Conceptualising Cyber Sovereignty And Information Security: China's Image Of A Global Cyber Order

Muhammad Nadeem Mirza, Lubna Abid Ali, Irfan Hasnain Qaisrani

Webology (ISSN: 1735-188X)
Volume 18, Number 5, 2021

Conceptualising Cyber Sovereignty And Information Security: China's Image Of A Global Cyber Order

Muhammad Nadeem Mirza[1] , Lubna Abid Ali[2] , Irfan Hasnain Qaisrani[3]

[1]Faculty Member School of Politics and International Relations, Quaid-i-Azam University Islamabad, Pakistan. ORCID: https://orcid.org/0000-0002-2196-9174

[2]Dean, Faculty of Contemporary Studies, National Defense University Islamabad, Pakistan.

[3]Faculty Member Department and Humanities and Social Sciences Bahria University Islamabad, Pakistan.

Abstract

Cyber sovereignty means that states have authority within a fixed boundary to devise rules, laws, and norms about behaviour of individuals, institutions, applications, and other actors and factors in the cyberspace. This idea is intrinsically associated with information security propagated by China, which is a broader concept and is not only limited to defending networks, computers, and confidentiality – dealt by the Western idea of cyber security – but also includes controlling and filtering content in the cyberspace and the communication tools, especially the ones that may damage the government and create schisms in the society. China's ultimate objective remains to try to establish a multilateral global cyber order – within the ambit of rule of law – based upon nationalised cyberspace, mutual respect, non-interference in the internal affairs of other states, cyber sovereignty, and mutual honour. An order based upon the principles of equality and justice where every state, small or big, will be having fair share in the management of the cyberspace. This is an exploratory and explanatory study conducted using content analysis in which data is drawn from primary and secondary sources. It tries to conceptualise the idea of China's cyber sovereignty and notes that how is China utilising it to make the cyberspace in its image and develop a global cyber order – in stark contrast to the Western and US image of the cyber order.

Keywords: Cyber Sovereignty, Global Cyber Order, Information Security, Cyber Security, National Internet, Nationalised Cyberspace.

Introduction

There are around 6.26 billion smartphone subscribers and 4.66 billion active internet users in 2021 (Internet users in the world, 2021; Smartphone users, 2021), that makes around 60 plus percent of the world population. While use of cell phones and internet has eased the lives of individuals, it has also created a dilemma for states to ensure that users' privacy, safety, and security remains intact. Smart phones aside, there are around 75 to 100 billion electronic devices connected with the internet – Internet of Things (IoT). Though this provides immense opportunities for the users, yet also creating incentive for some actors to exploit those opportunities. Internet connected devices can be hacked by actors to steal confidential and personal information, monitor activities, disrupt functioning of the devices, and force them to function differently as is intended by the disrupter. Not only they steal and damage, but those actors can even make use of the internet to launch information operations intended for influencing or even engineering public opinion, affecting electoral processes, bringing down morale of the people, fanning cleavages within the society with the intention of causing damage to the national cohesion, creating mistrust about institutions of the state, creating distrust between intuitions and fanning hatred among the society.

Most important actor involved in the cyber-attacks remains the state or state sponsored individuals and institutions. States steal, conduct espionage, damage, and attack other states. Geneva Internet Platform noted that there were around 53 states in 2021 which were either having or are developing cyber offensive capabilities (Gavrilović, 2021). Israel and the United States have continuously been involved in conducting cyber-attacks against Iran. Similarly, Israel's NSO Group developed zero-click Pegasus spyware and sold it to different states. It was found in the mobile phones and systems of thousands of political dissidents and allies alike, through most of the world. The software was even used by Israel itself. Pressure on Hungarian government is mounting to launch independent investigations about its use of Pegasus against opposition members and journalists (F-24, 2021). The software was found in the mobile phones of several US Department of State officials – several US agencies had also bought this spyware. Individuals of interest for the Pegasus customers included "French President Emmanuel Macron, Iraqi President Barham Salih and South African President Cyril Ramaphosa. Also on it are seven former prime ministers and three current ones, Pakistan's Imran Khan, Egypt's Mostafa Madbouly and Morocco's Saad-Eddine El Othmani. King Mohammed VI of Morocco also is on the list". That makes 3 presidents, ten prime ministers, and a king who have been the target of spying by Pegasus (Timberg et al., 2021). Use of Stuxnet to sabotage Iranian nuclear program is another example of how the states have adopted the new mode of warfare in the cyberspace (Farwell & Rohozinski, 2011).

