The Case for Cybersecurity Cooperation in Northeast Asia: Songdo, Korea as a Minilateralist Model

Hyunwoo Jo
George Mason University Korea

Abstract

This paper examines the prospects for cybersecurity cooperation in Northeast Asia, where intensifying cyber dependencies intersect with great power rivalry. While claims of a "new era of warfare" are often overstated, cybercrime targeting private sectors has become increasingly widespread, and sophisticated attacks on critical infrastructure remain a pressing concern. Despite skepticism toward global "tech alliances," minilateral cooperation offers a more pragmatic path for trust-building and information sharing. This study addresses two central questions: Can Northeast Asian middle powers foster meaningful cybersecurity cooperation despite great power tensions? And how can Korea, through Songdo, Incheon, leverage its technological capacity and middle-power identity to establish a regional cybersecurity hub? By exploring these questions, the paper highlights the potential of Songdo as a platform for shaping norms and advancing security governance in the cyber domain.

Keywords: Cybersecurity Cooperation; Northeast Asia; Minilateralism; Middle Power Diplomacy; Songdo

Introduction

The rapid growth of information technology has transformed security, creating new vulnerabilities while challenging traditional concepts of deterrence and power. Cyber incidents are now frequent, prompting calls for stronger national and international responses. Yet scholars remain divided on whether meaningful cooperation is achievable, given diverging national interests and the lack of trust among major powers.

Northeast Asia illustrates these challenges vividly. The region is marked by deep geopolitical rivalries, but it is also highly interconnected through trade, technology, and digital infrastructure. As cyber dependencies intensify, the limitations of broad multilateral frameworks highlight the importance of smaller, flexible, minilateral arrangements. Middle powers in particular can serve as critical actors in advancing cooperation where major powers hesitate.

This paper argues that Korea, with its advanced technological base and established role as a middle power, is uniquely positioned to advance cybersecurity cooperation. By leveraging Songdo, Incheon as a hub for regional cyber incident response and cooperation, Korea can strengthen trust-building, promote information sharing, and contribute to shaping emerging cyber norms in Northeast Asia.

Asymmetrical Power in the 'Cyber Revolution'

The Cyber Revolution thesis holds that the Internet "gives militarily weaker actors asymmetric advantages, that offense is becoming easier while defense is growing harder, and that the attacker's anonymity undermines deterrence."[1] As malicious cyber activities have become increasingly recognized as a major threat to national security and warnings of a "digital Pearl Harbor" or "digital 9/11" echoed throughout the last three decades among policymakers,[2] questions have been raised regarding whether a 'cyber war' is impending and why such a war has yet to be witnessed at the global level.

Fears of an all-out global cyberwar are by no means new. "Digital weapons" targeting critical industrial control systems (ICS) have surfaced; for example, Stuxnet, a worm first discovered in 2010 and suspected to have been developed by the United States and Israel against Iran's nuclear program. At the same time, some in the intelligence community have estimated that North Korea could defeat the United States with only "600 cyber experts, three years, and $50 million" in a digital war.[3]

Yet, sophisticated cyberattacks are by no means easy to plan, design, and execute; weapons such as Stuxnet are of the strong, not the weak.[4] Further research tells us that Stuxnet had to be designed precisely with the target infrastructure in mind under large sums of funding over the span of numerous years and administrations.[5] There exists no "general purpose round for cyberwar" to this day,[6] and attacks to the likes of Stuxnet will require only the most well-funded and sophisticated actors willing to use cyber means alongside their traditional deterrence ladder.

The Transnational Threat and U.S.-China Rivalry

It is still true that more states have devoted their attention and capability toward the cyber dimension, with its growing importance and interwovenness in the traditional security arena. Much like the physical dimension, one of the most contentious and consequential rivalries in the cyber dimension is that between the United States and China, specifically

about attacks conducted by state-sponsored hackers known as advanced persistent threats (APTs).

