IE University IE International Policy Review (IPR)
Journal **6 Issue 1** (2025)
https://ipr.blogs.ie.edu/

Virtual Frontlines: Analysing the Role of Cyberspace in State-Sponsored Conflict and Techno-authoritarianism

Ananya Singh

Sciences Po, Paris, France.
Flame University, India.
International Security

E-mail: anya.singh0511@gmail.com

Published 27th of January 2025

Abstract

Sample text inserted for illustration. Replace with abstract text. Your abstract should give readers a brief summary of your article. It should concisely describe the contents of your article, and include key terms. It should be informative, accessible and not only indicate the general scope of the article but also state the main results obtained and conclusions drawn. The abstract should be complete in itself; it should not contain undefined abbreviations and no table numbers, figure numbers, references or equations should be referred to. It should be suitable for direct inclusion in abstracting services and should not normally be more than 300 words.

Keywords: Techno-authoritarianism, Cyberwarfare, State-sponsored, Security Frameworks, Global Governance

I. Introduction

"Mass communication, in a word, is neither good nor bad; it is simply a force and, like any other force, it can be used either well or ill. Used in one way, the press, the radio and the cinema are indispensable to the survival of democracy. Used in another way, they are among the most powerful weapons in the dictator's armoury." —— Aldous Huxley, Brave New World Revisited.

The increasing global dependency on ICT (information and communication technology) and its corresponding growing vulnerabilities have led to the newfound threat of cyberspace being used as a battleground for states to not only pursue attacks on foreign threats but also attain authoritative control on and combat opposition in its own populace. This dual threat of techno-authoritarianism and cyber aggression reflects a paradigm shift where the lines between national security and accountability are becoming increasingly blurred— especially due to the lack of cohesive international legal frameworks to address such acts of aggression.

Techno-authoritarianism is the use of digital tools and technologies by authoritarian leaders and governments usually in order to increase control or limit freedom. Its use forms a vast expanse including collecting data on a state's populace without explicit consent, surveillance, disinformation campaigns, internet shutdowns, curtailing free speech online, hacking national/voting databases, and IT warfare etc (Polyakova and Meserole). Events in recent years have confirmed suspicions that the internet can be used to further destabilise democracies and prop up autocracies. Examples of this range from the infamous Cambridge Analytica scandal in which millions of Facebook users' data was collected for political actors to the attacks on the integrity of various elections including the US and Philippines in 2016 (Shahbaz). The highlight of this issue is exemplified by the facial recognition software used by China to profile Uyghur Muslims and Hong Kong protestors (Hillman, 2021). However, these belligerent measures are not limited to a domestic context. Nations have historically used cyberspace as a platform to wage shadow warfare and surreptitiously attack others. China has also exported its techno-authoritarianism through its Digital Silk Road initiative as part of its BRI (Belt and Road Initiative) wherein it has sold AI and surveillance systems to over 18 countries and the interest in these technologies is only set to rise (Chatzky, 2020). The issue of cyberwarfare has recently been brought back to the spotlight with the Israeli pager attacks on Hezbollah, and there is a history of the use of IT warfare by Israel and its Intelligence agency, MOSSAD, with its regional enemies such as Iran. Several nations at the forefront of addressing cyberwarfare have given it legitimacy by incorporating it as one of the pillars in their mainstream national doctrines of security and warfare, such as the US Pentagon in 2011. However, individual nations are not equipped to be able to completely manage transnational cyber threats alone.

In the politics of emerging digital warfare, the ability to engage with a degree of separation and plausible deniability makes it difficult to apply existing rules of engagement and international laws. There does not exist a formal mechanism or body wherein to address acts of cyberwarfare and digital authoritarianism undertaken by nations. This transnational collective threat requires the integration of traditional standards and rules of acts of aggression into cyberspace. Governments can no longer act in silos— it necessarily calls for collaboration across levels and institutions. Some nations are also at higher risk of facing cyber insecurity than others due to the increased vulnerability of their digital critical infrastructure and need multilateral cooperation to build resilience against cyberattacks. Therefore, it is necessary to develop a resilient approach towards managing global cyber insecurities which is equitable, multilateral, and preemptive. Hence, this paper seeks to provide a comprehensive analysis of existing relevant international law and security frameworks to demonstrate the gap in the literature in terms of accountability for states' belligerent actions in the digital space. To conclude, it advocates for global

governance to outline the legalities of cyberspace conduct with recommendations for the creation of a Transnational Digital Security Framework.