India in 2013 launched an information and cyber operation – known as Patchwork – with the purpose of espionage, and data theft targeting Pakistan, Sri Lanka, Bangladesh, the United States, and several other countries. Similarly, it is alleged that Pakistan also launched several attacks against India such as Mythic Leopard in 2018 (CS, 2021), Stealth Mango and Tangelo in 2018 (O'Neill, 2018), and APT36 in 2020 (Team, 2020). Moreover, Russia had successfully launched a successful cyber campaign again Georgia during 2008 Russo-Georgia war and

against Ukraine during Crimean crisis (Babar & Mirza, 2020; CCDCOE, 2021; Deibert et al., 2012). The United States faced a crisis in its 2016 elections when Russia allegedly interfered in its electoral process by influencing the voters' behaviour and choices through extensive use of the cyber operations. US Department of Justice report found that the Russian Internet Research Agency (IRA) had started "information warfare" in and against the United States well before the elections with the objective of sowing "political and social discord" within the American society (Mueller, 2019). The operation soon was transformed into a project of discrediting Democratic candidate Hillary Clinton in favour of Republican candidate Donald Trump. Russians hacked computers and accounts related with the Democratic Party and leaked selected data to the public in order to successfully discredit Clinton (Mueller, 2019). Investigating Committee found that "Moscow's intent was to … undermine the U.S. democratic process" (Hosenball, 2020). Immediately after the elections US expelled 35 Russian diplomats over charges of cyber operations. US agencies claim that Russia has been involved in the cyber espionage since more than a decade (BBC, 2016). Similarly, the United States again expelled 10 Russian diplomats and sanctions 32 individuals and entities accusing them of hacking and trying to affect the 2020 elections. President Biden notes that "We cannot allow a foreign power to interfere in our democratic process with impunity" (Tucker & Madhani, 2021). United States is not only the target but is also the biggest cyber power in the world having both offensive and defensive capabilities (Marks & Schaffer, 2021; Pomerleau, 2021). It remained engaged in cyber-espionage of the friends and foes alike – and ironically considered it as its right to do so, what China and Russia considers a cyber hegemony. In parallel to the Biden statement, we have a similar statement from China whose 2017 International Strategy of Cooperation on Cyberspace note that "China firmly opposes any country using the Internet to interfere in other countries' internal affairs" (Department of Arms Control, 2017).

In response to the cyber-attacks carried out throughout the world by the states, state-sponsored actors, lone individuals, and non-state actors a big debate has started that the internet should be controlled, contained, and filtered to ensure that only correct information reaches the user. States are in a catch-22 situation here. On the one hand, it intends to ensure that its citizens and institutions remain secure from the cyber threats, which demands it to put certain restrictions on the flow of information, curtailing some features of the softwares, binding cyber applications to follow certain national rules and conditions, and regulating behaviour of certain individuals and organisations. On the other hand, it also wishes internet to remain freely available to everyone with easy and open access to the flow of information without any restrictions.

