-telos-tou-eleutherou-diadiktuou/, (In Greek).

[40] Pelevani, M. (2019), "How the Black Mirror Applies in China", Tvxs, https://tvxs.gr/news/kosmos/pos-black-mirror-efarmozetai-stin-kina, (In Greek).

[41] Polyakova Alina & Meserole, Chris,2019, Exporting digital authoritarianism The Russian and Chinese models, Brookings, https://www.brookings.edu/research/exporting-digital-authoritarianism/.

[42] Puddington, A. (2017), "Breaking down Democracy: Goals, strategies and methods of modern authoritarians", Freedom House, σ. 7.

[43] Rondeaux, C. 2019, "Why Russia's Attempt to Create Its Own Tightly Controlled Internet Could Backfire", World Politics Review, https://www.worldpoliticsreview.com/articles/28313/why-russia-s-attempt-tocreate-its-own-tightly-controlled-internet-could-backfire .

[44] [44] SecNews, 2014, Which countries have banned Social Media?, https://www.secnews.gr/122848/social-media-bans/,(In Greek) .

[45] Soldatov Andrei, 2017, The Taming of the Internet, Russian Social Science Review, vol. 58, no. 1 "Media Studies,Taylor & Francis Group, LLC, p53.

[46] Stone Oliver, 2019, Interview with Putin, Translated by Papadakis Konstantinos, Oxy, Athens, p. 265, (In Greek).

[47] Stoycheff, Elizabeth & Nisbet, Erik, 2016, Is internet freedom a tool for democracy or authoritarianism?, The Conversation, https://theconversation.com/is-internet-freedom-a-tool-for-democra cy-or-authoritarianism-61956.

[48] Tai, Zixue, 2006, The Internet in China, Cyberspace and civil society, Routledge Studies in New Media and Cyberculture, Routledge Taylor & Francis Group, New York London, page xxii.

[49] Tzifakis, Nikolaos (2012), Change in International Politics: An Introduction to the Contemporary Debate in Tzifakis, Nikolaos International Politics in Times of Change, The Konstantinos Karamanlis Institute for Democracy series on European and International Affairs, Centre for European Studies Publications, Springer, Series editor Konstantina E. Botsiou, Athens.

[50] Uchill, Joe (2019), Russia and China get a big win on internet sovereignty, axios, https://www.axios.com/russia-china-united-nations-internet-sovereignty-3b4c14d0-a875-43a2-85cf-21497723c2ab.html.

[51] Veratis, Christos, 2020, 5G Network and US-China Geopolitical Games, Center for International Strategic Analysis, https://kedisa.gr/%ce%b4%ce%af%ce%ba%cf%84%cf%85%ce%bf-5g-%ce%ba%ce%b1%ce%b9-%ce%b3%ce%b5%cf%89%cf%80%ce%bf%ce%bb%ce%b9%cf%84%ce%b9%ce%ba%ce%ac-%cf%80%ce%b1%ce%b9%cf%87%ce%bd%ce%af%ce%b4%ce%b9%ce%b1-%ce%b7%cf%80%ce %b1/, (In Greek).

[52] Veratis, Christos, 2015, Cyberspace- Cyber-attacks- Cyber defense-Part 2 (malicious programs - attack techniques), Center for International Strategic Analysis, https://kedisa.gr/kybernoxwros-kybernoepitheseis-akberosolaos- -epithesewn /, (In Greek).

[53] Wakefield, Jane (2019), Russia successfully tests its unplugged internet, BBC, https://www.bbc.com/news/technology-50902496.

[54] Weber, Valentin, 2019, The Worldwide Web of Chinese and Russian Information Controls, Centre for technology & Global Affairs, University of Oxford, Working Paper Series, p3.

[55] Xu Xueyang & Mao, Z. & Halderman, J, 2011, Internet Censorship in China Where Does the Filtering Occur, International Conference on Passive and Active Network Measurement, pp 133-142: 133.

[56] Ziccardi, Giovanni, 2012, Digital Activism, Internet Control, Transparency, Censorship, Surveillance and Human Rights: An International Perspective, Chapter 6, p201.

[57] Zucchi, Kristina, 2019, Why Facebook Is Banned in China & How to Access It China's "Great Firewall" is a disruptor in the social media sector, https://www.investopedia.com/articles/investing/04 2915/why-facebook-banned-china.asp.

Citation: *Eirini Sotiriou. "Internet, Cyber Attacks, Rare Earths: Sino-Russian Confrontation with the West" International Journal of Political Science (IJPS), vol 7, no.1, 2021, pp. 25-33. doi: https://doi.org/10.20431/2454-9452.0701003.*