II. Research Questions, Methodology and Theoretical Basis

Ii. i Research Question-

- What are the current gaps and challenges in international law and security frameworks to address acts of aggression in the cyberspace by nation-states?

This further includes the two sub-questions of 'How have states weaponised information technology to meet their belligerent strategic objectives?' and 'How can a global governance system help address issues of cyber-insecurity?'

II.II Methodology-

The research paper employs a mixed-methods framework with a hybrid of qualitative methods for research analysis. It is descriptive in providing an account of the dual forms of aggressive use of cyberspace by nations, explanatory in depicting why there is a lack of formal mechanisms to address such aggressions, and normative in its final legal and policy recommendations provided at the end. The secondary qualitative data is collected through a thorough review of the contemporary literature on the research questions and this is supplemented with quantitative data from studies by data analysis organisations in the field of International Relations such as the Freedom House, AI Global Surveillance (AIGS) Index, ACLED, Amnesty International, etc wherever applicable as well as data from a study by Dragu et al wherein the quantitative and qualitative justification of the negative use of digital tools by authoritarians is demonstrated. It quotes international law, treaties, and multilateral agreements extensively to evaluate the state of current frameworks in addressing this challenge. It uses theoretical frameworks arising from the study of geopolitics, principles from the IR field of realism, concepts such as complex interdependence by Robert O. Keohane and Joseph S. Nye Jr, and liberal institutionalism as its underlying basis. Additionally, there are practical examples provided throughout to justify the claims made in this paper along with a focused case study of the history of cyberwarfare between Israel and Iran along with its allies.

II.III Theoretical Framework-

A theoretical framework within which the issue of cybersecurity can be studied is based on a linkage of emerging ICT to enhanced vulnerability of nation-states to establish complex interdependence. Robert O. Keohane and Joseph S. Nye Jr., defined interdependence as correlative interactions among actors as a consequence of 'international transactions-flows of money, goods, people and messages across international boundaries' (Nye, 2011, 285). While there has been extensive research on the first three factors, it is

the last one that is slowly gaining traction in contemporary research. Keohane and Nye have written on "Power and Interdependence in the Information Age"(1998) and highlighted the extent to which the "new world" of cyber merges with the "traditional world" which rests on the basis of geography (Keohane & Nye Jr., 1998, 81-94). No states are left insulated from cyberwarfare, including the continental states of USA or UK who were seen to have great defensive strength based on their geography in Mahan's theory. Rather, states and non-state actors can now acquire global power despite being landlocked (Sprout, 1954, 24). Mackinder emphasised the role of integration and communication linkages between Eurasia and Africa as the reason for their predicted dominance on global power (Topalidis et al., 2024). However, in today's globalised world, all nations and NSAs are integrated into the global order, with even critical supply chains being transcontinental. Therefore, every actor has the ability to shift the dynamics of the multipolar international order.

Irrespective of the fluid nature of cyberspace, it will require governance and authority structures for containment. As a result, global institutions will play a key role based on the theory of liberal institutionalism (Topalidis et al., 2024). The nature of complex interdependence is impacted greatly by advances in the cyber domain resulting in an expansion of cross-connecting channels of communications in global politics across different actors. This leads to a situation in world politics, where there exists a multitude of nation-states harbouring multiple channels of contact that link the different societies without any imposition of the state or fixed hierarchy of issues. In fact, the network of information flows bypasses the territorial boundary of the state and has engendered a system which is not reigned in by state sovereignty. The close linkage between emerging technologies and power politics will impact the patterns and networks of cooperation and conflict based on strategic imperatives which in turn will influence the outcomes, viz. norms and institutions. This paper will apply the concepts of complex interdependence to analyse how nation-states collaborate or compete in the field of cyber security.