These two positions are advocated by two groups of the states led by the United States and China. China has been advocating for a more splintered cyberspace where states would be exercising their sovereignty – sovereignty in the cyberspace, just like territorial sovereignty. Ideas such as data localization and nationalization, information filtering, and state control over the cyberspace created huge appeal in the United Nations members already facing the onslaught of cyberattacks, misinformation campaigns, data theft, espionage. China, with the support of Russia, has been quite successful in developing and propagating this conception of cyber

sovereignty. China considers any state to be independent in passing its domestic rules and laws to regulate the cyberspace in pursuit of its national interest. China specifically criticises any attempt by the United States or any state that tries to interfere or criticise these domestic rules or laws, considering them to be a violation of the state sovereignty. China specifically criticises the behaviour of the United States whom it considers is pursuing a cyber hegemony. President Xi Jinping notes, “No country should pursue cyber hegemony or interfere in other country's internal affairs" (DW, 2015). China is working for a global cyber order where the rule of engagement would be determined by the states in consultation with each other and not by only one state – the United States.

The second position of having an open and global internet is supported by the United States. A transnational cyberspace fulfils the American national interests in the political, economic, security, and cultural perspectives. This is so because the United States holds the biggest sway over the management of the global cyberspace, something that is belittled by China and rising powers. China and Russia accuse other great power of using the open and globalised cyberspace as a tool to instigate rebellious behaviour in their societies. They, thus, are pushing an idea of cyber sovereignty which would help them protect and regulate their cyberspaces.

This study endeavours to conceptualise the idea of cyber sovereignty. What is cyber sovereignty and how is China utilising it to make the cyberspace in its image? How does China visualise information security and how is it different from cyber security? What are the objectives that China wishes to achieve through adopting and propagating the idea of cyber sovereignty? What is the Chinese image of a global cyber order? Why does West criticise the cyber sovereignty conception of China? This exploratory and explanatory study is conducted using content analysis in which data is drawn from the primary and secondary sources.

Cyber Security vs. Information Security

Cyberspace is “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form” (Hogan & Newton, 2015). Absence of the physical form often gives actors the advantage of anonymity. Nye noted that it provides anonymity to the actors who with a low cost can “exercise hard and soft power in cyberspace” more efficiently and easily “than in many more traditional domains of world politics” (Nye Jr., 2010).

Cybersecurity deals with protecting “confidentiality, integrity and assurance of data” (Segal, 2020). This objective can be achieved once states ensure that the communication transpiring in the cyberspace and networks integrated therein remain free from the threat of any unauthorised use. The United States usually builds upon the cybersecurity conception as compared to information security – the idea supported and propagated by China and Russia. Information security is a broader concept that is not only limited to defending networks, computers, and confidentiality but also includes controlling and filtering content in the cyberspace, and the communication tools, especially the ones that may damage the government and create schisms in the society (Segal, 2017). China, Russia, and four other states sponsored International Code of Conduct for Information Security (ICCIS) to the United Nations. The code asks states to

cooperate in order to contain information that may incite "terrorism, separatism or extremism" and also to not use the information and communication technologies for destabilising other states' political, economic, and social status (UNGA, Sixty-ninth session, Agenda item 91, 2015). China and Russia have expanded the scope of information security as compared to cyber security in order to control the flow of information that may cause damage to their regime stability. The United States' intelligence agencies have effectively utilised cyberspace to damage other states' stability. Contrarily Russia has also engaged in information operations against the United States. Moreover, domestic actors made effective utilisation of the cyberspace to spread disinformation against the governments and each other through social media (Fidler, 2017). Media and cyberspace which once were considered as one of the pillars of democracy are being manipulated by the rivals – state, individuals, and institutions. In order to address these challenge ICCIS re-affirmed the cyber sovereignty while noting that the internet-related issues remain the exclusive and sovereign right of the states (UNGA, Sixty-ninth session, Agenda item 91, 2015). Only cyber sovereignty can ensure information security of the states.

Cyber Sovereignty

Sovereignty simply means "supreme authority within a given territory" (Philpott, 2020). States are independent to make rules, laws, decisions, and their implementation within a given territory. Supreme authority means no actor – domestic and foreign – may force the state to make a particular law or decision contrary to its wish. Though sovereignty is about authority, yet states ensure that other states and its domestic populations consider its behaviour and existence legitimate. Sovereignty demands loyalty and its population will remain loyal only if state fulfils its basic functions efficiently and in concert with the needs and demands of the people.