The 2024 Annual Threat Assessment of the U.S. Intelligence Community, published by the United States' Office of the Director of National Intelligence, notes China as "the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks" amid an increasingly fragile global order.[7] In addition to its ambitions to become a science and technology superpower through heavy state-backed funding and espionage, China has on many occasions been accused of causing disruptive cyberattacks against U.S. critical infrastructure, such as its communications and energy sectors.[8]

The rise of state-backed cyberattacks, too, continues to hinder cybersecurity cooperation, as these APTs seemingly appear to operate without any restraint or regard for the traditional deterrence ladder. Meanwhile, cybercrime continues to show that it may very well be offense-dominant, as a diverse range of aggressors whose identity and motivations may be unknown operate in the domain. The purchase of exploits and vulnerabilities for malware is available at low costs on black markets, targeting a potentially limitless list of victims.[9]

Unsurprisingly, it is often the private sector hit most frequently and hardest by these attacks, suffering direct financial costs or leading to potentially devastating and cascading effects throughout a variety of systems, which is why governments have increasingly put their attention toward securing cyberspace,[10] but without any clear solution as to how they can cooperate when the aggressor at hand may be a fellow member state.

Trust in the Cyber Dimension

The problem we face with cyberattacks is that, despite their transnational risk and the growing recognition of the need for a broad agreement or alliance, nation-states have different interests and objectives that hinder cooperation in the cyber dimension. Indeed, many scholars refer to Hobbesian logic when describing the cyber dimension, a space in which the war of "all against all" is a real possibility,[11] cautioning that "the idea of ultimately negotiating a worldwide, comprehensive cybersecurity treaty is a pipe dream."[12]

This view of 'cyber pessimism' is worrying for cooperation prospects between states in cyberspace. Literature furthering these pessimists' claims has described this emerging crisis as a "tragedy of the commons,"

in which individual users overexploit and, as a result, deplete a common resource, that is trust, in cyberspace.[13] Confidence in others can be problematic because of the anonymity and ambiguity of interactions that take place online,[14] and governments are often ambivalent in their posture, valuing their use of cyberspace on the one hand but constraining its use by others on the other through censorship.[15] Pundits argue that in the absence of a central authority, cyberspace is distinguished in "providing" for itself versus the concept of states agreeing to limit their behaviors and "provide" for their collective wellbeing in the traditional understanding of the tragedy of the commons.[16]

Yet, despite grim outlooks that "conditions are not ripe for reaching and enforcing international agreements on the uses of cyberspace" and that an international cyber treaty would not "sufficiently protect states, organizations, and individuals from the various attacks arising in cyberspace,"[17] James Forsyth Jr. provides a rather optimistic view of cooperation, albeit one that emphasizes the role of great powers. Diverging from the notion of cyberspace as a self-providing realm, he argues that it is in no way independent, but rather that "the contemporary political structure has begotten today's cyber disorder."[18]

As international structures change and cyber dependencies intensify, cooperation, in this aspect, is all but inevitable for the survival of great powers, as their security "will be tightly coupled to the security of the commons."[19] In the case of China, which critics may argue as incompatible with cyber norms held by Western states, Forsyth argues that it "can *and* will learn how [to] adapt to the demands of "societal expectations" and behave in ways similar to … ordinary great powers of the past."[20]

Using this argument, cooperation seems rather inevitable in cyberspace as preexisting security challenges demonstrate. Important to note is that normative arguments alone, democratic theory, for example, cannot fully illustrate why states cooperate, as did the United States and the former Soviet Union during the Cold War: seeking "to contain war and joint action are of particular importance here."[21] As Wendt argues in the three roles that are constituted by, and constitute, three distinct "cultures" of anarchy – enemy, rival, and friend, or Hobbesian, Lockean, and Kantian – international systems are nuanced and, in the case of cyberspace, need not be "all Hobbesian all the time."[22]

Transitioning into a Global Cyber Order

Echoing these claims, great powers have a vested interest in creating a legitimate and lasting order in the international system, one that "members willingly participate and agree with [its] overall orientation"[23] and facilitate "the further growth of intergovernmental institutions and commitments."[24] Insofar as international order may be anarchic, it is not chaotic;[25] and the emergence of regimes, norms, and principles, guided by these powers, will be an inevitable step in the governance of cyberspace.