III. Virtual Frontlines: Cyberwarfare as a Geopolitical Strategy

The role of geopolitics in cyber attacks has revealed how national vulnerabilities in the cybersecurity domain need to be contextualised at a regional and global level. Cybersecurity has changed the face of global conflicts and impacted the way wars are fought and attacks are launched on enemies. This involvement blurs the lines between politically motivated cyber operations and cyberwar, complicating legal responses. Nation-states play a significant role as "threat actors and danger to society and other states" when they pursue tactics of cyberattacks with examples such as the Chinese PLA army's alleged cyberattack division (Cavelty & Egloff, 2019, 42).

Existing geopolitical stressors coupled with turmoils in Europe and West Asia, challenging health of the economy and elections scheduled in major countries have created the right mix for cyber volatility to pose an imminent threat to geopolitical security. The forces of globalisation have paved the way for geopolitical unrest in one region to result in a major cybersecurity challenge spillover to other regions. Additionally, nations and actors can launch attacks across continents to destabilise their enemies with no identification. This is seen in Russia's cyberattacks on Ukraine with the motivation to attain a buffer region and frontier territory against the EU regional domain, and to expand their territorial lebensraum based on Ratzel's organic theory to acquire key resources (Sprout, 1954, 32). Russia's cyber tactics have included shutting down power grids, government websites, banking institutions, satellite services provided by private companies like SpaceX, etc. Additionally, China has been known to cyberattack critical infrastructure on foreign US bases such as the military base on the Guam island in the Pacific ocean which poses a geopolitical threat to them (Proctor, 2022). Cyberattacks are also a way for distant nations such as North Korea to overcome their geographical boundaries to attack their adversaries such as the US.

State-of-the-art targeted attacks on critical infrastructure is the latest covert weapon employed in geopolitical conflicts. Critical infrastructure refers to assets, systems and networks - such as communications, data storage or processing, financial services and markets, water and sewerage, energy, healthcare and medical, higher education and research, food and grocery, transport, space technology; and the defence industry sector - whether physical or virtual, which are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof (Rege and Bleiman, 2020). This is not limited to national infrastructure only— The US database for example incorporates external major trading ports, weapons manufacturers, international pharmaceutical manufacturers, etc. Any interruption or severance of these systems would result in strategic risks of major consequence in those sectors as well as have repercussions across geographies.

Two critical aspects in the cyber security space as identified by (Cavelty & Wenger, 2020) are - 1) the low entry costs for disruptive cyber "weapons" and 2) the high vulnerability of critical infrastructures, which are dependent on digital technologies. This dependency has raised the cyber security issue into the realm of " high politics" of national and global security concerns. Contemporary cyberattacks on infrastructure are being executed with a plethora of objectives. This includes goals of exertion of influence and force, sabotaging national security and economic growth, endangering public health and safety, subversion of critical infrastructures and so on (Choucri, 2013). While the

energy sector is a prime target of cyber-attacks against critical infrastructure, other sectors such as telecommunications, ports and critical manufacturing industries are also vulnerable. States and non-state actors are able to extract sensitive security data from remote untraceable locations through espionage and can engage in sabotage operations damaging critical infrastructures e.g. electrical grids, financial institutions, healthcare systems, and so on. Additionally, cyber warfare can integrate such operations with traditional military offensives. A recent example of a transnational cyberattack on critical infrastructure is of the 2017 NotPetya malware employed primarily against Ukraine, which shut down its major national institutions and electric grids. The attack then became global with reports extending to the USA, UK, France, etc.