Historically French scholar Jean Bodin defined sovereignty as the "supreme power over citizens and subjects, unrestrained by the laws" (Dunning, 1896). Thomas Hobbes also held similar conceptions and considered sovereign to be someone above all. Someone Who can make laws but cannot be subjected to the same laws (Dunning, 1896; Philpott, 2020). With the passage of time the concept of sovereignty which was ascribed to the person – a monarch usually – transferred to the state.

The transformation of sovereignty from an absolute to relative concept has transpired because of the dynamic nature of the international system, rise of transnational forces, processes associated with globalization, international institutions, Multinational corporations, and inter-governmental and non-governmental organisations and actors (Krasner, 2001a, 2001b). Still the Westphalian conception of sovereignty is something on the basis of which system and society of the states is being run. It remains the most potent force in the hands of the states to exercise their authority, challenge foreign actors and establish legitimate authority domestically – external and internal dimensions of sovereignty respectively (Brahm, 2004).

Taking cue from the territorial dimension of the sovereignty, cyber sovereignty implies that states have authority within a fixed boundary to devise rules, laws, norms, and behaviour of

individuals, organisations, applications, and other actors and factors in the cyberspace. Xi Jinping at the 2015 World Internet Conference in Wuzhen considered that cyber sovereignty means "respect the right of individual countries to choose their own path to cyber development, model of cyber regulation and participate on the same footing" (Xi Jinping quoted by Griffiths, 2015) – every country should have independent control over its own Internet (DW, 2015). China wishes to extend the sovereignty as is enunciated in the United Nations Charter to the cyberspace (Kolton, 2017).

In response to internet being the global and open platform dominated by the United States, Chinese conception of cyber sovereignty entails control over the information, infrastructure, and anything that is going on in the cyberspace. Every state has its own culture, traditions, values, rules, and laws, and has its own dearth for the information. Some information acceptable in the United States may not be acceptable and even against the cultural and indigenous values of China, or for that matter other states such as Saudi Arabia or Iraq. Sovereignty in the cyber space implies that the government can control, and censor information prevent access to the harmful and anti-indigenous information for the public. Data, China proposes, should be controlled by the state. China's 2010 Internet White Paper declares "Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected" (Information Office of the State Council, 2010). For the purpose of controlling information dissemination in China, it developed a system of controls what Western scholars call a Great Firewall.

China which remained defensive in the cyberspace through most of the 1990s and 2000s, has started asserting itself since mid 2000's. Entry of President Xi Jinping in the office furthered China's tough stance about management of the global cyberspace. He propagated that cyberspace is not beyond the rule of law and that no state should interfere in the internal matters of other states and create chaos therein using commination and information technology (Segal, 2015b).

Objectives of China's Conception of Cyber Sovereignty: Global Cyber Order

President Xi Jinping during a speech at the Second World Internet Conference outlined some of the principles that China wishes other states to pursue, specifically his conceptualisation of cyber sovereignty (Jinping, 2015):

1. States should respect cyber sovereignty of other states – sovereignty as a norm is the already established principle of the United Nations.
2. No states should try to pursue cyber hegemony and try to destabilise other states by create discord in the society using ICT (Information and Communication Technology).
3. States will be interacting with each based on sovereign equality.
4. Every state small or big has a right to adopt its own rule and regulations vis-à-vis cyberspace.
5. Every state should try to maintain "peace and security" in the cyberspace. Cyberspace should not become a "battleground" for states. Equally important remains the fact that it should not become "a hotbed for crimes." States need to ensure that cybersecurity

remain important for everyone – big and small states alike. He noted, "We cannot just have the security of one or some countries while leaving the rest insecure" (Jinping, 2015).

6. Openness and cooperation should be ensured between the states for the "cultivation of the good order." He noted that "Like in the real world, freedom and order are both necessary in cyberspace. Freedom is what order is meant for and order is the guarantee for freedom" (Jinping, 2015). Moreover, to have an order, it is a must to ensure that cyberspace should be run within the ambit of rule of law.