Existing cases already demonstrate the growing importance of deterring and defending against cyberattacks, albeit limited in scope. In 2021, NATO member states recognized the possibility of "significant malicious cumulative cyber activities" to invoke Article 5 of the North Atlantic Treaty and agreed upon a Comprehensive Cyber Defence Policy, aiming to integrate the cyber domain into its overall defense and deterrence strategy.[26] In the European Union, its cyber defense policy has led to the establishment of the Military Computer Emergency Response Team Operational Network (MICNET), a network of military computer emergency response teams (milCERTs) managed by the European Defence Agency.[27]

Yet, the biggest challenge in the development and creation of a global alliance has been in its purpose. Existing security arrangements, which have traditionally been led by the United States, describe its primary adversaries—Russia and China—as seeking "to degrade… critical infrastructure… and impede… military activities."[28] Yet, maintaining U.S. technological dominance is not a shared problem among states, and nor is competition against China, given their economic relations with the country. Many, including Europe, have remained largely ambivalent to the idea of a new tech regime, given their emphasis on "technology sovereignty" to become independent not only from China, but also the United States.[29]

The intensifying U.S.-China rivalry today raises much doubt as to when and if a meaningful form of cooperation will arise. The rivalry between the two nation-states has contributed to an increasingly fragile global order and economy. At the same time, the role of the United States as a hegemonic stabilizer has been questioned under the rise of China.[30] Under the first and second Trump administrations, it has reinforced a 'transactional' view on global policy by pressuring allies to take a more active role in 'burden-sharing,' as reflected in the U.S. Indo-Pacific Strategy.[31]

Some scholars have suggested that in the meantime, middle powers can emerge as a stabilizer by moving beyond the traditional alliance framework and acting as an active contributor to regional security.[32] Specifically in Northeast Asia, a region "characterized by some of the most complex and multi-layered security threats in the world,"[33] South Korea is one power with the capabilities to act as a broker and promoter for regional dialogue amid the U.S.-China power struggle. In terms of cybersecurity, in which the role of middle powers has remained conceptually underdeveloped, perhaps such could apply until cybersecurity cooperation is realized at the global level in a transitional sense.

Cooperation in Northeast Asia and South Korea as a Middle Power

Northeast Asia is a region with a history of long resistance to multilateral governance and security cooperation, "foundered on disinterest or even outright hostility from the great powers, and competition between them."[34] In a highly contentious environment, states have traditionally positioned themselves as subordinates within the great power rivalry without the rigid bloc formations seen in other regions.[35] This makes an interesting case for a key middle-power such as South Korea, which scholars have increasingly suggested take a more proactive role to shape regional stability: how does this apply to cybersecurity and what can we learn from past or existing cases of cybersecurity cooperation?

Given the uniqueness of the Northeast Asia region, which lacks a "Western-style security international organization,"[36] an alternative to the traditional 'maxilateral' approaches to facilitate cooperation among countries may be found in minilateralism, which positions itself as "a smarter, more targeted approach, bringing to the table the smallest possible number of countries needed to have the largest possible impact on solving a particular problem."[37] Consisting of three to five states meeting and interacting informally "to build regional security and order,"[38] consistently included in these groupings, such as the Quadrilateral Security Dialogue (Quad) or AUKUS, are secondary actors such as Japan, South Korea, and Australia, under the leadership of the United States.[39]

This approach, as noted by Gordon Ahl, provides "a much-needed alternative path to efficient and strong mutual cooperation on specific issues,"[40] without the 'bloat' associated with multilateral organizations. Yet, minilateralism is not without its challenges, notably the concern that these partnerships are "designed to serve large power interests and not

individual state interests in the region,"[41] thereby pressuring states to align with one side in the great power rivalry. To this, Brendan Howe proposes that middle powers, specifically second-tier powers such as Japan, South Korea, and Australia, can serve as leaders and agenda-setters in non-traditional security operations.[42]