IV. A Case Study of Iran-Israel Cyber Conflicts

West Asia is exceptionally plagued by cyber warfare, with state actors such as UAE and Saudi Arabia being accused, along with NSAs such as Hezbollah or Hamas. This case study focuses on the use of cyberattacks between Iran and Israel as the two biggest perpetrators using this as a strategy part of their larger conflicts. Such cyberwarfare tactics are being used as retaliatory measures by either party after the recent conflagrations and cyberattacks in the region have massively surged since October 7th. One of the biggest instances of a cyberattack on critical infrastructure was the impact of Stuxnet on Iran's Natanz nuclear facilities (Farewell, 2023), which has been repeated in 2024. It is viewed by many theorists as the first cyberweapon and was allegedly used bilaterally by the USA and Israel to pursue their geopolitical goals of destabilising Iran's nuclear programme. A cyberattack had better results on a risk-benefit analysis compared to conducting an airstrike on the base. Stuxnet also went ahead to create collateral damage transnationally in other countries, it is unclear whether intentionally or unintentionally. It evolved into a transnational threat with attacks on Russia, Indonesia, India, etc (Farewell, 2023). Similar attacks on a variety of Iran's critical infrastructure have continued up to this date.

An interesting allegation also is that further attacks on the Natanz did not arise from external countries, rather, it was done by dissident groups within the nation such as the Irani Cheetahs of the Homeland group who accepted blame for a later attack (Gol, 2020). Similarly, there has been a sharp rise in cyberattacks conducted by extremist groups supported by Iran such as the hezbollah against the critical infrastructure of Israel and infiltrating into infrastructures such as international airports as well. This involves the complex growing role of non-state actors, specifically, domestic cybercrime within cyberwarfare. Iran has conducted several state-backed cyberattacks and supported the NSAs part of its axis of resistance to pursue the same. They allegedly attempted a major attack on the Israeli water and sewage system, which was a direct unprecedented target on civilian critical infrastructure (Siman-Tov,

2020). Additionally, they also gained control of the floodgates of the transcontinental new york-based dams. This demonstrates the critical impact of cyberwarfare as attacks taken out against common civilians. Iran has also been victim to other cyberattacks blamed on Israel on its critical infrastructure including one in Shahid Rajaee which is a key shipping harbour where over 50% of Iran's imports and exports take place. Iranian attackers have also been accused of extending to private enterprises such as Saudi's Aramco oil company (Siman-Tov, 2020). These attacks, while directed at a key target nation, had an immense global impact on energy resources and international trade. Iran and Israel's cyberwarfare against each other is a key case study that encompasses the involvement of both state and non-state actors, governments and private enterprises, and military and civilian-directed attacks. It demonstrates the ability of a regional cyberwarfare campaign to extend beyond regional boundaries and exacerbating a global dilemma.

V. Beyond the Battlefield: Cyberpower for Digital Authoritarianism

One of the oldest feats of technology- Gutenberg's printing press was first seen as a method for Catholics to further their power; however, the very same technology was used against the Catholics leading to the Protestant revolution. Drawing a parallel, current digital advancements are seen as a way to further the authoritarians' stronghold. The belligerent use of cyberspace extends beyond attacks on enemy nations to attacks on a country's own populace by the leaders to attai control and suppress any opposition. Digital technologies are a double-edged sword. While technology's advancement brings a larger scope for mobilisation and communication among individuals which can be used to counter undemocratic regimes, the regimes can counter this by using technology to prevent these in the first place (Dragu et al 4).

Three such key case studies analysed within prominent literature arise from China. They include China's facial recognition software used in protests (Mozur); China's social credit system (Lee); and the export of digital surveillance systems as part of the Digital Silk Road (DSR) through the Belt and Road Initiative (BRI) (Chatzky et al.). China has been reported to use facial recognition technology in their surveillance of protests. Every public sphere is fitted with surveillance tools and when protests like the one in Hong Kong in 2019 occur, the protestors are immediately identified. Every person can be surveilled without their consent. This is an easy mechanism often used to shut down any opposition present which makes it fundamentally undemocratic. (Mozur) This is combined with their social credit system which is governmental monitoring of individuals and companies alike to give them a score of how trustworthy they are. This score is based on their financial and social behaviour, in accordance with the expectations of the Chinese government (Lee). These two examples primarily demonstrate the extent and

capabilities of the Chinese state to use their digital tools against their own populace. What takes this a step further is that this technology is no longer restricted to just 2 nations in this world. Through exports and trade, these nations are able to cause other states to adopt their techniques and therefore, worsen the global decline in democracies.