We, thus, can draw certain objectives of China's pursuance of the cyber-sovereignty conceptions.

1. First and foremost, objective remains securitising the state from threats of cyber-terrorism. It also intends to ensure that terrorist may not utilise cyberspace for communication, planning, and carrying out acts of sabotage.
2. It wishes to protect its ICT (Information and Communications Technology) from foreign interventions. China's traditional foreign policy principle of non-interference in internal affairs of other states applies to the cyberspace as well.
3. Other great powers, especially the United States held sway over the control of cyberspace. China remains wary of this American position and made it clear that it cannot accept cyber hegemony of any state. China's objective through cyber sovereignty remains to dimmish, control or limit the control of the United States in cyber space. The US has already made cyberspace in its image, now China is trying to shape the internet – at least within its own state – in its own image. This is possible only when it will be able to limit, roll back, or tarnish the image that is been established by the United Sates in the cyberspace.
4. China wishes to control and regulate the flow of information within the state in order to ensure its regime stability. Access to information that can instigate population against the government is strictly limited. Moreover, providing specific information to its population in order to establish and strengthen regime legitimacy also remains one of its prime objectives. For the purpose it has also drafted several laws to regulate cyberspace. China's 2017 International Strategy of Cooperation on Cyberspace notes that states "are entitled to administer cyberspace in accordance with law" (Department of Arms Control, 2017).
5. Another objective remains to expand China's regional and international clout in the cyberspace by supporting states facing cyber-threats specifically from the United States. Besides, rising populist leaders in the world led to the nationalistic policies which often result in containing and controlling the flow of information – coinciding with China's propagation of cyber sovereignty. China's ideas vis-à-vis cyberspace, thus, got huge acceptance in the world leading to the establishment of two blocs in the United Nations – one led by the United States and other led by China. Attraction for China's cyber-sovereignty ideas is specifically predominant in the developing states which are facing challenged to the domestic stability, as compared to the developed states, which have robust ICT security mechanism in place.

The catchwords for China, thus, are cyber sovereignty, cyber authority, non-interference in other states' cyberspace and issues, sovereign equality, and just and equitable cyber order. China considers cyberspace as important in the twenty-first century as maritime in the nineteenth and aerospace in the twentieth century. Nineteenth century predominance of Great Britain in the maritime space led to other states exploiting it for carving out China into spheres of influence – what is known as century of humiliation in China (Kaufman, 2010; Mirza et al., 2020; Mirza & Khan, 2020). Similarly, twentieth century predominance of the United States in the aerospace arena led to encirclement of China in the South China Sea and East China Sea. China does not want to repeat the humiliation in the twenty-first century and that can only be ensured by its predominance or at least independence in the cyberspace (Kolton, 2017).

Criticism on China's Conception of Cyber Sovereignty

Scholars, mostly associated with the West, have called the cyber sovereignty as a ruse to divert the attention away from the activities of the Chinese government. Freedom House, a US democracy watchdog for example, has considered that China is having one of the worst internet censorship policies in place. One of its reports noted that China is helping promote norms related to protectionism in the cyberspace (Shahbaz et al., 2020). In it states such as Turkey, India, Brazil, and the like are restricting the flow of information in the name of security of the users. Its 2020 report notes that China remained the world's worst abuser of the internet for the consecutive sixth year (FH, 2020b). Covid-19 provided states opportunities to abuse human rights. Several Artificial Intelligence tools were developed and used by the states for contact tracing through accessing the confidential data of the individuals (FH, 2020a). The report also notes that cyber sovereignty is on the rise in the world with several states, such as Russia, Brazil, Pakistan, Turkey, India, and even the United States, banning specific sites and applications. Some of these states also passed legislations to 'nationalise the internet' and give access to governmental agencies to access private and confidential data of the population (FH, 2020a). China is also criticised for the establishment of "Great Firewall" over the internet which "implements many different types of censorship and content filtering to control China's Internet traffic" (Ensafi et al., 2015). China is accused of rewriting the rule of internet in the guise of ensuring safety, security, and sovereignty of the state (DW, 2015).

