Global Focus *Vol. 2 No. 1, 2022*
http://doi.org//xxx.xxx *[pp. 17-26]*

ASEAN Digital Masterplan: Responding Cyber Security Dilemma in The Post-Covid Era

Muhammad Abdurrohim
Jilin University

ABSTRACT
The COVID-19 pandemic has brought people to stay longer to disconnected from the face-to-face world than before and rely on the cyber domain daily. Because of the pandemic, Southeast Asia countries added a new 40 million internet users and in total 400 million internet users in the region. The new environment of interaction in the virtual domain generates the bipolarity of dominant power between the U.S and China to establish how cyberspace needs to regulate. The increasing penetration of internet users in the region creates an opportunity for ASEAN to establish ASEAN digital master plan that aims to accelerate region recovery from the pandemic through cyber cooperation. Despite ASEAN as a regional institution promote openness and freedom of cyber domain among its members, ASEAN member states taking contradiction policy to its regional institution. This research tries to answer why ASEAN member states take contradiction policy to their regional institution. Utilizing government politic model theory and insecurity dilemma concept, the author argues that insecurity dilemma that faced by ASEAN member states shaping its member states taking an opposite policy of connectivity on cyberspace that regional institution digital masterplan aim for.

Keywords: ASEAN, Cyberspace, Domestic Politics, Third World, China, International Order

A. INTRODUCTION

COVID-19 has brought people to stay longer to disconnected from the face-to-face world than before and rely on the cyber domain on their daily basis. Because of the pandemic, Southeast Asia country added a new 40 million internet user and in total 400 million internet user in the region (Choudhury n.d.). The interaction of peoples within this virtual domain creates a domain that we refer to as cyberspace. Cyberspace itself known as the term's popular use often refers to the virtual environment of people's knowledge and experiences (White House 2009). As more people are connecting throughout this environment, cyberspace has starting to utilize an influence on the interaction of international relations. Cyberspace creates an equilibrium of good and bad for an international politic that need policymakers to pay attention to where an anarchical environment of cyberspace becomes a space to struggle for power among the states, especially for dominant power.

Although the ASEAN region is becoming increasingly relevant for global cybersecurity, few studies have looked into the reach of regional efforts to tackle cross-border cyber-related incidents, or whether more could be done to supplement national initiatives and promote international cooperation on the cyber domain (Heinl 2014). In response to the increasing of COVID-19 cases in the region, ASEAN as the main organization in the region releases ASEAN digital master plan that aims to accelerate recovery in the region from the pandemic (ASEAN 2021).

[*corresponding author: abdurrohim.muhm@gmail.com]

ASEAN digital master plan as a new framework for ASEAN member states digital cooperation, especially to accelerating recovery in the region from the pandemic. Amid the regional institution create a guideline to its member to support digital connectivity, there is a tendency between ASEAN member states that taking opposite direction. This trend between ASEAN members states raises the question of why ASEAN member states taking the opposite direction amid the promise of a cooperation framework within ASEAN. This article tried to explore the effect of the struggle for power between major power in cyberspace, especially between China model of digital policy and U.S digital policy, and its implications throughout ASEAN as a regional institution and ASEAN member state.

B. LITERATURE REVIEW

The current literature review is focused on the bipolarity of states deterrence model to how conducting their cyberspace in the international system. The bipolarity of power over state digital sovereignty and cyberspace consisted of U.S led alliance as an established power in the international system and China as a rising power that supported by Russian share its influence over cyberspace and state digital sovereignty. The U.S as an established power seeing cyberspaces as a new domain of international system exercise deterrence model that relies on the broad consensus on permissible and unacceptable conduct in international society is focused on substantial normative, ideational, and definitive power, articulated both unilaterally and by international organizations. On other hand, China and Russia are more focused on the correlation between ideas and the interests of those in power, and the connection between the power of one actor and the power of other influential actors in the international community (Harold, Libicki, and Cevallos 2016).

This struggle for power situation over conducting cyberspace in the international system by the U.S led alliance versus China and Russia to create prosperous literature review about digital deterrence model of cyberspace. Mueller (Mueller 2012) argues that China framework of cyberspace is heavily controlled by the state that makes internet content also more restrictive to ensure the harmony of the state. For the U.S, cyberspace believed as a self-governed entity where the community within itself need to operate how should it works (Lewis 2010). By taking economic and human rights issue into account, U.S led the alliance to believe in non-state-centred digital sovereignty, while Russia and China aggressively spread state-centred digital sovereignty with security issues and values of non-interference.

The ambiguity over the digital sovereignty of the states become the new domain of influence between both sides. U.S led alliance publish "Tallinn Manual" as a principle of international law over cyberspace. Base on Tallinn Manual, whose main focus is: the definition of sovereignty relates to network space, the statement presented as " a state can enforce control over information infrastructures and activities within its sovereign territory," Where the concept of sovereignty, based on the ruling on international law of the Island of Palmas in 1928, stressed that the internal policies of a government are separate without interference from other nations; and on this basis, cyberspace-related jurisdiction is expressed as a reference to information infrastructures in the territories of the state, airspace, coastal waters and seas territorial (including the seabed and subsoil); the immediate implication is that information infrastructures fall under the sovereignty of a country's judicial and administrative authority, independent of their specific owners or users, which is secured by sovereignty (Schmitt 2017). On other hand, because China worried about how the effect of

cyberspace destabilize social and political order (Onsos 2018), that make internet policies of China embody a centralized knowledge paradigm of Internet creation and regulatory model, which incorporates elements of capitalism, authoritarianism, and Confucianism (Han 2018).

The growing number of ASEAN internet use during the pandemic also create an opportunity to explore cyberspace issue in the region toward regional institution member states regarding their cyberspace deterrence model. Even though the ASEAN region is becoming increasingly important for global cybersecurity, few studies have looked into the scope of regional efforts to combat cross-border cyber-related incidents, or whether more could be done to supplement national initiatives and promote international cooperation (Heinl 2014).

This article desires to explain the contractionary policies that the ASEAN member state takes to ASEAN as a regional institution that tries to promote liberal value in the region. This situation also created by the effect of a power struggle between U.S led alliance deterrence model and China deterrence model over cyberspace that happens in Southeast Asia states. After ASEAN publish ASEAN digital masterplan 2025, we need to examine the possibility of ASEAN as a regional institution and ASEAN relations toward its member state. Connecting how ASEAN member conducting cyberspace policy with ASEAN digital masterplan raise a question why ASEAN member takes different approach policy to ASEAN digital masterplan and the effect of power competition over cyberspace deterrence model to the discourse of cyberspace.

C. THEORETICAL APPROACH

To explain this issue regarding ASEAN as a regional institution and ASEAN as a member state contradiction on cyberspace model, this research employed the governmental politic models by Graham T. Allison and combining it with the insecurity dilemma that most of the third world face on their security issue. Unlike security dilemma which increases the possibility of a conflict between sovereign states that often happen between the developed country, most of the third country more worried about the security issue within their country that refers to insecurity dilemma. In the third world, the instability problem faces a looming threat of violent domestic conflict (Sørensen 2007).

Three requirements need to consider by states to be generated as security dilemma: first, an intangible inconsistency between the attendees; second, ambiguity about their intentions, which can lead to a misunderstanding of threat; third, the pursuit of contradictory policies that increase insecurity, resulting in the tragedy of a dispute neither wanted (Alan Collins 2000). For third world country like most of ASEAN member state, is more concerned to what Mohammed Ayoob refers to security predicament where the internal matters of state-making and nation-building generated security issue for the state (Ayoob 1995). Regimes to stay in power are preoccupied with their security, believing it is reasonable to 'spend scarce resources on military arms, to view protest as a threatening movement to the regime seeking broader public dialogue, and to consider as risky collective movements that advocate alternative identities or loyalties (Job 1992).

The insecurity dilemma is focused on, first, how the regime's actions are paradoxical since its state-making and nation-building programmed have had the contradictory result to that project, and second, the incompetence of the regime's position since there appears to be no acceptable solutions to its problems (Alan Collins 2000). Combining it with Graham T.

Allison work on a governmental model we can examining why ASEAN member state takes paradoxical policies to their regional institution. Governmental or bureaucratic model of decision emphasizes that: first, a state's policy is best understood as the result of politic at the domestic level and negotiation by its top leaders; second, even if a leader has ultimate control or authority, he must reach a consensus with his subordinates or face getting his or her orders confused or ignored; third, even if they share the same goal, leaders have different approaches to achieving it due to personal priorities and backgrounds (Allison 1971). In third world countries, most of the regime that change to be more democratic still inherit transition problem from an authoritarian rule before, especially from military rule. Third World militaries have developed a much greater influence into the political arena; an association that might obstruct the state-building process (Tilly 1990). The consequence is that anything that affects the regime's "tranquillity" will be viewed as a threat and will be dealt with accordingly, implying that insecurity dilemmas are very likely (Alan Collins 2000). This situation created a bureaucratic policy model for the ASEAN member state.

ASEAN member state mostly is included in the criteria of third world countries. As third world countries, many ASEAN member state has different security problem and approach with developed countries. Generally, ASEAN country incorporated in democratic state after the third wave of democratization. This wave began in the mid-1970s and gained momentum as the Cold War ended and the Soviet Union fell apart in the late 1980s and early 1990s (Haggard and Kaufman 2016). After a long period of authoritarian rule, ASEAN member state tried to build democratic value within their country. However, ASEAN country inherits the conflict of a power struggle between civil and military after the democratization that became a security issue afterwards (Thomas 2003). The accumulation of insecurity dilemma and bureaucratic model create a policy that reflected ASEAN member state on cyberspace deterrence model issue.

D. RESEARCH METHOD

As highlighted before, this research seeks to analyze ASEAN member states output that have a contradiction policy with its regional institution over cyberspace. To achieve the objective, the research was done using a qualitative method with disciplined configurative several reports and government document regarding their cyber policy. Using documentary analysis of existing documents to comprehend their substantive content or to disclose deeper meanings that their nature and coverage can discover (Ritchie 2003). This article addressed official documents from related governments, reputable literature, and multiple news outlets to address the research question. The collective data then analyzed using an established theory, which government politic model by Graham T. Allison and the concept of insecurity dilemma.

E. RESULT AND ANALYSIS

Cyberspace and The Difference Approach on Cyberspace Deterrence Model

The characteristic of cyberspace has created a new dimension of interaction between the international actor in an anarchical environment. International actors need to adjust and adapt their interest in the rapid pace of cyberspace. As a new domain of influence between states, cyberspace create multi-dimensional characteristics that forming an environment

between international actor to interact. Nazli Choucri argues that there is seven characteristics of cyberspace that became a new domain of interaction (Choucri 2012).

Temporality	Replace near instantaneity for conventional temporality
Physically	Surpasses geography and physical location limits
Permeation	Penetrates authorities and borders
Fluidity	Discloses sustained adjustments and reconfigurations
Participation	Decreases obstacles to freedom of speech and activism
Attribution	Obscures actors' names and connections to actions
Accountability	Bypassing transparency mechanisms

These characteristics of cyberspace create multi-dimensional approach for international actor to adjust themselves in the pursuing of their interest in international environment. This co-existence of virtual domain (cyber) and international politic often called cyberpolitics.

Consist with Clark layered model of the internet, cyberspace itself created as a hierarchical liable system composed of (1) the physical foundations and infrastructures that allow the virtual playing field, (2) the conceptual building blocks that sustain the physical network and enable services, (3) the information material processed, distributed, or converted, and (4) the participants, organizations and consumers of diverse interest who engage in this arena in different roles (Clark et al. 2005). This layered complexity of the virtual domain applies to cyberpolitics in international relations, but at different degrees and in different modalities. However, like any political, cyber or real domain in the anarchical world of the international system, a great power will seek an opportunity to overcome its rivals and become hegemony as a final goal (Mearsheimer 2001).

Nowadays, there is the bipolarity of power that desire to conduct how cyberspace should operate in an international system, it's between U.S and China. For U.S led deterrence model over cyberspace reflected by the U.S. experience during the cold war when each side of major power could destroy each other regardless of which side had more destructive force at their control (Harold, Libicki, and Cevallos 2016). As a technology that originated in the U.S itself, the internet and cyberspace need to imitated U.S. value over the international system and community. The U.S. and its alliance have argued that cyberspace should be a free, transparent, and global environment controlled principally by a bottom-up approach driven by technical organizations, civil society, and the private sector (Segal 2020). Because of its origin, cyberspace also promoting a value of the U.S where the internet and cyberspace value automatic operating system became privacy, free speech, information access, and the function of control over it. And China tried to resist this operating system in cyberspace because they are seeing it threatening the regime value of the country.

On other hand, China tried to "resist" the manual playbook of cyberspace that already establish with a similar value to western. China tried to promote cyberspace sovereignty which is based on China experience what China phrase of "century of humiliation" from 1840 till 1949 when numerous foreign power obligatory on the Qing dynasty until it falls in 1911 and create civil disorder and war between 1912 and 1949 (Harold, Libicki, and Cevallos 2016).

Adam Segal argues that there are three objectives of China regime to promoting cyber sovereignty (Segal 2020). First, to ensure domestic stability, regime authority, and the Chinese Communist Party's (CCP) continued rule, Chinese leaders want to keep a close grip on the flow of information within the country. Second, China policymakers want to form cyberspace to strengthen Beijing's political, military, and economic influence, as well as to counteract Washington's cyber advantages. Third, Beijing wants to encourage technical independence and reliance on domestic suppliers. These three objectives pushing China to become a cyber sovereignty state which cyber sovereignty has both a capacity and a normative aspect (Creemers 2020).

The difference in the cyberspace perspective of the deterrence model between the U.S and China is reflecting how both states seeing the international system. U.S cyberspace deterrence model is influenced by U.S history during the cold war where Washington see itself in a cold war situation when their rival has destructive power that could have destroyed them (Harold, Libicki, and Cevallos 2016). For China itself, unfair agreement and predisposed by the history of humiliation when China interference by a foreign power that makes China region detached to a foreign power (Harold, Libicki, and Cevallos 2016). The history of both cyber powers also reflected by ASEAN member states in seeing cyberspace their deterrence model to follow.

ASEAN digital masterplan and Its contradiction during the pandemic

The COVID-19 pandemic has augmented request for digital service in ASEAN country more than before. People are obliged to more virtually connected on their daily basis for commerce, education, health care, politics, socializing, etc. The increasing number of internet users in ASEAN member states during the pandemic brings an opportunity to increase cyber cooperation between its members. ASEAN digital master plan appears as an opportunity guideline for ASEAN member states to cooperating in the cyber environment that aims for accelerating recovery in the region from the pandemic. One of the most important aspects of this is ensuring that cybersecurity and digital data governance best practices are widely followed, both to reduce the direct effect of a breach on businesses and customers and to create confidence (ASEAN 2021).

To mitigate the effect of the pandemic, ASEAN digital masterplan inherits liberal value for connectivity resembling the U.S deterrence model on cyberspace where emphasize private (market) and society centred taking a role in the development of cyber connectivity (ASEAN 2021). The framework provides a guideline where stressing market players in the development of internet service in the region and also encouraging governments in the region to removing unneeded regulatory barriers to these markets process. The cyber cooperation framework visioned by ASEAN aims to liberalization of cyberspace in the region to supporting market recovery from the pandemic. However, during the pandemic, the government in ASEAN member states taking a contradiction policy.

Despite the COVID-19 pandemic has created an opportunity for ASEAN member states to the development of digitalization in the region, but not every ASEAN member states has a willingness to implement it. According to freedomhouse.org, a non-profit organization that advocates the development of democracy, political freedom and human right noted that three issues emerge in cyberspace during the COVID-19 pandemic (Shahbaz and Funk 2020). First, the pandemic has been used as a pretext by political leaders to restrict access to

information. Second, COVID-19 was used by governments to justify increased surveillance powers and the deployment of new technologies that were previously considered too intrusive. Third, the systematic "splintering" of the internet into a full-fledged race for "cyber sovereignty," with each government enacting its internet laws that limit the flow of information across national borders. The pandemic has increased the trend of cyber sovereignty modelled by the China cyber deterrence model, including in ASEAN member states.

The report from freedomhouse.org that measures internet freedom as one variable of the democracy development reporting that 5 countries (Indonesia, Myanmar, Philippines, Singapore, and Vietnam) of ASEAN member has decreased of internet freedom during the pandemic (Shahbaz and Funk 2020). The other 3 countries (Cambodia, Malaysia, and Thailand) that also surveyed by the organization noted that there is stagnation of internet freedom, and the number between them remain low. The negative trend of openness of cyberspace in ASEAN member states picturing the contradiction of vision between ASEAN as a regional institution with its member states.

The contradiction of ASEAN and its member states reflected by states policies regarding how ASEAN member states handling their cyberspace policy. During the pandemic, ASEAN member states like Cambodia pass The National Internet Gateway (NIG) law where the government can tighten control of internet traffic of the country. This new law believed to have the same value with China internet model where the government can appoint an internet provider and give a little check for the government control over the internet (Prashanth Parameswaran 2021). A similar policy also appears in other ASEAN member states that aim to tighten government control over cyberspace freedom and openness.

Unlike the Cambodia government where put the legal policy to undermine cyberspace openness and connectivity, the Thailand government activated an Emergency Decree on Public Administration in the State of Emergency in response to the COVID-19 pandemic, limiting both online free speech and press freedom while also giving state officials more authority to detain and prosecute users. The policy taken by the Thailand government reflected the value of the Chinese cyberspace deterrence model where heavily rely on cyber sovereignty to stabilize the Thailand junta military regime.

Similar to the Thailand government, the Philippine government also responded to the COVID-19 pandemic with an emergency decree known as Republic Act (RA) 11469 or Bayanihan to Heal as One Act. The law gave the president broad emergency powers and further criminalized people that the government seeing as a threat for government response to handle a pandemic situation in the country. According to RA 11469, individuals and groups who "create, perpetuate, or spread false information regarding the COVID-19 crisis on social media and other platforms," particularly those who are "clearly geared to encourage uncertainty, panic, anarchy, fear, or confusion," can be penalized and put on the prison or charge fines 10.000 pesos to 1 million pesos, or both. The Republic Act reflected the increasing power of the Philippine government over cyberspace.

For the Myanmar government before the coup d'etat by the military general, the Myanmar government presented a draft bill on the prevention and control of communicable diseases in February 2020. The bill contains a clause that could result in fines and a six-month jail sentence for health officials who disseminate such health details at times when it could

trigger fear or panic (Aung Phay Kyi Soe n.d.). However, the bill remains a draft in the parliament till August 2020. The military junta uses the COVID-19 pandemic as a reason to justify power and overthrow the elected government (Ronan Lee n.d.). Since the military general taking the Myanmar government, the junta already several times shutting down internet connection to cyberspace that undermine cyber connectivity (Rebecca Ratcliffe n.d.). Myanmar military government junta respond during the pandemic rise a big challenge to ASEAN digital masterplan goals.

Other ASEAN member states like Malaysia, Indonesia, and Singapore have a similar approach in regulating the cyber domain during the pandemic. Indonesia government, from January to June 2020 arrest 17 people from 104 report that accused spread false information online during the pandemic using Electronic Information and Transactions (ITE) Law. Singapore government using the Miscellaneous Offences (Public Order and Nuisance) Act as a tool to handling false information and arrest people that proofed by the government have a connection to it (Louisa Tang n.d.). And Malaysian government often use Section 233 of the 1998 CMA and Section 505(b) of the penal code to undermine government critic, especially during the pandemic. Under this law, the Malaysia government arrest the journalist that criticizes government action that allows cruise ship from China docking in Malaysia during the pandemic (Shawn W. Crispin n.d.). The government from Indonesia, Malaysia, and Singapore using existing law that expanded to undermine the spreading of information through cyber domain during the pandemic.

ASEAN digital master plan that aims to ensure that cybersecurity and digital data governance best practices are widely followed, both to reduce the direct effect of a breach on businesses and customers and to foster confidence on online platform face the big challenge during the pandemic. The increasing government control to maintain information on virtual domain indicate similarity to China cyber deterrence model or cyber sovereignty. This situation reflected by the ASEAN member states where put cyber domain as government control, especially during the pandemic as a reason to prevent spreading of false information.

The government policy tightens control to cyberspace because of the insecurity dilemma that still faced by the states in ASEAN. I argue that the insecurity dilemma faced by ASEAN member states shaping its member states taking an opposite policy of connectivity on cyberspace that regional institution digital masterplan aim for. The insecurity dilemma among ASEAN member states emerges because of the government ambiguity about their intentions, which can lead to a misunderstanding of threat and the pursuit of contradictory policies that increase insecurity over the increasing penetration of online activity. The ASEAN digital masterplan that inherits the same value as the U.S deterrence model of cyberspace faced a challenge by ASEAN member states that develop cyber sovereignty that reflected China cyber deterrence model. ASEAN member states also replicate the problem of third world countries where international powers, whether military, political, economic, or technical, have a significant and meaningful impact on the fortunes of the state-making enterprise as well as the broader security issue that Third World countries face (Ayoob 1991). The government in ASEAN member states still faced instability within the domestic level to identify the category of threat toward regime because of the inheritance of military regime government model that experienced by most of its members.

F. CONCLUSION

The spreading of COVID-19 has brought people to stay longer to disconnected from the face-to-face world than before and rely on through the cyber domain on their daily basis. Because of the pandemic, Southeast Asia country added a new 40 million internet user and in total 400 million internet user in the region. More people are relying on virtual domain to interact with each other that create a new environment that known as cyberspace. The new environment of interaction that happens in the virtual domain generate the bipolarity of dominant power between the U.S and China to establish how cyberspace needs to conduct. U.S deterrence model emphasizes cyber freedom and openness that reflect its original value and on the other hand, China deterrence model emphasize cyber sovereignty that makes cyber domain free from the interference of foreign power. This rivalry between U.S and China influence how countries regulating their cyber domain, especially among ASEAN member states. The increasing penetration of internet user in the region creates an opportunity for ASEAN to establish a digital masterplan that aims to accelerate the recovery of the region from the pandemic through cyber cooperation among its member. ASEAN digital masterplan tries to promote internet openness and connectivity in the region that will accelerate economic recovery that crumbles during the pandemic. Despite the increasing penetration through cyberspace that generates an opportunity to establish cyber cooperation among its members, ASEAN member states taking contradiction policy toward the goal of the ASEAN digital masterplan. Utilizing government politic model theory and combining with insecurity dilemma concept, this research recognizes that the contradiction of ASEAN as a regional institution with its member. I argue that the insecurity dilemma faced by ASEAN member states shaping its member states taking an opposite policy of connectivity on cyberspace that regional institution digital masterplan aim for. The insecurity dilemma among ASEAN member states arises as a result of government uncertainty about their intentions, which can lead to a misinterpretation of threat and the pursuit of conflicting policies that increase insecurity as online activity becomes more pervasive.

DAFTAR PUSTAKA

Collins, A. (2000). *The Security Dilemmas of Southeast Asia*. Singapore: Institute of Southeast Asian Studies.

Allison, G. T. (1971). *Essence of Decision: Explaining the Cuban Missile Crisis,*. Canada: Little, Brown & Company.

ASEAN. (2021). *ASEAN DIGITAL MASTERPLAN 2025.*

Ayoob, M. (1995). *The Third World Security Predicament: State Making, Regional Conflict, and the International System*. Boulder: Lynne Rienner.

Choucri, N. (2012). *Cyberpolitics in International Relations*. Cambridge, Massachusetts: The MIT Press.

Choudhury, S. R. *Southeast Asia: 40 Million New Internet Users in 2020*. Report Finds. https://www.cnbc.com/2020/11/10/southeast-asia-40-million-new-internet-users-in-2020-report-finds.html (March 20, 2021).

Clark, D. (2005). Tussle in Cyberspace: Defining Tomorrow's Internet. *IEEE/ACM Transactions on Networking*, *13*(3), 462–475.

Creemers, R. (2020). China's Conception of Cyber Sovereignty: Rhetoric and Realization. http://dx.doi.org/10.2139/ssrn.3532421.

Haggard, S., Kaufman, R. R. (2016). Democratization during the Third Wave. *Annual Review of Political Science 19*, 125–44.

Han, R. (2018). Contesting Cyberspace in China: Online Expression and Authoritarian Resilience. *Contemporary Sociology: A Journal of Reviews, 48*(4), 673.

Harold, S., Libicki, M., Cevallos, A. (2016). *Getting to Yes with China in Cyberspace*. Santa Monica, Calif: RAND Corporation.

Heinl, C. H. (2014). Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. *Asia Policy, 18*(1), 131–59.

Job, B., (1992). *The Insecurity Dilemma: National Security of Third World States*. L. Rienner Publishers.

Lewis, J. A. (2010). Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs, 16*(2), 55–65.

Mearsheimer, J. J. (2001). *The Tragedy of Great Power Politics*. New York: W.W Norton & Company.

Mueller, M. T. (2012). *China and Global Internet Governance: A Tiger by the Tail*. In Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics, eds. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. Cambridge, Massachusetts: The MIT Press, 414.

Onsos, E. (2018). Age of Ambition: Chasing Fortune, Truth, and Faith in the New China. *Armstrong Undergraduate Journal of History, 8*(1), 416.

Ritchie, J. 2003. The Applications of Qualitative Methods to Social Research. In *QUALITATIVE RESEARCH PRACTICE: A Guide for Social Science Students and Researchers*, eds. Jane Ritchie and Jane Lewis. London: SAGE Publications Ltd.

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, United Kingdom: Cambridge University Press.

Segal, A. (2020). China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. In *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, ed. Nadège Rolland. Washington: The National Bureau of Asian Research, 85–100. https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/.

Sørensen, G. (2007). After the Security Dilemma: The Challenges of Insecurity in Weak States and the Dilemma of Liberal Values. *Security Dialogue*, *38*(3), 357–78.

Thomas, R. G.C. (2003). What Is Third World Security?. *Annual Review of Political Science* 6: 205–32.

Tilly, C. (1990). *Coercion, Capital, and European States: AD 990 - 1990*. Oxford: Blackwell Pub. http://www.ncbi.nlm.nih.gov/pubmed/11445135%5Cnhttp://www.ncbi.nlm.nih.gov/pubmed/16914980%5Cnhttp://www.ncbi.nlm.nih.gov/pubmed/18381770%5Cnhttp://www.ncbi.nlm.nih.gov/pubmed/11322980%5Cnhttp://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2323975&t.

White House. (2009). *Cyberspace Policy Review*. Security 3: 1–37. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.