The main concern regarding this is tied in with China's Belt and Road initiative, and its latest addition of the Digital Silk Road initiative. The BRI is a massive infrastructural trade project launched in 2013 covering a geographical expanse of East Asia to Europe. Bringing China a level of power, connectivity and trade opportunities reminiscent of dynastic times. However, there is considerable opposition to this endeavour. Primarily since it frequently exploits countries with misleading contracts and supports other authoritarian regimes (Chatzky et al.). Over 18 countries have purchased AI and surveillance systems and the interest in these technologies is only set to rise. Left unchecked without any protection for human rights, this will further the rise of authoritarians globally (Polyakova and Meserole).

Often referred to as the "Firehose of Falsehood" Propaganda Model, Russia is the second nation party to blame within existing literature and research studies from various think tanks. (Paul and Matthews) They have undertaken prominent propaganda disseminating campaigns in their peripheral regions of Ukraine and Georgia; supported their campaigns in foreign conflict areas like Syria and Afghanistan; as well as allegedly made an attempt to interfere with the 2016 US election (Jozwiak).

Western nations aren't blame free either—the USA has historically been at the centre of controversy regarding surveillance and disinformation too. Post 9/11, the enactment of the patriot act and the revelations provided by Edward Snowden are infamous tales of US surveillance (Pilkington). The patriot act used national security letters in order to allow the government to track citizens and obtain data on them through private or third-party companies. The Snowden documents proved the existence of NSA surveillance on US citizens. The USA and its ally European states were also an equal match to Russia in terms of spreading disinformation and propaganda during the Cold War period (Whitton and John 152). The argument for this is not solely historical, the USA and the European States are perennial subjects of surveillance capitalist endeavours. The Facebook and Cambridge Analytica scandal exemplified this in how two private companies were able to acquire and sell the data of millions of people for a political campaign (Ozer and Conley). The European Court of Justice's judgement on "Schrems II" of 16 July 2020 affirmed this. Officially stating that the EU-US "Privacy Shield" agreement does not provide an adequate level of protection for personal data because of insufficient human rights safeguards for access to data by the US government surveillance programmes.

VI. Evaluation of Current International Cybersecurity Frameworks

There are increasing accusations made against nations for participating in cyberwarfare, yet no formal mechanism to address it. This has created a collective threat perception which points to the need for integration of existing rules of international intervention at different levels. Defence partnerships on cybersecurity are also required to mitigate belligerent threats. Concerns over cybersecurity are no longer confined to the territorial boundaries of a nation, hence, it calls for enhanced efforts towards regional securitisation. It becomes imperative to adopt a collaborative, preemptive and resilient approach to cybersecurity risk management.

In the politics of emerging digital technologies, the ability to engage in disruptive actions with a degree of separation and deniability makes it difficult to apply existing rules of engagement and international laws in the cybersecurity space. Governments can no longer act in silos— it necessarily calls for collaboration across levels and institutions. Richard Haass, President of the Council on Foreign Relations points out that "Cyber is exactly at the point today where nuclear was maybe 50 years ago, where people are beginning to think, what sort of rules do we set up? What sort of arrangements do we put into place?" (Haass, 2010). Measures are being taken at the level of national governments as well as regional and international organisations to engage in coordination efforts and come up with a framework that places a binding legal and juridical system such as the Budapest Convention on Cybercrime of the Council of Europe. Internationally, nation-states in 2013 came to a consensus that international law, including the U.N. Charter is applicable to cyberspace. However, while the UN charter decrees against the use of force— it remains unclear at what point a cyber attack can be deemed as a use of force or aggression. A cyber attack on critical infrastructure could cripple people's lives too demonstrated with recent attacks on electricity grids or water systems. The UN General Assembly has established working groups to report on cybersecurity matters such as the application of international law, emerging threats, norm establishment for its use by states, international cooperation, capacity building, etc to bring clarity to such grey areas. These are formulated into UN resolutions such as the UN GGE 2015 endorsed non-binding, voluntary rules on preventing nation-states from launching a cyber offensive on the critical infrastructure of another nation-state or its cyber security response teams, during peaceful times (Choucri, 2013). It is imperative for the GGE to re-group to continue drafting norms based on mandates of international law for cyber attacks after its failure to attain consensus in 2017. There are various capacity-building initiatives that have emerged over time e.g.- International Telecommunications Union (ITU), the Global Forum on Cyber Expertise (GFCE), etc. In 2023, 40 states have proposed a Programme of Action

(PoA) for formalising a singular entity, a permanent UN forum on cyberspace (Choucri, 2013). Endeavours such as this are necessary to create a basis for collaboration on cybersecurity.