Conclusion

Advent of the internet, and proliferation of several softwares and applications has given rise to a precarious situation where one individual using merely 140 characters – on Twitter for example – can cause the unavoidable damage to one's own or other state, organisation, or individuals. Where internet and cyberspace have brought positive change in the lives of the actors, there it has also become a tool in the hands of other actors to steal information and private data, sabotage infrastructure of other states, sow seeds of discords in the societies, and even paralyse other states' economies (Segal, 2015a). States have been cooperation with each other in the cyberspace while ironically the same states – often allies – have been engaged in the theft and exploitation of the cyberspace against each other. The United States being the biggest cyber power of the world has remained engaged in cyber espionage against friends and

foes alike. Hacking governmental accounts, leaving trojan houses, and infesting networks with the unwanted and incorrect information remains the main types of the cyber-attacks by one state against the other state. Edward Snowden's revelations brought the United States face to face against several of its own allies (BBC, 2014). United States has utilised open internet, social media campaigns, and big data to launch even regime change programs in other states. China's Xinjiang, Iran, Syria, North Korea are few of the examples. Regime change earlier required use of military force, now the US could simply utilise the free internet to create dissent in the society and instigate rebellious behaviour against other states, governments, regimes, institutions, and individuals.

Similarly, China and Russia have been cooperating with each other in almost every domain of the state's life, yet there exists huge trust deficit between the two. Western sanctions on Russia left it with no option, but to cooperate with China in accessing the technology especially that is been offered by Huawei. Also, the fact remains that the United States has no such company that can challenge and offer alternative in place of the equipment developed by Huawei. China's Huawei provides technical equipment to critical Russian infrastructure and industries especially in the ICT sector. China's developing 5G networks in Russia and other areas usually considered as the Russian sphere of influence, such as the Central Asia may create tensions between the two. Similarly cyber-attacks by Chinese hackers against "Russian industries, including defense, nuclear, and aviation" have increased tremendously in the recent past – thus infuriating Russians on the issue (Segal, 2020). Yet, overtly, they have signed several bilateral agreements to enhance cooperation in the cyberspace and have been engaged in promoting cyber sovereignty at different regional and internal fora, such as, the United Nations, Shanghai Cooperation Organisation, and the like. They have developed a pool of the like-minded states who have been cooperating in developing rules and norms that can be used to run the global cyberspace based upon nationalised internet.

Century of humiliation conception of China has affected its policy making processes and China intends to not lose the opportunity of cyberspace leadership in the twenty-first century. It has challenged the US dominated global cyber order by offering an appealing order based upon nationalised cyberspace, mutual respect, non-interference in the internal affairs of each other, cyber sovereignty, and mutual honour. Xi Jinping calls for a multilateral cyber order in the world. He notes, "There should be no unilateralism … Decisions should not be made with one party calling the shots or only a few parties discussing among themselves" (BBC, 2015). He furthered stressed that states should avoid pursuing arms race in the cyberspace. China and Russia have also been wary of the US behaviour of naming and shaming other states with the accusations that state-backed hackers have launched attacks against it. It sanctioned 5 officials of Chinese PLA of being involved in the cyber-attacks against US and its companies. "In all these cases attribution included a mix of private security company reports and US government releases of threat information and attack data. While the US government has gradually argued that it is getting better at attribution, the Chinese government has been consistent that such efforts often are 'unprofessional' and 'unscientific'"(Segal, 2017). The United States, on the other hand, has always looked towards China's intentions and actions with scepticism. It

wished to maintain a global and open internet for all, because that is exactly what serves its strategic, political, economic, military, and cultural interests.

References

Babar, S. I., & Mirza, M. N. (2020). Indian Hybrid Warfare Strategy: Implications for Pakistan. Progressive Research Journal of Arts and Humanities, 2(1), 39–52.