In light of this new security challenge, then, Northeast Asia requires an approach different from that seen in the West: "a focus on non-military rather than military threats, transnational rather than national threats, and multilateral or collective rather than self-help security solutions." [43] Perhaps it may be rather easy to envisage: working alliances that share cyber threat intelligence, such as that between computer emergency response teams (CERTs) in Japan, China, and South Korea and Asia-Pacific CERT (APCERT), have shown that cooperation is not only a possibility but an extant reality.[44]

Songdo as a Hub for Cooperation

Songdo, located in Incheon, South Korea, is an inspiring spot for realizing this opportunity as a hub for international cybersecurity cooperation. What existing cybersecurity cooperation measures in the Asia-Pacific region lack, including APCERT, is a mechanism for teams to convene and respond to cyber threats cooperatively as soon as they emerge. Here, Korea can take an active role in promoting regional dialogue as a regional cybersecurity stabilizer in an uncertain and unstable environment, helping to combat cyber threats on a transnational scale.

The establishment of a 'cybersecurity hub' in Songdo will have multiple benefits for the region and country. For member states to prepare for a nimble response, such a hub would need to be easily accessible by parties, located in a technologically developed area, and ready for transnational cooperation. Songdo is one location that meets these demands: located near Incheon International Airport, situated in Korea—a technologically developed nation—and as an international city positioning itself as the gateway to Northeast Asia.

Housing the Green Climate Fund (GCF) and United Nations Office of Sustainable Development (UNOSD), the city has already been battle-tested for its capabilities for cooperation on non-traditional security issues such as the environment. Following the minilateral maxim, the hub would be operated on an informal and voluntary basis, focusing on a specific set of threats at hand, providing states with the flexibility to adapt and react as needed without the need to strategically 'balance' or 'hedge' themselves

within the U.S.-China power dynamic. This would require the country to distance itself from the U.S. 'bandwagoning' seen in existing security arrangements, at least in the cyber realm, differentiating this form of cybersecurity cooperation from the likes of U.S.-led Quad or AUKUS.

Korea has already shown its capability to lead in the cyber realm, as demonstrated by the rise of "digital minilateralism." In 2014, the country, alongside Estonia, Israel, New Zealand, and the United Kingdom, founded the Digital 5 or D5, a group of countries committed to cooperating on digital governance.[45] Now known as the Digital Nations or DN, Korea can utilize much of the framework established from this peer network to ignite a new era of cyber minilateralism. First, the DN was formed on the basis of members willing to break "from past norms and practices" and bringing in their own strengths and backgrounds from a broadly shared set of principles.[46] Defining characteristics of the group include (1) an emphasis on openness and transparency, (2) three distinct tiers of attendees, and (3) its relative informality.[47]

Likewise, a minilateral effort for cybersecurity cooperation will require members to engage in open information sharing and threat analysis, while a distinct tiering of practitioners, ministers, and leaders will allow for routine discussions that build up toward charters or declarations signed at the official level. Specifically, Korea can utilize its own CERT, KrCERT/CC, at the forefront of cybersecurity cooperation while also benefiting from the collective knowledge pooled from its members. At the expert level, working groups would be aided by a diverse range of individuals from institutions and corporations to share ideas and promote future collaboration. Here, Songdo can leverage its Global Campus and Startup Park to act as an incubator to invite and foster future talent, contributing to a stronger and more diverse cybersecurity community.

Of course, such an effort will also require a closer look at the challenges that existing minilateral arrangements face. Reaching consensus, especially on a broader set of ideas or sensitive issues such as APTs, may prove to be difficult while the network will have to pursue organizational development without the bureaucracy of multilateral organizations.[48] How resources and assets will be acquired also remains to be seen as secretariats are often voluntarily funded by member countries, as is the case with the Digital Nations.[49]

Despite the pessimistic outlooks for a comprehensive agreement or alliance in the cyber dimension, international cooperation has proven itself inevitable and effective in non-traditional security issues such as

cyberattacks. While the emergence and rise of state-based attacks have gained much traction in public discourse and among multilateral organizations, fears of a global 'cyber war' are often overblown. To this, the Northeast Asia region is rather uniquely well-positioned to react to cyber threats by building trust and confidence through cooperation. Insofar as cyber regimes may arise from a collective need by the great powers, there is an unfilled opportunity for second-tier actors to foster their regional security and norms until then, in a minilateral form.

Songdo, Korea, may be able to fill this gap through its accessibility and experience with transnational cooperation, in which a cybersecurity hub may open up avenues for collective, nimble responses and private development. To this end, Korea and Incheon have the chance to lead in intelligence sharing and creating an environment in which the city can emerge as a hub for regional cybersecurity research and development.

Conclusion

Cybersecurity has become one of the defining challenges of Northeast Asia's interconnected security environment. While sweeping global agreements remain elusive, minilateral cooperation provides a realistic path for building trust and enhancing resilience. This paper has argued that South Korea, leveraging Songdo's infrastructure and international profile, is well-positioned to act as a regional hub for cybersecurity governance and incident response. Such an initiative would not only strengthen information sharing and collective responses to cybercrime but also allow middle powers to exercise agency in shaping regional norms amid U.S.–China rivalry.

Future research should examine how Songdo's model of urban-based cooperation can be scaled to other domains of non-traditional security, such as climate resilience or health governance, and assess how middle powers collectively can sustain autonomy in digital governance. By situating Songdo as a practical testbed for minilateralism, Korea has the prime opportunity to bridge gaps in trust, advance regional cybersecurity cooperation, and help lay the foundation for a more stable and rules-based cyber order.

Notes:

[1] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365, https://doi.org/10.1080/09636412.2013.816122.

[2] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," I*nternational Security* 41, no. 3 (2017): 45, https://doi.org/10.1162/ISEC_a_00266.

[3] Mark Clayton, "The New Cyber Arms Race," *Christian Science Monitor*, March 7, 2011, https://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race.

[4] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 385.

[5] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 388.

[6] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 388.

[7] Office of the Director of National Intelligence, 2024 Annual Threat Assessment of the U.S. Intelligence Community (2024), 11, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

[8] Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[9] Samantha Bradshaw, "Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity," *Global Commission on Internet Governance Paper Series,* no. 23 (December 2015): 6, https://doi.org/10.2139/ssrn.2700899.

[10] Bradshaw, "Combating Cyber Threats," 6.

[11] James Wood Forsyth, "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace," *Strategic Studies Quarterly* 7, no. 1 (2013): 94.

[12] Adam Segal and Matthew Waxman, "Why a Cybersecurity Treaty Is a Pipe Dream," *Council on Foreign Relations*, October 27, 2011.

[13] Roger Hurwitz, "Depleted Trust in the Cyber Commons," *Strategic Studies Quarterly* 6, no. 3 (2012): 21.

[14] Hurwitz, "Depleted Trust in the Cyber Commons," 25.

[15] Hurwitz, "Depleted Trust in the Cyber Commons," 27.

[16] Forsyth, "What Great Powers Make It," 96–97.

[17] Hurwitz, "Depleted Trust in the Cyber Commons," 41.

[18] Forsyth, "What Great Powers Make It," 97.

[19] Forsyth, "What Great Powers Make It," 97–98.

[20] Forsyth, "What Great Powers Make It," 100.

[21] Forsyth, "What Great Powers Make It," 102.

[22] Alexander Wendt, *Social Theory of International Politics*, Cambridge Studies in International Relations (Cambridge: Cambridge University Press, 1999), 43; Forsyth, "What Great Powers Make It," 98.

[23] G. John Ikenberry, *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars*, New Edition (Princeton, NJ: Princeton University Press, 2019), 52, https://muse.jhu.edu/pub/267/monograph/book/62935.

[24] Ikenberry, *After Victory*, 5.

[25] Forsyth, "What Great Powers Make It," 104.

[26] North Atlantic Treaty Organization, "Cyber Defence," July 30, 2024, https://www.nato.int/cps/en/natohq/topics_78170.htm.

[27] European Defence Agency, "EDA-Led Network of Cyber Defence Teams Starts with 18 EU Countries," February 10, 2023, https://eda.europa.eu/news-and-events/news/2023/02/10/eda-led-network-of-cyber-defence-teams-starts-with-18-eu-countries.

[28] North Atlantic Treaty Organization, "Cyber Defence."

[29] James A. Lewis, "Building a Tech Alliance," in Staying Ahead in the Global Technology Race: A Roadmap for Economic Security, ed. Navin Girishankar (Washington, DC: Center for Strategic and International Studies, October 2024), 42, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-10/241029_Girishankar_Staying_Ahead.pdf.

[30] Inseok Yoo, "'Stabilizer' in International Relations: Concept and Practice," *The Korean Journal of Defense Analysis* 37, no. 2 (2025): 171, https://doi.org/10.22883/KJDA.2025.37.2.001.

[31] Yoo, "'Stabilizer' in International Relations," 171.

[32] Yoo, "'Stabilizer' in International Relations," 175.

[33] Yoo, "'Stabilizer' in International Relations," 172.

[34] Brendan M. Howe, "East Asian Security Cooperation Shortcomings and Opportunities for Second-Tier Actors in the Region," *The Journal of East Asian Affairs* 36, no. 1 (2023): 46.

[35] Yoo, "'Stabilizer' in International Relations," 174.

[36] Howe, "East Asian Security Cooperation Shortcomings and Opportunities for Second-Tier Actors in the Region," 45.

[37] Moisés Naím, "Minilateralism," *Foreign Policy*, June 21, 2009, https://foreignpolicy.com/2009/06/21/minilateralism/.

[38] William T. Tow and H. D. P. Envall, "The US and Implementing Multilateral Security in the Asia-Pacific: Can Convergent Security Work?," *IFANS Review* 19, no. 2 (2011): 62.

[39] Howe, "East Asian Security Cooperation Shortcomings and Opportunities for Second-Tier Actors in the Region," 49.

[40] Gordon Ahl, "The Benefits of Minilateral Diplomacy," *The Lighthouse*, 2009, https://www.lighthousejournal.co.uk/post/the-benefits-of-minilateral-diplomacy.

[41] Alisha Chhangani et al., "Are Minilaterals the New Multilateral in the Indo-Pacific?," *Asia Society Policy Institute* (2022), 3, https://asiasociety.org/policy-institute/are-minilaterals-new-multilateral-indo-pacific-0.

[42] Howe, "East Asian Security Cooperation Shortcomings and Opportunities for Second-Tier Actors in the Region," 63.

[43] Acharya Amitav, "Human Security: What Kind for the Asia Pacific?," in *The Human Face of Security: Asia-Pacific Perspectives*, ed. David Dickens, Canberra Papers on Strategy and Defence 144 (Australian National University, 2002); Ole Wæver, "Securitization and Desecuritization," in *On Security*, ed. Ronnie D. Lipschutz (Columbia University Press, 1995); Howe, "East Asian Security Cooperation Shortcomings and Opportunities for Second-Tier Actors in the Region," 63.

[44] Hurwitz, "Depleted Trust in the Cyber Commons"; "Member Teams," Asia Pacific Computer Emergency Team, 2025, https://www.apcert.org/about/structure/members.html#top.

[45] Tanya Filer and Antonio Weiss, *Digital Minilateralism: How Governments Cooperate on Digital Governance* (Bennett Institute for Public Policy, 2020), 5, https://www.bennettschool.cam.ac.uk/publications/digital-minilateralism-how-governments-cooperate-d/.

[46] Filer and Weiss, *Digital Minilateralism*, 10.

[47] Filer and Weiss, *Digital Minilateralism*, 11.

[48] Filer and Weiss, *Digital Minilateralism,* 15.

[49] Filer and Weiss, D*igital Minilateralism,* 17.