VII. Conclusion: Crafting a Global Digital Security Framework

It is not adequate to have forums only for the exchange of information. It is of immediate importance to carve out a clear space for international cooperation to counter cyber attacks on critical infrastructure backed by regulations that incorporate public-private partnerships. This would require coming to a consensus on developing a code of conduct and appropriate mechanisms at the national, regional and global levels. The lack of binding treaties and agreements on cyber security issues aids the ongoing practices of covert cyber attacks. There is progress being made to this end with the first UN cybersecurity alliance of the International Multilateral Partnership Against Cyber Threats (IMPACT) but this acts as a resource centre, rather than true diplomatic multilateral engagement (Choucri, 2013). Diplomatic engagements help create the groundwork for further cooperation and can help answer such questions in a multipolar regionalised world order. Cyber diplomacy can assume a pivotal role in cultivating global partnerships, creating global standards and securing the preservation of critical infrastructure. Cyber-diplomacy is needed to maintain a constant dialogue between countries to develop norms of accountable government behaviour in cyberspace and address disagreements between role-players (Maizland, 2020). Additionally, cyber diplomacy between nations can lead to an intelligence-sharing agreement which can allow for a robust offensive to be conducted upon identification of the cyberattack. The resiliency of critical infrastructures can be built through joint capacity-building and specialised training endeavours. A proactive approach towards safeguarding critical infrastructure is necessary and can be achieved through regional collaboration. For key advanced cyber-power nations, a policy of non-aggression pacts may be utilised as a confidence-building measure. Going beyond securitisation, regional or bilateral defence partnerships can also be constructed to formulate cyber attack responses and improve offensive capabilities under the mandates of international law.

To conclude, cybersecurity is a global geopolitical threat which impacts the critical infrastructure of countries and interconnected transnational systems which requires further international frameworks and regional collaboration to manoeuvre. This research paper aims to contribute to further academic scholarship required to formulate an IR theory to incorporate an understanding of cyber security as a new frontier of warfare and its underlying geopolitical implications.

References

Cavelty, M. D., & Egloff, F. (2019, June 14). The politics of cybersecurity: Balancing different roles of the states. St Antony's International Review, 15(1), 37–57. https://papers.ssrn.com/sol3/papers.cfm/abstract_id=3403971. Accessed October 5, 2024.

Cavelty, M. D., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855. Accessed October 5, 2024.

Chatzky, A., et al. (2020, January 28). China's massive Belt and Road Initiative. Council on Foreign Relations. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative#chapter-title-0-6. Accessed October 8, 2024.

Choucri, N. (2013, October 22). Institutions for cyber security: International responses and global imperatives. Wikipedia. https://www.tandfonline.com/doi/full/10.1080/02681102.2013.836699. Accessed October 25, 2024.

Davis, L. E. (2003). Globalization's security implications. RAND Corporation. https://www.rand.org/pubs/issue_papers/IP245.html. Accessed October 8, 2024.

Dragu, T., & Lupu, Y. (2021). Digital authoritarianism and the future of human rights. International Organization, 75(4), 1–27. https://doi.org/10.1017/s0020818320000624. Accessed October 4, 2024.

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. Accessed October 5, 2024.

Gol, J. (2020, July 6). Iran blasts: What is behind mysterious fires at key sites? BBC. https://www.bbc.com/news/world-middle-east-53305940. Accessed October 28, 2024.