BBC. (2014, January 17). Edward Snowden: Leaks that exposed US spy programme. British Broadcasting Corporation News. https://www.bbc.com/news/world-us-canada-23123964

BBC. (2015, December 16). China internet: Xi Jinping calls for 'cyber sovereignty'. British Broadcasting Corporation News. https://www.bbc.com/news/world-asia-china-35109453

BBC. (2016, December 29). US expels Russian diplomats over cyber attack allegations. British Broadcasting Corporation News. https://www.bbc.com/news/world-us-canada-38463025

Brahm, E. (2004, September). Sovereignty. Beyond Intractability. https://www.beyondintractability.org/essay/sovereignty

CCDCOE. (2021, September 17). Georgia-Russia conflict (2008). International Cyber Law: Interactive Toolkit. https://cyberlaw.ccdcoe.org/wiki/Georgia-Russia_conflict_(2008)

CS. (2021). Adversary: Mythic Leopard - Threat Actor. Crowdstrike Adversary Universe. https://adversary.crowdstrike.com/en-US/adversary/mythic-leopard/?L=168/

Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. Security Dialogue, 43(1), 3–24.

Department of Arms Control. (2017). International Strategy of Cooperation on Cyberspace. Ministry of Foreign Affairs of the People's Republic of China. https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html

Dunning, Wm. A. (1896). Jean Bodin on Sovereignty. Political Science Quarterly, 11(1), 82–104. https://doi.org/10.2307/2139603

DW. (2015, December 16). Chinese President Xi defends national sovereignty online. Deutsche Welle. https://www.dw.com/en/chinese-president-xi-defends-national-sovereignty-online/a-18920705

Ensafi, R., Winter, P., Mueen, A., & Crandall, J. R. (2015). Analyzing the Great Firewall of China over space and time. Proceedings on Privacy Enhancing Technologies, 2015(1), 61–76.

F-24. (2021, July 23). Talking Europe - 'Hungary must allow independent investigation' on Pegasus spyware: Top MEP Manfred Weber. France 24. https://www.france24.com/en/tv-shows/talking-europe/20210723-hungary-must-allow-independent-investigation-on-pegasus-spyware-top-mep-manfred-weber

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. Survival, 53(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

FH. (2020a). Report: Global Internet Freedom Declines in Shadow of Pandemic. Freedom House. https://freedomhouse.org/article/report-global-internet-freedom-declines-shadow-pandemic

FH. (2020b). Report: Amid Global Decline, China Remains World's Worst Abuser of Internet Freedom in 2020. Freedom House. https://freedomhouse.org/article/report-amid-global-decline-china-remains-worlds-worst-abuser-internet-freedom-2020

Fidler, D. P. (2017, October 18). Requiem for the Internet Freedom Strategy. Council on Foreign Relations. https://www.cfr.org/blog/requiem-internet-freedom-strategy

Gavrilović, A. (2021, June 6). What's new with cybersecurity negotiations? The UN GGE 2021 Report. Diplo. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-un-gge-2021-report/

Griffiths, J. (2015, December 16). Chinese President Xi Jinping: Hands off our Internet. CNN. https://www.cnn.com/2015/12/15/asia/wuzhen-china-internet-xi-jinping/index.html

Hogan, M., & Newton, E. (2015). Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (NIST IR 8074v2). National Institute of Standards and Technology - NIST. https://doi.org/10.6028/NIST.IR.8074v2

Hosenball, M. (2020, August 19). Factbox: Key findings from Senate inquiry into Russian interference in 2016 U.S. election. Reuters. https://www.reuters.com/article/us-usa-trump-russia-senate-findings-fact-idUSKCN25E2OY

Information Office of the State Council. (2010). Full Text: White paper on the Internet in China. The People's Republic of China. http://www.china.org.cn/government/whitepaper/node_7093508.htm

Internet users in the world. (2021, January). Global digital population as of January 2021. Statista. https://www.statista.com/statistics/617136/digital-population-worldwide/

Jinping, X. (2015). Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference, Wuzhen. MInistry of Foreign Affairs of the People's Republic of China. https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html

Kaufman, A. A. (2010). The "Century of Humiliation," Then and Now: Chinese Perceptions of the International Order. Pacific Focus, 25(1), 1–33. https://doi.org/10.1111/j.1976-5118.2010.01039.x

Kolton, M. (2017). Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. The Cyber Defense Review, 2(1), 119–154.

