McNair Scholars Research Journal

Volume 12 | Issue 1 Article 9

2019

Cyber Security: China and Russia's Erosion of 21st Century United States' Hegemony

Cyril K. Yancey
cyancey@emich.edu

CYBER SECURITY: CHINA AND RUSSIA'S EROSION OF 21ST CENTURY UNITED STATES' HEGEMONY

Cyril K. Yancey
Dr. Richard Stahler-Sholk, Mentor

ABSTRACT

With Russia and China emerging as challengers to U.S. hegemony, the use of cyber warfare could tilt the current balance of power in either of their favors. Using various methods, hackers can acquire sensitive information and destroy online infrastructures. In the development of cyber warfare, China has become a seasoned veteran with computer virus operations dating back to 1997[14]. Russia has emerged as a cyber aggressor, as seen in Russia's cyber attacks on several countries in the last decade. This paper argues that, with the growth of foreign cyber technology, the probability of cyberspace being used as a military front by state or non-state actors against the United States increases.

INTRODUCTION

International Power Measurements

The measure of power in international politics and state relations refers to the range of influence any single actor has over other actors on the world stage. In the international system, two ways to measure state power are *soft power* and *hard power.* The use of soft power in the international system allows a state to influence other states and actors via trade relations and diplomatic means. Hard power in the international system is based on the ability for states to reach their goals using force, threats, or coercive actions[27]. In the international system, the use of power by various states creates a system of power relations between states.

The levels of influence states and actors have over each other are measured by their military capabilities, strategic relationships, and economic performance. In competition between states for power, competitors look for new ways to increase their power, resulting in a search to find new means to keep pace with the current world leader.

The role of a hegemon in world politics has been noted as an important peacekeeping facet on the international stage. Hegemonic stability theory argues that a clear dominant state provides both economic and political stability worldwide[1]. Providing stability is a key function for a hegemonic state. This stability often comes in the form of a dominant military, as well as a strong economy, in order to maintain hegemonic status for a prolonged period. Without a hegemonic military power such as the United States, hegemonic stability theory suggests that maintaining global peace would be more difficult without a single dominant state establishing and maintaining order in the international system[1].

A hegemon comes into existence when a single power holds a higher sum of various measures of power over other states and actors. The factors used in this paper for hegemonic measurements consisted of forms of economic, diplomatic, and military capabilities. To measure hard power, the units of measurement were standing army size, military spending, and technological advancements. To measure economic and soft power, Gross Domestic Product (GDP), GDP per-capita, and stock market health were used to measure the economic and militaristic capabilities of a state. A macro evaluation of any state's health and relative power can be seen through these factors. With these measurements taken into account, a state can be evaluated to determine if it has reached a hegemonic status.

Joseph Nye's interpretation of soft power refers to a state's ability to use diplomatic persuasion and mutual interest to build power[2]. Transnational actors have greatly impacted state development, especially through economics. Transnational corporations, such as Apple, have the ability to transform an entire country's economy, as seen in the economic development of Ireland since Apple's arrival in the 1980's[3].

One soft power measure is the influence a state has in the United Nations (UN), a large part of the intergovernmental

system. The UN holds a unique ability in that it is able to provide humanitarian aid as well as deploy any of its voluntary forces to perform peace operations (including coercive enforcement, if authorized by the Security Council under Chapter VII of the UN Charter)[4]. In the UN Charter, the ability to veto resolutions put forth by any member is given to the five permanent members of the Security Council, which includes China, France, Russia, the United Kingdom, and the United States. The ability to veto any resolution grants these states the ability to influence world politics in a way no non-member state is able to achieve[4]. The structure of the UN provides an opportunity for states to deliberate issues and assist other states through a participatory format in which each state has one vote in the General Assembly. Much of the UN's success has been credited to its structural effectiveness, according to an article in *The International Journal of Peace Studies*, which concludes that active participation and direct involvement in peace efforts have a profound effect on the UN's overall success[5].

China's economic and diplomatic initiatives in Africa in recent years illustrate the exercise of soft power. Efforts by China to increase its geopolitical power have seen the state expand trade into Africa significantly, with over $100 billion loaned to African countries in the last 15 years alone, according to data from the China African Research Initiative[6]. As investment opportunities have dwindled inside its borders, China has sought increased investment internationally. China has also been a 21st century investor in countries with weaker governments. This strategy could be explained by a soft power tradeoff of financial risk for geopolitical advantages. By investing large sums of money in multiple important infrastructure and development efforts, China has gained influence while building strong relationships with all of the recipients of its funds. Over a billion people live on the continent of Africa, and the 54 states of the continent represent over one-quarter of the votes in the UN General Assembly. A concentrated expansion effort by China could provide both economic and political leverage, should a conflict arise between hegemonic contenders. The loans made to Algeria, Kenya, and Nigeria have provided China with strategic access to ports throughout the African continent. In addition to the hard power advantages provided by port use, the gain in soft power through

trade deals provides a point of leverage for China in its quest for hegemonic power.

China has also deepened its economic relationships with African countries in an effort to gain access to raw materials and to create new markets for Chinese goods and services. The economic value from improved African-Chinese relations can be observed in their arms dealings, with China accounting for 25% of conventional arms sales to the continent[7]. China's permanent seat on the UN Security Council affords it a unique opportunity to serve as a useful ally with developing African nations on the international stage. The African continent's development potentially provides China a large untapped market of both economic and political value.

In addition to increasing their presence in Africa, China's Belt and Road Initiative aims to expand Chinese influence and connectivity throughout Europe[26]. This plan was created with the hope of expanding Chinese trade while providing China with easier access to European markets. Expanding geopolitical power through economic projects will give China significant influence over the political activities of indebted states. The plans for this initiative include building special economic zones and expanding the use of Chinese currency[26].

The rise of an industrialized power with cyber security expertise, such as China, calls into question the perceived hegemonic status of the United States. For decades, the United States has been viewed as the major dominant power across the globe in terms of international influence. If China expands and strengthens its ties with a larger number of developing countries, it could become just as important a geopolitical ally to the continent of Africa as the U.S. has been in the past. In order for the soft power established by the U.S. in Africa to be truly threatened, the loans made by China to African nations must result in the continent's economic growth and stability. If these states were unable to repay their loans, China's loss of capital would be detrimental both to China and to the future economic health of the African continent.

Hard power remains important, but technology has altered some of its characteristics. With the destructive power of nuclear weapons, as well as the prohibitions against their use, this paper measures a state's hard power in terms of its advancements in

the acquisition of military armaments and the size of its standing army. The ability of a state to use significant funds for its military demonstrates a commitment to military advancement, whereas a large volume of armed forces demonstrates another use of human capital, stemming from the state's commitment to the military. The United States has led all other states in military spending, with an approved 2019 military budget of over $650 billion[8]. The 2017 military budget of the United States was $610 billion, which is the size of the combined military budgets of China, Russia, Saudi Arabia, India, France, Japan, and the United Kingdom[9]. Though the United States far outspends other states, Russia and China still spend a considerable amount on their military. China is the sole nation to rival the U.S. in military spending, with just over $228.2 billion spent in 2017. This is a very significant amount when compared to the military spending of other hegemonic contenders, such as Russia, which spent $66 billion in 2017[10]. In ranking the largest standing armies in the world, China's army is largest, while the U.S. ranks third, and Russia is fifth[11]. Of the five permanent Security Council members, only three states on the UN Security Council have large standing armies in addition to high military investment, when compared to total GDP and worldwide state military spending.

A nation's hegemonic solidification can be measured by the health of its stock market in addition to other economic factors, such as GDP and GDP per capita. In 2017, the United States held a $7 trillion annual GDP lead over China and surpassed the Russian Federation's GDP by over $17 trillion[12]. The United States also holds a significant positive gap between competitors in GDP per capita, which at $59,531, was considerably higher than Russia's $10,743 and China's per-capita GDP of $8,826.99[13].

Using hegemonic contenders' stock markets as a measure of economic health, a macro view of a state's general health and sector growth may be analyzed. From February 1, 2009 to February 1, 2019, the United States' stock market, as measured by the S&P 500, increased over 377%, with companies such as Facebook and Exxon Mobil having produced double-digit year-to-date returns[14]. The Moscow Exchange, or MOEX, is the index used to track 50 companies in Russia as a measure of Russian economic health. Similar to the growth of the S&P 500, from January 1, 2009 to January 1, 2019, the MOEX index increased over 380%[15]. Though both the

S&P 500 and MOEX markets saw similar increases in percentages, these numbers differ due to the S&P 500's market cap of $250 billion, while the MOEX's market cap is close to $160 billion[15]. The growth of the S&P 500 was largely due to the amount of total capital dictated by the market cap. The Russian Federation's heavy dependence on oil prices plays a significant role in the MOEX index, with energy corporations, such as Gazprom, contributing heavily to the Russian Federation's current economic boom.

The United States' strong economic performance, large active standing military, and extensive international soft power argues for its position as the current hegemon of the world. With the fall of the Soviet Union in 1991, China and the Russian Federation have emerged as the two major hegemonic challengers to the United States. For the past three decades, these states have competed with the U.S. for geopolitical power and hegemonic superiority.

LITERATURE REVIEW

In the development of technological infrastructure, the digital world has become a platform for business, communication, and military power. Similar to insurance for a home, proper cyber security is crucial for all digital consumers, from individuals to governmental agencies. Cyber and information warfare come in a variety of forms and can be executed through a plethora of technological entry points. Cyber warfare is defined by RAND as, "the actions by a nation-state of international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks"[16]. Information warfare is more commonly associated with the use of misinformation, which is currently commonly seen on social media platforms. In countries with a high volume of technology, such as laptops or smartphones, the magnitude of a cyber attack on digital infrastructure poses the threat of financial losses as well as disruptions in communication.

China currently holds the greatest cyber warfare ability, as well as the most experience in all of Asia, with the People's Liberation Army (PLA) of China being estimated to have conducted over 200 different information warfare military exercises from the late 1990s to 2010[17]. In information warfare exercises held by the

PLA, the use of Trojan horse viruses disguised as Microsoft Word and PowerPoint were installed in government office computers in several countries[17]. Once a file was saved on an infected computer, the information the file contained was uploaded to several Beijing-based websites in which the saved documents were stored[17]. Developments in China's cyber arsenal include software capable of obtaining passwords, code breaking, information-deception software, and other forms of malware. These methods have been tested, starting in 2000, and have since been developed into detailed procedures used by the PLA in other military procedures[17]. The online infrastructure of the world includes social media and other platforms in which information, goods, or services are exchanged. Any attacks on such infrastructure can cause problems ranging from financial losses due to unavailable banking services to widespread panic created by the spread of misinformation.

The use of misinformation is another sector of information warfare that can impact populations through quick information dissemination. The use of misinformation has reached a level of development proven to influence domestic and international politics. During the 2016 U.S. Presidential election, the use of "fake news" on social media became a form of information warfare. A study in *The Journal of Economic Perspectives* reported that fake news stories concerning the election were shared over 150 million times[18]. The source of the fake news differed, depending on whether the fake news websites aimed to earn a profit or primarily hoped to influence the opinions of others.

In cyberspace, information can be quickly spread, regardless of accuracy. Using popular keywords or "tags," a properly positioned story can become "viral" and spread information to a large number of people. The use of misinformation is not a new concept, but it has taken on a new and wider platform via the internet. Setting up accounts on a variety of platforms is a simple task that often only requires email verification. The potential impact that a fake newspaper article may have, compared to the potential of the same article on a social media site, such as Facebook or Instagram, greatly differs due the speed and range of readers the story may reach. Regardless of the spectrum of the information attack, the security of the digital infrastructure of a state is crucial to its structural integrity and the flow of information in and out of its borders.

Gaining an upper hand in the use of technology could prove to be a significant advantage, should any form of conflict break out between states. These attacks can also be perpetrated by non-state actors, which can have unclear identities. With the historical tensions between Russia and the United States, the notion of a cyber war between states would not be unreasonable. Due to the damage to infrastructure and human life caused by the use of nuclear weapons, a more sustainable form of conflict might be one waged without troops and with none of the costs of war. The ease of deniability related to cyber attacks could also make the proxy use of non-state actors an effective means of interstate conflict; the use of non-state actors in cyber attacks could be beneficial to a larger state as a means of disguising attacks.

Often, terrorist groups hope to spread their message to the widest audience possible. The internet provides a medium in which content can be freely posted and distributed, with few general regulations put in place by states. "Netwar" is a term used to describe a brand of war based on the use of information warfare[19]. In this style of warfare, the aggressive use of information systems siphons power from states to non-state actors. States have hard boundaries are not able to encroach on other states' territories. Through the internet, non-state actors have the means to recruit inside national borders while spreading propaganda.

The complexity of cyber attacks often causes significant issues when nations seek to develop a protocol to deal with them. In the spread of misinformation, whatever is posted can easily be screenshot and reposted, making it difficult to stop its spread. The global influence of terrorist networks, transnational corporations, and transnational criminal organizations poses a challenge to the power of the state[19].

Without proper measures for adequate security, a rogue attack on a transport or communication system could prove to be dangerous, as well as difficult to trace. The spread of Trojan horse viruses can be used to quickly infect and take over computers, in an age in which privacy policies and terms of services are often too dense to be thoroughly read by the average user. With the ease of misinformation dissemination, non-state actors have the ability to mobilize quickly, which poses a threat to security protocols that may not be adequately prepared for these sorts of strikes, due to

their unpredictability in form and timing. For the country facing the cyber attack, a reactionary response to a cyber attack could mean the loss of a large volume of e-commerce.

The security of cyberspace has direct effects on the outside world in a variety of ways. In the turmoil occurring from the denial of services such as water or electricity, a functioning society could come to a standstill. Without proper information services, people may be left without direction during times of need or in evacuation situations. Preparedness for the dangers of an event, such as a wide scale attack on digital infrastructure, should be met with carefully conceived protocols detailing procedures for the timely and accurate spread of relevant information. In addition to proper information dispersal, stores of food and water should be held by local governments to address a shortage of goods.

In 2007, the state of Estonia fell victim to a range of cyber attacks on its online infrastructure by a group of Russian hackers[21]. This attack was fueled by the tension between the two states, which reached a boiling point in 2007 over the relocation of a statue. After the statue was moved, Estonia was hit with denial-of-service attacks for 22 days, and, as a result, two major banks, the websites of all government ministries, and the websites of a few political parties were shut down[21]. Estonia is viewed as a European leader in terms of the integration of the internet in its citizens' daily lives, making its vulnerability to cyber crime more noteworthy. Some suggested that these attacks were the result of the transcendence of the Russian ethnic identity across geopolitical borders[21]. During the attacks, many financial organizations kept their losses private, with one bank only later admitting it had lost over a million dollars during the 22 day span[21]. The use of the internet in banking, communication, and voting in Estonia can be compared to the level that citizens of the United States use in their own daily lives. With both countries relying heavily on the digital world for information and basic services, any attack would threaten a major conduit for many forms of business and communications. The level of sophistication of the Estonian cyber attacks should serve as a warning to the United States about the importance of high-level cyber security measures.

The balance of power between hegemonic contenders has been a linear race in favor of the United States in the recent past. The introduction of cyber and information warfare offers a chance for other nations to tip the scales militarily in favor of either Russia or China, the two main hegemonic contenders to the United States, offsetting their relative lag in other military and economic power dimensions. The cyber experience of both Russia and China poses a great risk to the continued hegemonic power of the United States on the world stage. While a major cyber attack comparative to Estonia has yet to be enacted on the United States, cyber and information warfare poses a threat to the hegemonic state of the United States. These methods, combined with competitive economic and geopolitical performance, suggest that China and the Russian Federation could pose serious threats to United States' hegemony in the 21st century.

Power Relations in the 21st Century

The 2018 Department of Defense Cyber Strategy summary states: "We are engaged in a long-term strategic competition with China and Russia. These states have expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners"[24]. This document notes the erosion of military advantages of the U.S. due to the advancement of Chinese cyber technology, which has stolen information from both the public and private sectors[24]. It also states that Russian influence in the 2016 Presidential elections was made possible by cyber technology[24]. There is no anticipated end to these threats. China, Russia, and the cyber technology developed by these states will continue to pose a significant threat to the current balance of power. As the number of malicious cyber events continues to rise, the growth of cyber technology by actors who have a history of aggressive activities poses a threat to international security.

Power relations between states have been changed by the integration of the cyberworld into facets of daily life. Joseph Nye predicts that governments will not be able to control cyberspace as closely as physical spaces, such as attacks by land or sea[22]. He emphasizes the roles that non-state actors will play, due to the low

cost of cyber attacks[22]. The barriers that have traditionally kept non-state actors from engaging in conflict with states, such as the lack of armed forces or military resources, are made irrelevant with the possession and use of offensive cyber technology. These actors do not require the capital normally needed when launching an offensive; in addition, states that do not have traditional means of military or coercive power can also benefit through the use of cyber warfare. Russia's developments in cyber technology make them just as significant a threat, according to the U.S. Department of Defense, as China, a close hegemonic contender to the U.S. These factors argue for the need for increased funding to programs regarding cyber security issues.

As cyberspace expands its reach, the strength of a state's cyber defenses and technological advancement could become a more accurate measure of 21st century military capabilities, due to the range of cyberattacks[20]. The United States, as the current hegemon, has the most to lose by such a reassessment of power. The inclusion of cyber capabilities in military preparedness has the potential to shift the current measures of power, greatly changing the hegemonic competition in favor of China. States that may not have traditional measures of power, such as a large standing army or high military spending, could gain power through their development of cyber technology, as well as by developing relationships with non-state actors.

In order to prevent a major security attack such as that experienced in Estonia, laws and principles must be established to create and maintain order among digital consumers. Establishment of these policies should target different forms of cybercrime and create guidelines for internet use within state borders. The International Governance Forum held by the UN focused on cybercrime, with topics including how to combat fake news and other dangers in cyberspace. The intended outcomes of the forum were to provide strategies to better protect international cyberspace, limiting the potential sources of cybercrime[25]. States could voluntarily agree to participate in these agreements as they see fit for their constituents, with the option to opt in and out of treaties and agreements. As the structure of the internet grows to accommodate its increasing base of users, the way cyberspace is treated should also reflect its size and stature. The internet is used

by a majority of citizens in the nations in which it is available, and establishing safety standards for its use are critical.

Governing the internet could be done in the form of a UN-style council. In a forum such as this, states could have the ability to contribute to the rules affecting this arena of world power. This would then provide states that hold significant activity in cyberspace, in addition to those that aim to become more engaged, with a way to set international rules that are universally agreed upon and reflect fairness. With the establishment of global cyber rules, the supervision of the use of cyber technology in state borders could become more transparent. The use of non-state actors to carry out proxy cybercrimes for states could be lessened with higher accountability on the use of cyberspace between state borders.

The rise of "hacktivism," or hacking for the sake of political influence in the late 20th and early 21st centuries, demonstrates a need for these rules. The influential weight a single actor has on the world stage can greatly influence entire governments and organizations. "Sit-ins" on websites refer to an instance when a mass number of users log on to a website, crowding the server and potentially causing the server to shut down or experience any number of technological problems[19]. With the addition of "bot networks," a single person can lead a sit-in, influencing network access for thousands. In addition to cyber sit-in power, gaining visibility is often an important part for hacktivists and cyber attacks. Web defacements are used as a means of gaining notoriety as well as spreading a message. As the sophistication of cyber attacks develops, these defacements could become ways to disseminate false information through official government websites. An example of defacements would be the Chinese hackers who hacked Taiwanese websites, displaying pro-China messages[19].

The user-base of the internet has risen to over two billion, giving information and cyber warfare the potential to become the most dangerous and mobilized weapon of the 21st century. As the number of active internet users increases, the internet becomes an avenue in which states and non-state actors can increase their economic and diplomatic prowess through strategic and targeted manipulation of web content. The manipulation

of information provides a method for non-state actors to bribe states or individuals, accruing funds for their organizations, often by clandestine means. Non-state actors are not subject to states' laws and can perform violent and harmful acts that would elicit a strong retaliatory response if attempted in domestic settings. Since non-state actors do not work inside territorial boundaries, tracking them can prove a difficult task, resulting in the prolonged anonymity of sophisticated cyber criminals.

The hegemonic status of the United States has been solidified through its military advantages, GDP, and other means of keeping pace with world competitors. Through diplomacy and geopolitics, the United States has built a network of economic relationships, as well as political allies, to secure its physical and economic security. China has aimed to build its own network of partnerships throughout the world, in recent decades particularly within the continent of Africa. In building these networks and growing its geopolitical power, China aims to eventually become the hegemon of the international system. China is challenging the United States in its development of cyber technology and use of cyber warfare technology, a new measure of power that can undermine former units of hard power measurement. Large amounts of GDP spending used for the development of nuclear and other traditional forms of hard power could be completely wasted, should cyber warfare overtake them in practicality in this century. In addition to the efforts of hegemonic contention by China, Russia's development and willingness to use cyber arms adds an additional threat to the overall national security of the United States, as well as the cyber infrastructure of the world. Proper measures must be considered to ensure that the online infrastructure of the world is properly protected, while also protecting the sovereignty of the state. While states must have the ability to create their own regulation concerning internet use, the lack of territorial boundaries in the cyberworld call for a rethinking of the boundaries of information use and cybercrime.

The primary threat to the United States' hegemony comes in the form of cyberspace, with Russia and China benefiting through the lack of rules and punishment, as shown by their multiple incidents of political cyber interference in other states. As the United States aims to conserve its position as a hegemon,

proper defensive cyber technology is crucial. Measures of hard and soft power indicate that the United States possesses the capabilities to resist any form of land, sea, or air assault. While these are important measures of defense, in order to secure and protect its hegemonic status, the United States must focus on cyberspace as its next frontier. With such an open and vulnerable landscape, cyberspace is the most likely target for Russia and China to erode American hegemonic status.

REFERENCES

1. Mohd. Noor Mat Yazid, "The Theory of Hegemonic Stability, Hegemonic Power and International Political Economic Stability," *Global Journal of Political Science and Administration* 3, no.6 (2015): 67-79, http://www.eajournals.org/wp-content/uploads/The-Theory-of-Hegemonic-Stability-Hegemonic-Power-and-International-Political-Economic-Stability.pdf

2. Joseph S. Nye, "Soft Power, " *Foreign Policy* 80 (Autumn 1990) 153-71, doi:10.2307/1148580.

3. Adam Davidson, "How Apple Helped Create Ireland's Economies, Real and Fantastical," *New Yorker*, August 31, 2016, https://www.newyorker.com/business/currency/how-apple-helped-create-irelands-economies-real-and-fantastical

4. United Nations, "UN Charter," 2019, http://www.un.org/en/sections/un-charter/un-charter-full-text/

5. Courtney B. Smith, "Building Peace Through the Political Processes of the United Nations," *International Journal of Peace Studies* 9, no. 2 (2004): 11-29, http://www.jstor.org/stable/41852919.

6. China Africa Research Initiative, "Chinese Loans to Africa," 2017, http://www.sais-cari.org.

7. Larry Hanauer and Lyle J. Morris, *Chinese Engagement in Africa: Drivers, Reactions, and Implications for U.S. Policy* (Washington, DC: RAND Corporation, 2014), https://www.jstor.org/stable/10.7249/j.ctt6wq7ss.12

8. United States Department of Defense,"FY 2019 Budget," 2019, https://dod.defense.gov/News/SpecialReports/Budget2019.aspx

9. Peter G. Peterson Foundation,"U.S. Defense Spending Compared to Other Countries," 2018, https://www.pgpf.org/chart-archive/0053_defense-comparison

10. World Atlas, "29 Largest Armies in The World," 2018, https://www.worldatlas.com/articles/29-largest-armies-in-the-world.html

11. World Bank, "Military Expenditure," 2017, https://data.worldbank.org/indicator/MS.MIL.XPND.CD?locations=CN-RU-US

12. World Bank, "GDP," 2017, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2017&locations=US-CN-RU&start=2017&view=bar&year_high_desc=false

13. World Bank, "GDP Per Capita," 2017, https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=RU-CN-US

14. Yahoo Finance "S&P500. SNP Real Time Price," 2019, https://finance.yahoo.com/quote/%5EGSPC/

15. MOEX, "MOEX Russia Index," 2019, https://www.moex.com/en/index/IMOEX

16. RAND Corporation, "Cyber Warfare," 2019, https://www.rand.org/topics/cyber warfare.html

17. Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges* 7, no. 2 (2011): 81-103, https://www.jstor.org/stable/26461991

18. Hunt Allcott–and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election,." *The Journal of Economic Perspectives* 31 (2017): 211-35, http://www.jstor.org/stable/44235006.

19. John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-age Terrorism," in *Strategic Appraisal: The Changing Role of Information in Warfare*, ed. Zalmay M. Khalilzad and John P. White (Washington, DC: RAND Corporation, 1999), 75-112, http://www.jstor.org/stable/10.7249/mr1016af.12.

20. Patrick M. Hayden, David K. Woolrich, and Katherine D. Sobolewski, "Providing Cyber Situational Awareness on Defense Platform Networks," *The Cyber Defense Review* 2, no. 2 (2017): 125-40, http://www.jstor.org/stable/26267347.

21. Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (Summer 2011): 49-60, https://www.jstor.org/stable/26463926.

22. Joseph S. Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (Winter 2011): 18-38, http://www.jstor.org/stable/26270536.

23. Dorothy Denning, "Cyberwarriors: Activists and Terrorists Turn to Cyberspace," *Harvard International Review* 23, no. 2 (Summer 2001): 70-75. http://www.jstor.org/stable/42762711.

24. United States Department of Defense, "Department of Defense Cyber Strategy Summary," 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

25. United Nations, "Consensus on The Application of Rule of Law and UN Charter to Make Cyberspace Safe," 2018, https://www.un.org/sustainabledevelopment/blog/2018/11/consensus-on-the-application-of-rule-of-law-and-un-charter-to-make-cyberspace-safe/

26. Andrew Chatzky and James McBride,-"China's Massive Belt and Road Initiative," 2019, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

27. Aigerim Raimzhanova, "Power in IR: Hard, Soft, and Smart," 2015, http://www.culturaldiplomacy.org/academy/content/pdf/participant-papers/2015-12_annual/Power-In-Ir-By-Raimzhanova,-A.pdf