Hillman, J. E. (2021, November 17). Techno-authoritarianism: Platform for repression in China and abroad. Center for Strategic and International Studies. https://www.csis.org/analysis/techno-authoritarianism-platform-repression-china-and-abroad. Accessed October 7, 2024.

Jozwiak, R. (2021, September 22). Researcher says raw voting data points to massive fraud in United Russia's Duma victory. Radio Free Europe. https://www.rferl.org/a/russia-election-fraud-shpilkin/31472787.html. Accessed October 27, 2024.

Keohane, R. O., & Nye, J. S. Jr. (1998). Power and interdependence in the information age. Foreign Affairs, 77(5), 81–94. https://doi.org/10.2307/20049052. Accessed October 5, 2024.

Lee, A. (2020, August 9). What is China's social credit system and why is it controversial? South China Morning Post. https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial. Accessed October 29, 2024.

Maizland, L. (2020, June 10). The emergence of cyber diplomacy in an increasingly post-liberal cyberspace. Council on Foreign Relations.

https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace. Accessed October 27, 2024.

Mozur, P. (2019, July 26). In Hong Kong protests, faces become weapons. The New York Times. https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html. Accessed October 29, 2024.

Nye, J. S. (2011). The future of power. PublicAffairs. Accessed October 5, 2024.

Ozer, N., & Conley, C. (2018, March 23). After the Facebook privacy debacle, it's time for clear steps to protect users. American Civil Liberties Union. https://www.aclu.org/news/privacy-technology/after-facebook-privacy-debacle-its-time-clear-steps-protect. Accessed November 5, 2024.

Paul, C., & Matthews, M. (2016). The Russian "Firehose of Falsehood" propaganda model: Why it might work and options to counter it. RAND Corporation. https://www.rand.org/pubs/perspectives/PE198.html. Accessed November 5, 2024.

Pilkington, E. (2021, September 4). 'Panic made us vulnerable': How 9/11 made the US surveillance state – and the Americans who fought back. The Guardian. https://www.theguardian.com/world/2021/sep/04/surveillance-state-september-11-panic-made-us-vulnerable. Accessed November 5, 2024.

Polyakova, A., & Meserole, C. (2019, August 27). Exporting digital authoritarianism: The Russian and Chinese models. Foreign Policy at Brookings. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf. Accessed October 28, 2024.

Proctor, P. (2022, June 10). How geopolitics impacts the cyber-threat landscape. Gartner. https://www.gartner.com/en/newsroom/press-releases/2022-06-10-how-geopolitics-impacts-the-cyber-threat-landscape. Accessed October 8, 2024.

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. International Journal of Intelligence and Counter-Intelligence, 26(3), 453–481. https://doi.org/10.1080/08850607.2013.780552. Accessed October 5, 2024.

Siman-Tov, D. (2020, June 3). A new level in the cyber war between Israel and Iran. Wikipedia. https://www.jstor.org/stable/resrep25542. Accessed October 29, 2024.

Shahbaz, A. (2018). The rise of digital authoritarianism. Freedom House. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism. Accessed October 5, 2024.

Shahbaz, A., & Blunt, M. (2022). Freedom on the Net 2022: Countering an authoritarian overhaul of the internet. Freedom House. https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet. Accessed October 6, 2024.

Sprout, H. (1954, January). Geopolitical theories compared. Naval War College Review, 6(5), 19–36. http://www.jstor.org/stable/45104944. Accessed November 5, 2024.

Topalidis, G. T., Kartalis, N. N., Velentzas, J. R., & Sidiropoulou, C. G. (2024, February 9). New developments in geopolitics: A reassessment of theories after 2023. Social Sciences, 13(2), 109. https://doi.org/10.3390/socsci13020109. Accessed November 5, 2024.

Wang, M. (2021, April 8). China's techno-authoritarianism has gone global. Human Rights Watch. https://www.hrw.org/news/2021/04/08/chinas-techno-authoritarianism-has-gone-global. Accessed October 5, 2024.

Whitton, J. B. (1951). Cold war propaganda. American Journal of International Law, 45(1), 151–153.

https://doi.org/10.2307/2194791. Accessed October 27, 2024.