Krasner, S. D. (2001a). Abiding sovereignty. International Political Science Review, 22(3), 229–251.

Krasner, S. D. (2001b). Sovereignty. Foreign Policy, 122. https://doi.org/10.2307/3183223

Marks, J., & Schaffer, A. (2021, June 28). The Cybersecurity 202: The United States is still number one in cyber capabilities. The Washington Post. https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/

Mirza, M. N., Abbas, H., & Nizamani, M. Q. (2020). Evaluating China's Soft Power Discourse: Assumptions, Strategies, and Objectives. Global Strategic and Security Studies Review, 5(4), 40–50. https://doi.org/10.31703/gsssr.2020(V-IV).05

Mirza, M. N., & Khan, F. Z. (2020). Systemic Transformations and Chinese Image of the World Order: Transcending Great Wall through Neo-Confucianism and Tianxia Systems. Asia Pacific, 38, 22–38.

Mueller, R. S. (2019). Report on the Investigation into Russian Interference in the 2016 Presidential Election, Submitted Pursuant to 28 C.F.R. § 600.8(c). US Department of Justice. https://www.justice.gov/archives/sco/file/1373816/download

Nye Jr., J. S. (2010). Cyber Power. Belfer Center for Science and International Affairs. https://apps.dtic.mil/sti/pdfs/ADA522626.pdf

O'Neill, P. H. (2018, May 15). Pakistani military leverages Facebook Messenger for wide-ranging spyware campaign. Cyber Scoop. https://www.cyberscoop.com/pakistani-military-spyware-stealth-mango-tangelo-lookout/

Philpott, D. (2020). Sovereignty. In E. N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy (Fall 2020). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/fall2020/entries/sovereignty/

Pomerleau, M. (2021, June 29). Who can match the US as a cyber superpower? No one. C4ISRNet. https://www.c4isrnet.com/cyber/2021/06/28/who-can-match-the-us-as-a-cyber-superpower-no-one/

Segal, A. (2015a). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. PublicAffairs.

Segal, A. (2015b, December 16). China's Internet Conference: Xi Jinping's Message to Washington. Council on Foreign Relations. https://www.cfr.org/blog/chinas-internet-conference-xi-jinpings-message-washington

Segal, A. (2017). Chinese Cyber Diplomacy in a New Era of Uncertainty. A Hoover Institution Essay, Stanford University, Aegis Paper series no. 1703.

Segal, A. (2020, August 10). Peering into the Future of Sino-Russian Cyber Security Cooperation. War on the Rocks. https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/

Shahbaz, A., Funk, A., & Hackl, A. (2020). User Privacy or Cyber Sovereignty? Assessing the human rights implications of data localization. Freedom House, Special Report. https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty

Smartphone users. (2021). Number of smartphone subscriptions worldwide from 2016 to 2027. Statista. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Team, T. I. (2020, March 16). APT36 jumps on the coronavirus bandwagon, delivers Crimson RAT. Malwarebytes Labs. https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/

Timberg, C., Birnbaum, M., Harwell, D., & Sabbagh, D. (2021, July 20). On the list: Ten prime ministers, three presidents and a king. The Washington Post. https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/

Tucker, E., & Madhani, A. (2021, April 16). US expels Russian diplomats, imposes sanctions for hacking. AP NEWS. https://apnews.com/article/us-expel-russia-diplomats-sanctions-6a8a54c7932ee8cbe51b0ce505121995

UNGA, Sixty-ninth session, Agenda item 91. (2015). International code of conduct for information security: Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. United Nations General Assembly. https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf