# Coping with Security Challenges in the Post COVID-19 World:

## Climate Change, Pandemic, Economic and Cyberspace Security

**코로나19 이후의 안보 도전과 대응:** 기후변화, 감염병, 경제안보 및 사이버 안보

Monday and Tuesday, December 11 and 12, 2023

Orchid Room, Westin Josun Seoul

EAI
EAST ASIA INSTITUTE

# Coping with Security Challenges in the Post COVID-19 World: Climate Change, Pandemic, Economic and Cyberspace Security

# 코로나19 이후의 안보 도전과 대응: 기후변화, 감염병, 경제안보 및 사이버 안보

Monday and Tuesday, December 11 and 12, 2023

Orchid Room, Westin Josun Seoul

# Table of Contents

# Greetings

The COVID-19 Pandemic demonstrates how infectious diseases, initially perceived as matters of personal hygiene and health, swiftly became concerns for collective security, seriously impacting national competitiveness and stability. Concurrently, challenges such as abnormal climate patterns and rising sea levels due to global warming, weapon development facilitated by cryptocurrency theft in cyberspace, and the weaponization of economic interdependence for coercive diplomacy underscore that national security can no longer be confined to the realm of traditional military security.

The study of "emerging security" delves into how individual safety issues at the micro-level, such as energy consumption, infectious diseases, and computer hacking, are progressively accumulated and interconnected with each other. This accumulation and interconnection surpass a critical point, evolving into a qualitatively different challenge and eventually exacerbating into macro-level national security problems. Considering the challenges faced in predicting the causes, spread, and impact of COVID-19, effectively tackling emerging security issues necessitates transcending passive concepts like "non-traditional security." It involves adopting new analytical frameworks and conducting rigorous research to gain accurate insights and craft suitable responses to these evolving challenges.

The East Asia Institute is hosting an international conference "Coping with Security Challenges in the Post COVID-19 World" to analyze the key issues and challenges in emerging security that has become increasingly more significant. By convening discussions led by experts from diverse fields—ranging from the environment, health, economy, to cybersecurity—the event seeks to chart pathways for Korea and the global community to adeptly tackle the emerging security issues.

Yul Sohn

President, East Asia Institute

# 인사말

코로나19 팬데믹은 개인 위생과 보건의 문제로 인식된 감염병 이슈가 얼마나 급격한 속도로 국가 경쟁력과 안정성에 심대한 영향을 미치는 집단 안보의 문제로 심화될 수 있는지 여실히 보여 주었습니다. 이와 함께, 지구 온난화에 따른 이상기후 현상과 해수면 상승, 사이버 공간에서 가상 화폐 탈취를 활용한 무기 개발, 경제적 상호의존을 무기화하여 강압외교의 자산으로 삼는 문제 등은 국가안보의 문제가 더 이상 전통적 군사 안보에 머무를 수 없다는 점을 분명히 보여 줍니다.

신흥안보 개념은 이처럼 미시적 차원의 에너지 소비, 감염병, 컴퓨터 해킹 등 개별 안전 문제가 양적으로 급증하고 상호 연계되는 과정에서 임계점을 넘어서는 질적 변화를 일으켜 거시적 차원의 국가안보 문제로 확산되는 현상을 이해하기 위해 등장했습니다. 코로나19의 발생 원인과 확산 경로 및 파급 효과를 예측하는 것이 쉽지 않았던 것에서 보듯, 신흥안보 문제를 정확히 분석하고 이에 적절히 대응하기 위해서는 비전통 안보(non-traditional security)와 같은 소극적 개념을 넘어서는 새로운 분석과 엄밀한 연구가 필요합니다.

동아시아연구원은 “코로나19 이후의 안보 도전과 대응” 국제 컨퍼런스를 개최하여, 급증하는 신흥안보 주요 현안과 도전 과제를 논의합니다. 환경, 보건, 사이버, 경제 등 각 분야 국내외 전문가의 발표와 토론을 통해, 신흥안보 문제에 대응하는 한국과 국제사회의 방향을 모색할 수 있기를 기대합니다.

동아시아연구원
원장 손 열

# Program

Day 1: Monday, December 11, 2023

2:30 – 3:00 pm | **Opening Ceremony**
Opening Remarks: Yul Sohn (EAI; Yonsei University)
Keynote Speech: Young-Sun Ha (EAI; Seoul National University)

3:00 – 4:30 pm | **Session 1: Climate Change and International Cooperation**

**Moderator**: Younkyoo Kim (Hanyang University)

**Keynote Presentation**:
H.E. Maria Castillo-Fernandez (European Union Ambassador to the Republic of Korea)

**Presenters**:
Senem Atvur (Akdeniz University)
"*European Union's Perspective on Climate Change and Environmental Security*"
Eun-Ah Kim (National Assembly Futures Institute)
"*Defining the Supply Chain Risk of Critical Raw Materials and the Strategies of Key Countries*"
Heejin Han (Pukyong National University)
"*Climate Change and Energy Security as Reconcilable Goals*"

**Discussants**:
Taedong Lee (Yonsei University)
Eun Ju Lee (Korea University)
Young Song (Yonsei University)

4:30 – 6:00 pm | **Session 2: Health Security and the Global Vaccine Supply Chain**

**Moderator**: Yul Sohn (EAI; Yonsei University)

**Presenters**:
Yanzhong Huang (Council on Foreign Relations)
"*Pandemic Preparedness in an Era of Geopolitical Rivalries: The Challenges to Global Health Security and China's Response*"
Sun-Young Kim (Seoul National University)
"*The Global Vaccine Supply Chain after the COVID-19 Pandemic: Prospects and Challenges for Korea from the Global Health Security Perspective*"
Taekyoon Kim (Seoul National University)
"*Global South's Challenge to Global Health Security: China, India, and the Rest of the Global South*"

**Discussants**:
Seonjou Kang (Korea National Diplomatic Academy)
Manki Song (International Vaccine Institute)
Hyeyoung Chang (Chung-Ang University)

Day 2: Tuesday, December 12, 2023

3:30 – 5:00 pm | **Session 3: Conflicts and Cooperation in Cybersecurity**

**Moderator**: Won Gon Park (EAI; Ewha Womans University)

**Presenters**:
Motohiro Tsuchiya (Keio University)
"*Japan's Response to Cyber Threats in East Asia*"
So Jeong Kim (Institute for National Security Strategy)
"*Malicious Cyber Threat from DPRK: Implication for ROK*"
Minwoo Yun (Gachon University)
"*The Future of Cyberwarfare: An Emphasis of Cyber Cognitive Warfare*"

**Discussants**:
In Tae Yoo (Dankook University)
Yonghan Park (Korea Institute for Defense Analyses)
Jungmi Cha (National Assembly Futures Institute)

5:00 – 6:30 pm | **Session 4: U.S.-China Strategic Competition and Economic Security**

**Moderator**: Chaesung Chun (EAI; Seoul National University)

**Presenters**:
Kuik Cheng-Chwee (National University of Malaysia)
"*Southeast Asian Hedging amid U.S.-China 5G Competition: Explaining the Economy-Security Tradeoffs*"
Seungjoo Lee (EAI; Chung-Ang University)
"*High Technology and the Evolution of South Korea's Economic Security Strategy*"
Yongshin Kim (Inha University)
"*South Korea's Experiences of Different Economic Coercions from China and Japan and Lessons for Countering Economic Coercion*"

**Discussants**:
Wang Hwi Lee (Ajou University)
Yong Wook Lee (Korea University)
Ryo Sahashi (University of Tokyo)

# Biographies of Participants

ATVUR, Senem
CASTILLO-FERNANDEZ, Maria
CHA, Jungmi
CHANG, Hyeyoung
CHUN, Chaesung
HA, Young-Sun
HAN, Heejin
HUANG, Yanzhong
KANG, Seonjou
KIM, Eun-Ah
KIM, So Jeong
KIM, Sun-Young
KIM, Taekyoon
KIM, Yongshin
KIM, Younkyoo
KUIK, Cheng-Chwee
LEE, Eun Ju
LEE, Seungjoo
LEE, Taedong
LEE, Wang Hwi
LEE, Yong Wook
PARK, Won Gon
PARK, Yonghan
SAHASHI, Ryo
SOHN, Yul
SONG, Manki
SONG, Young
TSUCHIYA, Motohiro
YOO, In Tae
YUN, Minwoo

(in alphabetical order)

**ATVUR, Senem**
Associate Professor,
Department of International Relations, Akdeniz University

Senem Atvur is an associate professor in the Department of International Relations at Akdeniz University where she has been working since 2014. She graduated from Galatasaray University, International Relations Programme in 2004. She received her master's and PhD degrees from the Department of Public Administration at Akdeniz University where she also worked as a Research Assistant. Her Ph.D. thesis was on global water politics and the social movements against the local reflections of these politics. Between 2010-2011 she conducted research for her PhD thesis at Université de Poitiers, France. In 2014, she was granted a scholarship by the Scientific and Technological Research Council of Turkey (TUBITAK) and she completed her post-doc research at Coventry University, the Centre for Trust, Peace and Social Relations (CTPSR), England in 2015. She is interested in environmental politics, climate change and water issues, ecological security, international and regional politics. She is the author or co-author of many book chapters and articles on these subjects and she gives lectures on international politics, international security and global environmental politics.

**CASTILLO-FERNANDEZ, Maria**
Ambassador of the European Union to the Republic of Korea

Maria Castillo Fernandez, European official diplomat of Spanish nationality, now Ambassador of the European Union to the Republic of Korea, previously served as EU Ambassador in Malaysia from 2016-2020, Head of Division for India, Nepal, Bhutan, and Bangladesh since September 2012 at the European External Action Service of the European Union, in charge of managing and coordinating the European Union's overall relations with these South Asian countries as well as with the South Asia Association for Regional Cooperation (SAARC).

From 2008 to September 2012, posted in Hong Kong, representing the EU as the Head of the Office of the European Union accredited to Hong Kong and Macao SARs.

From September 2005-2008, she worked as Deputy Head of Mission at the EU Delegation in Seoul (Republic of Korea) in charge of EU political relations and economic cooperation activities with the Republic of Korea and the Democratic People's Republic of Korea.

Prior to this, Mrs. Castillo was responsible, in Brussels, for the European Commission's overall relations with the Korean Peninsula, including both Republic of Korea and DPRK (2000-2005).

Mrs. Castillo completed postgraduate studies in European law, economics and international relations with two masters, one at the College of Europe (Bruges, Belgium) and a second at the Institute of European Studies (Strasbourg, France) following a degree in law from the Universidad Autónoma de Madrid (Spain).

Her mother tongue is Spanish, but she is fluent in English and French, with good knowledge of German and Dutch and passive knowledge of Portuguese and Italian. She has some notions of Mandarin and Korean from her postings abroad.

Mrs. Castillo was decorated with the Cruz de Oficial de la Orden del Mérito Civil by the King of Spain on 24 June 2008 for strengthening relations between the EU and the Korean Peninsula.

**CHA, Jungmi**
Director of Center for International Strategies, National Assembly Futures Institute

Jungmi Cha is a Director of Center for International Strategies at National Assembly Futures Institute since 2021. She also serves as an Adjunct Professor at Yonsei University, Chair of the Chinese Politics Study Committee at the Korean Association of International Studies,
Chair of the Regional Cyber Security Studies of the Korean Association of Cyber Security Studies, and Non-resident Research Fellow of Space Security Studies Lab of Institute of International Studies at Seoul National University.
Dr. Cha received her BA and MS degree from Yonsei University, and Ph.D degree from Yonsei University in the field of International Relations and Chinese Foreign Policy. Her research is focused on Chinese Foreign Policy and Military Innovation, US-China Tech Competition, and ROK-China Relations.

**CHANG, Hyeyoung**
Associate Professor,
Department of Political Science and International Relations, Chung-Ang University

Dr. Hyeyoung Chang is an Associate Professor in the Department of Political Science and International Relations at Chung-Ang University, Republic of Korea. She holds a BA and MA in Political Science from Chung-Ang University and received an MA and Ph.D. in Political Science from the University of Southern California. Her research interests encompass comparative politics, international development cooperation, urban politics, and democracy, and she has published several articles and book chapters on these topics.

Dr. Chang also collaborates with Korea Foundations (KF) on various programs, including KF Global e-School and KF Public Diplomacy Academy. Since 2011, she has been a deputy program manager/ participating professor of the KF Global e-Shool program. She also serves as a program manager of the KF Public Diplomacy program since 2021. In addition to teaching, she actively participates in government committees such as the Committee of International Development Cooperation (2018-2022), the Ministry of Economy and Finance (2019-2022), the Ministry of Foreign Affairs (2018-present), and the Ministry of Personnel Management (2021-present).

Dr. Chang's research focuses on comparative politics, the evolution of city-regions/megacities globally, city diplomacy, international development cooperation, and democracy in crisis.

**CHUN, Chaesung**

Chair, National Security Center, East Asia Institute; Professor, Department of Political Science and International Relations, Seoul National University

Chaesung Chun is a Professor at the Department of Political Science and International Relations at Seoul National University. He is also a Chair of National Security Center of East Asian Institute(EAI). He was the President of the Korean Association of International Studies in 2021, a Director of Center for International Studies at Seoul National University, and a Vice President of the Institute of Peace and Unification Studies, Seoul National University.

He was a visiting professor at Keio University in Tokyo from 2017-2018, and 2010-2011.

He is a member or the Advisory Committee to the Ministry of Unification, Ministry of Foreign Affairs, Ministry of Defense, ROK Army and Navy. He received his B.A and M.A degree from the Seoul National University, and Ph.D degree from Northwestern University in the field of International Relations Theory. Major books include *Sovereignty and International Relations: Northeast Asian International Relations Theory: Politics among Incomplete Sovereign States* (2020), *Sovereignty and International Relations: Modern Sovereign States System and the Evolution of the Empire* (2019), *Is Politics Moral: Reinhold Niebuhr's Transcendental Realism* (2012), and *East Asian International Relations* (2011).

**HA, Young-Sun**

Chairman, Board of Trustees, East Asia Institute;
Professor Emeritus, Seoul National University

Young-Sun Ha is the Chairman of the board of trustees at the East Asia Institute (EAI) and Professor Emeritus of the Seoul National University. Dr. Ha served as a member of senior advisory group for the inter-Korean summit talks preparation committee and a member of the Presidential National Security Advisory Group (2008-2016). He received his B.A. and M.A. from Seoul National University, and holds a Ph.D. in international politics from the University of Washington. He was Professor of International Relations at Seoul National University (1980-2012). He was a research fellow at the Center for International Studies at Princeton University and the Stockholm International Peace Research Institute. His recent books and edited volumes include: *World Politics of Love: War and Peace* (2019*), A New Perspective on the Diplomatic History of Korea: Tradition and Modernity* (2019), *U.S.-China Competition in the Architecture of a Regional Order in the Asia-Pacific* (2017).

**HAN, Heejin**
Associate Professor, Division of Global and Interdisciplinary Studies, Pukyong National University

Dr. Heejin Han serves as Associate Professor in the Division of Global & Interdisciplinary Studies at Pukyong National university(PKNU). She obtained a doctoral degree in political science from Northern Illinois University(NIU) in 2011 and taught at NIU and National University in Singapore. Since she joined the PKNU in 2017, she has published several books (including edited volumes) and articles in the field of environmental and energy politics. Her most recent works include *Global Politics of Climate Change* (2023, Pusan National University Press) and "Varieties of Green Stimulus Policies: Comparative Analysis of the Green Growth and Green New Deal Policies in South Korea" (*Journal of Environment & Development*, 2023, co-authored with Taedong Lee).

**HUANG, Yanzhong**
Senior Fellow for Global Health, Council on Foreign Relations

Yanzhong Huang is a senior fellow for global health at the Council on Foreign Relations, where he directs the Global Health Governance roundtable series. He is also a professor and director of global health studies at Seton Hall University's School of Diplomacy and International Relations, where he developed the first academic concentration among U.S. professional international affairs schools that explicitly addresses the security and foreign policy aspects of health issues. He is the founding editor of *Global Health Governance: The Scholarly Journal for the New Health Security Paradigm*.

Dr. Huang has written extensively on China and global health. He is the author of *Governing Health in Contemporary China* (2013), *Toxic Politics: China's Environmental Health Crisis and Its Challenge to the Chinese State* (2020), and *The COVID-19 Pandemic and China's Global Health Leadership* (2022). His scholarly work has appeared in Survival, Foreign Affairs, Public Health, Health Security, and the China Leadership Monitor, as well as opinion pieces in the *New York Times*, the *Washington Post*, *Wall Street Journal*, and *American Journal of Public Health*, among others. In 2006, he coauthored the first scholarly article that systematically examined China's soft power.

Dr. Huang has testified before U.S. congressional committees multiple times and is regularly consulted by major media outlets, the private sector, and governmental and nongovernmental organizations on global health issues and China. He is a life member of the Council on Foreign Relations, a member of the National Committee on U.S.-China Relations, and a board member of the Institute of Global Health (Georgia). He is co-chair of the CSIS Working Group on U.S.-China Cooperation on Health Security. In 2012, InsideJersey listed him as one of the "20 Brainiest People in New Jersey." He previously was a research associate at the National Asia Research Program, a public intellectuals fellow at the National Committee on U.S.-China Relations, an associate fellow at the Asia Society, a visiting senior research fellow at the National University of Singapore, and a visiting fellow at the Center for Strategic and International Studies. He has taught at Barnard College and Columbia University. He obtained his BA and MA from Fudan University and his PhD from the University of Chicago.

**KANG, Seonjou**
Professor, Korea National Diplomatic Academy-Institute of Foreign Affairs and National Security

Seonjou KANG is a professor at Korea National Diplomatic Academy-Institute of Foreign Affairs and National Security (KNDA-IFANS). Her research centers on rules-based international order/global governance, geo-economics of Asian regionalism, and economic security. Her widely cited research includes “2023 G7 Summit,” “The US-led Indo-Pacific Economic Framework for Prosperity,” “Global Response to COVID-19: Politicization of Infectious Diseases and Decline of Global Cooperation,” “US-China Competition for Monetary Finance Hegemony,” “The US Indo-Pacific Strategy as Geo-economics,” and “South Korea and France’s Indo-Pacific Strategies: Potential Partnership and Challenges” (IFRI). She also published academic research in *Korean Journal of International Studies* (2020, 2015), *European Journal of Political Research* (2007), *The Journal of Politics* (2005), and *Journal of Peace Research* (2004).

She received her Ph.D. in political science from Michigan State University in 2000. Her other degrees are B.A. in international relations and M.A. in political science both from Seoul National University in Korea.

**KIM, Eun-Ah**
Head and Research Fellow, Innovative Growth Group, National Assembly Futures Institute

Eun Ah Kim is a Head and Research Fellow of Innovative Growth Group at the National Assembly Futures Institute. She is taking charge of policy research projects with special focus on climate change impacts, circular economy, and green transition technology. She previously served as a Head and Senior Research Scientist of Chemical Safety Research Center at Korea Research Institute of Chemical Technology, and a Research Professor at Ewha Womans University.

Dr. Kim received her B.S degree from Seoul National University, and M.S degree from Korea Advanced Institute of Science and Technology. She received her Ph.D. degree in Civil and Environmental Engineering from Stanford University.

**KIM, So Jeong**
Senior Research Fellow and Director of Emerging Security Studies,
Institute for the National Security Strategy

Dr. So Jeong KIM is a director of Emerging Security Studies and a senior research fellow of the Institute for the National Security Strategy(INSS). And she is also an adjunct fellow of Center for Strategic and International Studies(CSIS). She is currently an advisor in the science and technology field of the Ministry of Foreign Affairs and an advisor to the Korea-U.S. Cyber Security Working Group. Before joining the INSS, she worked at the National Security Research Institute(NSR) which is South Korea's government-funded research institution from 2004 to Feb. of 2022 as team lead.

Dr. KIM has spent 20 years working at the intersection of technology and policy issues of cybersecurity. Since joining NSR, she led the cybersecurity policy team and provides recommendations on cybersecurity policy and regulatory issues. She was involved in drafting South Korea's National Cyber Security Strategy, published in April 2019. She was also involved in the 4th and 5th UN Information Security Group of Governmental Experts as an adviser, and the MERIDIAN process as an adviser and organizer.

Her main research area is various policy issues regarding national cybersecurity policy such as international norm setting processes, developing confidence building measures, critical information infrastructure protection, law and regulations, national cybersecurity capacity evaluation methodology development, etc. Dr. Kim has authored or coauthored more various publications, including articles, reports and academic papers. Her recent academic paper is about the evaluation of cyberattack severity and proposing national response matrix and recently contribute to the CEIP paper and EU ISS. Dr. KIM received her Ph.D. in engineering from the Graduate School of Information Security of Korea University in 2005. She earned a Master degree in political science and a Bachelor in history.

**KIM, Sun-Young**
Associate Professor, Graduate School of Public Health, Seoul National University

Sun-Young Kim is an associate professor of Graduate School of Public Health at Seoul National University, in which she serves as a Director of Center for Global Health Research and a Deputy Vice President of International Affairs. She is a member of advisory committees at World Health Organization, Korea's Prime Minister's Office, and Korea International Cooperation Agency. Dr. Kim received her Ph.D. degree from Harvard University and served as Research Scientist at Harvard School of Public Health, Consultant of U.S. Centers for Disease Control and Prevention, and Assistant Professor at University of Texas. She also served as a visiting scholar at Heidelberg University and Max Planck Institute for Comparative Public Law and International Law.

**KIM, Taekyoon**
Professor, Graduate School of International Studies, Seoul National University

Taekyoon Kim is a professor of international development at the Graduate School of International Studies (GSIS) at Seoul National University. Prior to SNU, he was assistant professor at Ewha Womans University and Waseda University. He received a B.A. in Sociology and a M.A. in International Studies from SNU, a M.Phil in International Relations and a D.Phil in Social Policy from the University of Oxford, and a Ph.D. in International Relations from the Johns Hopkins School of Advanced International Studies SAIS). He is currently working for the SNU Social Responsibility as the Chair, and was appointed as an Executive Director of the Korea International Cooperation Agency (KOICA), a Board Member of the National Committee on Sustainable Development Cooperation at the Prime Minister's Office, the Policy Committee at the Ministry of Justice, etc. He also worked for UNESCO as a consultant, the UNRISD as collaborative researcher, the Woodrow Wilson International Center for Scholars as Fulbright fellow, and Tubingen University and University of Paris IV as visiting professors. His main research areas include international development, international political sociology, peace studies, global south studies, and global governance.

**KIM, Yongshin**
Assistant Professor, Department of China Studies, Inha University

Yongshin Kim is an Assistant Professor in the Department of China Studies at Inha University, Incheon, South Korea. He received his Ph.D. from the University of Hawai'i at Mānoa, specializing in comparative political economy, international relations, and Asian studies with a particular emphasis on China and East Asia. Yongshin studied sociology, Chinese language & literature as an undergraduate, and political science for his master's and doctoral degrees. Combining these academic backgrounds, he takes an interdisciplinary approach to political-economic phenomena in China and East Asia. His recent research interests include the political economy of China, the U.S.-China technology competition, industrial policy, and digital governance. In his previous studies, he analyzed domestic sources of nationalistic mobilization, changes in East Asia's geopolitical structure, and rapid industrialization's political economy. He has been a visiting scholar at Peking University, Nankai University, and the Chinese University of Hong Kong. His recent works have been published in the *Korean Political Science Review*, *Pacific Focus*, *The Pacific Review*, and *China: An International Journal*, among others. He also published multiple refereed book chapters in English and Korean. His research has been funded by the National Research Foundation of Korea and the Northeast Asian History Foundation from South Korea, the Ministry of Education of the People's Republic of China, the Chiang Ching-Kuo (CCK) Foundation for International Scholarly Exchange from Taiwan, and the Konosuke Matsushita Memorial Foundation from Japan.

**KIM, Younkyoo**

Dean, Graduate School of International Studies; Director, Hanyang Institute of Energy and the Environment, Hanyang University

Younkyoo Kim is Dean of Graduate School of International Studies and Director of the Hanyang Institute of Energy and the Environment (HY-IEE) at Hanyang University. He is also Founder and Director of Center for Global Circular Economy and Center for Energy Governance and Security at the University. His main research area is international energy security. Recently, he published <Poor America, Rich China: US-China Rare Earth Element Competition and 21st Century Economic Security >, a book dealing with global supply chain issues and the security of rare earth minerals. From August 2021 to April 2022, he worked for the enactment of the <Special Act on Resource Security> as the civilian chairman of the Resource Security Diagnosis Committee of the Ministry of Trade, Industry and Energy. Professor Kim has served in numerous committees in Korean government and received several awards, including Excellence in Research from the Ministry of Education. He received Ph.D. in Political Science from Purdue University.

**KUIK, Cheng-Chwee**
Professor, International Relations; Head of Asian Studies, Institute of Malaysian and International Studies, National University of Malaysia

Kuik Cheng-Chwee is Professor of International Relations and Head of Asian Studies at the Institute of Malaysian and International Studies (IKMAS), National University of Malaysia (UKM). He is concurrently a Senior Fellow at the Foreign Policy Institute of the Johns Hopkins University School of Advanced International Studies (SAIS). He served as Head of the Writing Team for the Government of Malaysia's inaugural Defence White Paper (2020). Currently he serves as a member of the Consultative Council on Foreign Policy, Malaysian Ministry of Foreign Affairs. Previously he was a postdoctoral research associate at the Princeton-Harvard "China and the World" Program (CWP).

Professor Kuik's research focuses on small-state foreign and defence policies, Asian security, and international relations. Cheng-Chwee's publications have appeared in such peer-reviewed journals as *International Affairs*, *Pacific Review*, *Journal of Contemporary China*, *Chinese Journal of International Politics*, and *Contemporary Southeast Asia*. He is co-author with David M. Lampton and Selina Ho of *Rivers of Iron: Railroads and Chinese Power in Southeast Asia* (University of California Press, October 2020), and co-editor with Alice Ba and Sueo Sudo of *Institutionalizing East Asia: Mapping and Reconfiguring Regional Cooperation* (Routledge 2016). Kuik's essay, "The Essence of Hedging" was awarded the biennial 2009 Michael Leifer Memorial Prize by the Institute of Southeast Asian Studies for best article published in any of the three ISEAS journals. Kuik is a regular invited speaker to international conferences and closed-door policy roundtables.

His current projects include: hedging in international relations, elite legitimation and foreign policy choices, and the host-country agency in connectivity cooperation. Cheng-Chwee serves on the editorial boards/committees of *Contemporary Southeast Asia*, *Australian Journal of International Affairs*, *Asian Perspective*, *Asian Politics and Policy*, *International Journal of Asian Studies*, and *East Asian Policy*. He holds an M.Litt. from the University of St. Andrews and a PhD from Johns Hopkins University.

**LEE, Eun Ju**
Postdoctoral Fellow, Graduate School of Energy and Environment, Korea University

Eun Ju LEE is a postdoctoral fellow at the Graduate School of Energy and Environment, Korea University. Her research interests include global energy and environmental politics, comparative politics, and international relations, with a special focus on China's energy transition policy and its implication on just transition, global GHG emissions reduction markets, and energy security in a changing geopolitical landscape. Her recent publications include *Policy Implications of the Clean Heating Transition: A Case Study of Shanxi* (co-authored with Jae-Seung Lee, 2021), *China's Energy Transition Governance and Policy Implementation Gap* (co-authored with Jae-Seung Lee, 2022), and *Role of Natural Gas in China's Energy Transition Policy* (KEI Policy Brief, 2023). Lee holds a Ph.D. in Energy and Environment Policy from Korea University, an MA in International Relations from Tsinghua University (Mandarin-taught program), and a BA in International Relations from Boston University.

**LEE, Seungjoo**
Chair, Trade, Technology and Transformation Research Center, East Asia Institute;
Professor, Political Science and International Relations, Chung-Ang University

Seungjoo Lee is chair of the East Asia Institute's (EAI) Trade, Technology, and Transformation Research Center and professor of political science and international relations at Chung-Ang University. He currently serves as a member of the Ministry of Foreign Affairs' Advisory Committee on Economic Security and Foreign Affairs. Lee's research focuses on the nexus of economics and security, economic statecraft, U.S.-China technology competition, and global digital governance. He previously taught at the National University of Singapore and Yonsei University. Lee has held various positions in academic associations in Korea such as the Korean Political Science Association and the Korean Association of International Studies. He is coauthor of *The Political Economy of Change and Continuity in Korea: Twenty Years After the Crisis*. Lee also edited *Northeast Asia: Ripe for Integration?*, *International Political Economy in Cyberspace*, and *Korea's Middle Power Diplomacy*. His publications have appeared in various journals such as the *Asian Journal of Peacebuilding*, *Asian Survey*, *Comparative Political Studies*, *Korean Political Science Review*, *Natural Hazards Review*, and *Pacific Review*. Lee received his PhD in political science from the University of California, Berkeley.

**LEE, Taedong**
Underwood Distinguished Professor, Department of Political Science and International Relations, Yonsei University

TAEDONG LEE is Underwood Distinguished Professor at the Department of Political Science and International Relations in Yonsei University, Seoul. He received his bachelor's degree of Political Science, Yonsei University; Master's degree of Environmental Studies and Urban Planning, Seoul National University; and Doctoral degree in Political Science from University of Washington, Seattle. His areas of research include global and sub-national environmental politics and policy, NGO and civic politics. Professor Lee published his monograph, *Global Cities and Climate Change: Translocal Relations of Environmental Governance* (Routledge, 2015), *Politics of Energy Transition* (2021), *Climate Change and Cities* (2023), and *Civic Politics and NGO* (2023). His articles have appeared in journals including *Policy Sciences*, *Nonprofit and Voluntary Sector Quarterly*, *Policy Studies Journal*, *Energy Policy*, *International Environmental Agreements*, *Environmental and Planning C*, *Global Environmental Politics* and other Korean and international peer-reviewed journals. He serves governmental committees members including National Council on Climate and Air Quality; IPCC Korean Expert Council; and other local and national committees. Currently he is a principal investigator for a national R&D on climate change adaptation living labs (2023-2028). Professor Lee also work on book projects: translocal relations and companies and climate change.

**LEE, Wang Hwi**
Professor, Political Science, Ajou University

Wang Hwi LEE, Ph.D. (London School of Economics and Political Science), is professor of political science at Ajou University, Suwon, South Korea, where he has taught international political economy since 2006. This year, he is a vice president of Korea Association of International Studies (KAIS). Currently he advises the Ministry of Foreign Affairs, Ministry of Industry, Commerce and Energy, and Ministry of Science and ICT on economic security issues. His research interests have been focused on issues of the political economy of East Asia and the US-China strategic competition. He is the author of "The Politics of Economic Reform in South Korea: Crony Capitalism after Ten Years", "Pulling South Korea away from China's Orbit: The Strategic Implications of the Korea-US Free Trade Agreement", "US-China Cooperation on Climate Change at COP26 - Policy Implications for Environment and Energy", "Crisis Management of the COVID-19 Pandemic in South Korea, Taiwan, Hong Kong, and Singapore" and "The Emergence of Digital Economy and Fintech in the Post Pandemic Era: Implications for East Asia."

**LEE, Yong Wook**
Professor, Department of Political Science and International Relations, Korea University

Yong Wook Lee is Professor in the Department of Political Science and International Relations at Korea University (Seoul, Korea). His research examines how identities and norms affect and are affected by states and their practices within domestic and international contexts with focus on international political economy. Lee has a forthcoming book entitled *The Politics of Relations: The Making of East Asian Financial Autonomy*, which is a sequel to his earlier book (*The Japanese Challenge to the American Neoliberal World Order: Identity, Meaning, and Foreign Policy*, Stanford University Press, 2008). On the issue of China in world politics, He co-edited a volume in 2014 entitled *China's Rise and Regional Integration in East Asia: Hegemony or Community?* (Routledge). Additionally, Lee has been investigating China's efforts to internationalize its currency, the RMB, for the possibility of challenging US dollar's dominance. Lee holds a Ph.D. in International Relations at the University of Southern California. He held visiting positions at the University of Tokyo, Tüebingen University (Germany), and Korea National Defense University. Before coming to Korea University, Lee previously taught at the University of Oklahoma and Brown University.

**PARK, Won Gon**
Chair, Center for North Korea Studies, East Asia Institute;
Professor, Department of North Korean Studies, Ewha Womans University

PARK, Won Gon is currently a Professor in the Department of North Korean Studies and Director of the Institute of Unification Studies at Ewha Womans University. In addition, he holds a position as a member of the Security Office of the Presidential Office, the Ministry of Defense, and the Ministry of National Unification advisory committees. He also served as a Chair of the Center for North Korean Studies at East Asia Institute (EAI) and editor-in-chief of the Journal of Peace and Unification. He was previously a professor of international studies at Handong Global University and a research fellow at the Korea Institute for Defense Analyses (KIDA). His main research interests include (history of) international relations in Northeast Asia, ROK-US Alliance, and North Korean studies. Professor Park earned his M.A. from Boston College and received his Ph.D. in international relations from Seoul National University. His recent publications include: "U.S. Indo-Pacific Strategy and the ROK-U.S. Alliance: Integrated Deterrence and Global Posture Review (GPR)" (2022); "Kim Jong Un's Policy Direction or 'Line': Heading for Radicalization?" (2022); "The Persistence of 'Balancing': The relationship between the U.S. and North Korea under Kim Jung Un's ten years" (2021); "The U.S.'s China Policy and the Advent of the Biden Administration" (2021); "Quo Vadis America: The decay of the U.S. and the Advent of the Biden Administration" (2021).

**PARK, Yonghan**

Associate Research Fellow, Center for Security and Strategy,
Korea Institute for Defense Analyses

Yonghan Park is an Associate research fellow at the Center for Security and Strategy at Korea Institute for Defense Analyses. He is a member of board to the Korean Association of Area Studies, a member of Research Committee to the SLOC Study Group Korea, and a member of Research Committee to the Korean Association of Cybersecurity Studies.

He was a journalist at the *JoongAng* and mainly covered diplomacy & security and defense issues. He was a senior researcher at the Asiatic Research Institute at Korea University and a member of Advisory Committee to the National Institute for Unification Education.

He received his PhD degree from the Department of North Korean Studies at Korea University in the field of North Korean Politics and Military.

Major books & articles include *North Korea and Security: A study on the estimation and forecast of the quantity of North Korean nuclear warheads* (2023), *Evaluation of Stability of Kim Jong Un regime based on the Revisions of the Party Rules at the 8th Party Congress* (2022), *The Assessment of Arms Control between Two Koreas and Military Strategy* (2020), *North Korea Nuclear Poker Game* (2020), *Case and Current Status of Bloated Military Economy in North Korea* (2018), and *North Korean Contingency and The Determinants of Its Stability* (2016).

**SAHASHI, Ryo**
Associate Professor of International Relations,
Institute for Advanced Studies on Asia, The University of Tokyo

Ryo Sahashi is an Associate Professor of International Relations, Institute for Advanced Studies on Asia, the University of Tokyo. He concurrently serves as a visiting research fellow at Institute of International Affairs, Seoul National University. Dr. Sahashi specializes on international politics in East Asia. He sits on government panels including Council on the Actual State of Land Use, Advisory Panel on Science & Technology Diplomacy, and Expert Panel on 50th Year of Japan-ASEAN Friendship and Cooperation. He also works as Research Fellow of Japan Center for International Exchange; Faculty Fellow, Research Institute of Economy, Trade, and Industry; Visiting Fellow, 21st Century Policy Institute, Keidanren. He has been Visiting Associate Professor, Walter H. Shorenstein Asia Pacific Research Center, Stanford University, a Japan Scholar at the Wilson Center and a visiting fellow, Georgetown University. He sits on the Board of Advisors, National Bureau of Asian Research, U.S.A.

Dr. Sahashi received his B.A. from International Christian University and his Ph.D. from the Graduate Schools for Law and Politics at the University of Tokyo. His recent book is *US-China Rivalry: A Shift of American Strategy and Divided Worlds* (Tokyo: Chuko, 2021), *In a Search for Coexistence: the United States and Two Chinas during the Cold War* (Tokyo: Keiso, 2015), and he edits *East Asian Order in the Post-Cold War Era* (Tokyo: Keiso, 2020) and *Indo-Pacific Rising: A Handbook of History and International Relations in Asia* (Springer, forthcoming).

**SOHN, Yul**
President, East Asia Institute; Professor, Graduate School of International Studies and Underwood International College, Yonsei University

Yul Sohn is president of the East Asia Institute and professor at the Graduate School of International Studies (GSIS) and Underwood International College at Yonsei University, Seoul Korea. He served as the president of the Korean Association of International Studies (KAIS) in 2019, served as dean of GSIS from 2012 to 2016, and was president of the Association for Contemporary Japan in 2012. Before joining Yonsei University, Sohn taught at Chung-Ang University and was a visiting scholar at institutions in the University of Tokyo, Waseda University; University of North Carolina, Chapel Hill; and University of California, Berkeley. Sohn has served on a number of government advisory committees, including the South Korean Ministry of Foreign Affairs; and the South Korean Ministry of Trade; the Korean National Diplomatic Academy the Northeast Asian History Foundation; and the Korea Foundation. Sohn has written extensively on Japanese and East Asian political economics, East Asian regionalism, and global governance. His recent publications include *Japan and Asia's Contested Order* (2018, with T.J. Pempel), and *Understanding Public Diplomacy in East Asia* (2016, with Jan Melissen) both from Palgrave MacMillan, and *South Korea under US-China Rivalry: the Dynamics of the Economic-Security Nexus in the Trade Policy Making* (2019, The Pacific Review). Sohn received his PhD in political science from the University of Chicago.

**SONG, Manki**
Deputy Director General of Science, International Vaccine Institute

Dr. Manki Song is the Deputy Director General of IVI's Science Unit. He has had a longstanding interest in public health and threats to health of developing country populations. In the first years of his career, he focused on viral diseases, particularly HIV, HBV and HCV. Most recently, as the Head of the Clinical Research Lab Department at IVI, he broadened the scope of his studies to include SARS-CoV-2, MERS-CoV, and SFTS vaccine development. Before joining IVI as a research scientist in 2004, Dr. Song served as an IVI postdoctoral fellow in 2001 at Prof. Myron Levine's Center for Vaccine Development (CVD) at the University of Maryland School of Medicine in Baltimore, U.S.A. During this period, he focused on the development of new-generation measles vaccines using naked DNA, attenuated Shigella, and Salmonella. Dr. Song has also actively served on steering committees of many academic societies including the Korea Association of Immunologists and the Korean Vaccine Society. After two years of service as a Review Board member of the Korea National Research Foundation (Immunology in Medical Science), he has been working as a Program Manager of the state-run Korea Health Industry Development Institute (KHIDI) since 2015. Dr. Song received his B.Sc. degree from Seoul National University, and his M.Sc. and Ph.D. degrees from Pohang University of Science and Technology (POSTECH).

**SONG, Young**
Assistant Professor, Department of International Relations, Yonsei University

Dr. Annie Young Song is working as Assistant Professor at the Department of International Relations, Yonsei University, Mirae Campus in South Korea. Previously, she held a postdoctoral research associate position in the Faculty of Arts and Social Sciences and an Ocean Nexus Research Fellow affiliated with the University of Washington EarthLab. She obtained her PhD in politics from the University of Hong Kong and received a BAH in Economics and Psychology and an MPA from Queen's University, Canada. Her research interests cover environmental politics in the East Asian region. Currently, she examines China's role in ocean governance, including marine biodiversity and fishing activities, and environmental security in the Korean peninsula. Prior to her PhD, she worked as a data analyst at the City of Hamilton in Canada and a research analyst at the Korea Institute of Public Finance.

**TSUCHIYA, Motohiro**
Vice-President for Global Engagement and Information;
Professor, Graduate School of Media and Governance, Keio University

Dr. Motohiro Tsuchiya is Vice-President for Global Engagement and Information Technology at Keio University and Professor at Keio University Graduate School of Media and Governance. He is serving as guest editorialist of *Nikkei* since April 2019 and is an expert member of the Cybersecurity Strategy Headquarters of the Japanese government since February 2023. He authored *Intelligence and National Security* (Tokyo: Keio University Press, 2007, in Japanese), *Cyber Terror* (Tokyo: Bungeishunju, 2012, in Japanese), *Cyber Security and International Relations* (Tokyo: Chikura Shobo, 2015, in Japanese), *Cyber Great Game* (Tokyo: Chikura Shobo, 2020, in Japanese) and co-authored *Cybersecurity: Public Sector Threats and Responses* (Boca Raton, FL: CRC Press, 2012) and 40 other books. He earned his BA in political science, MA in international relations, and Ph.D. in media and governance from Keio University. He received 15th Nakasone Yasuhiro Award in 2019.

**YOO, In Tae**
Assistant Professor and Chair, Department of Political Science and International Relations;
Director, Center for Advanced Political Research, Dankook University

In Tae Yoo is an Assistant Professor and Chair in the Department of Political Science and International Relations at Dankook University, and Director of the DKU Center for Advanced Political Research. Formerly, an assistant professor at Jeonbuk National University, research professor at Yonsei University, and Visiting Research Fellow at Waseda University. He has been a member for the Internet Governance Research Council at the Korea Internet & Security Agency (KISA). Yoo has published a number of articles, book chapters and think-tank analyses, with regard to politics of cybersecurity, (international) political economy of (digital) trade, and Internet governance. Some of the topics of his work include "Bilateral Cyber Confidence Building Measures in Northeast Asia," "Cybersecurity Crisscrossing International Development Cooperation: Unraveling the Cyber Capacity Building of East Asian Middle Powers Amid Rising Great Power Conflicts," "Multistakeholderism in Global Internet Governance amid the US-China Strategic Competition," "Internet Governance Regimes by Epistemic Community: Formation and Diffusion in Asia," "The Five Eyes on Huawei: Middle Powers at the Crossroad amid Great Power Competition on Digital Hegemony," "Is the Liberal International Trade Order Fragmenting or Diverging? Contested Digital Trade Regimes through Preferential Trade Agreements," "The Emergence of Competitive Cybersecurity Multilateralism: From the 2004 UNGGE Through the 2021 OEWG."

**YUN, Minwoo**
Professor, Department of Police Science and Security Studies, Gachon University

Minwoo Yun received the first Ph.D. in Criminal Justice from the College of Criminal Justice, Sam Houston State University, USA and the second Ph.D. in International Politics from the Department of Political Science and Diplomacy, Seoul National University, ROK. Previously, he taught at Wheeling Jesuit University, USA as an Assistant Professor. He now teaches in the Department of Police Science & Security Studies at Gachon University, ROK as a Full Professor. He is also Researcher for "Future Warfare Research Center" at Seoul National University and Visiting Researcher for "Asia Center" at Seoul National University. He has also served as a consultant and advisor for various agencies and institutions including National Intelligence Service, Defense Counterintelligence Command, and other government agencies and military branches. He has published over 140 research articles, books, book chapters, and government policy reports including 20 SSCI listed journal articles. His research works include counterterrorism, transnational organized crime, cyber security, information-psychological warfare, cognitive warfare, future warfare, military affairs, intelligence, national security, and other diplomatic policies matters. Hie recent publications include "All War: A strategic discourse on cognitive warfare, information warfare, cyberwarfare, and future war (2023)," "Cyber cognitive warfare as an emerging new war domain and its strategies and tactics: Cases of Russia Ukraine war and violent extremism. *The Korean Journal of Defense Analysis* (2022)" "An Ethnographic Study on the Indonesian Immigrant Community and its Islamic Radicalization in South Korea. *Studies in Conflict & Terrorism* (2019)," "The domestic framework and system of Russian Cyber Security In Boemsik Shin, Minwoo Yun, Gyucheol Kim, and Dongju Seo (eds.). *Russian Cyber Security* (2021)."

# Position Papers

# Session 1

# Climate Change and International Cooperation

| | |
|---|---|
| **Moderator** | **Younkyoo Kim** (Hanyang University) |
| **Keynote Presentation** | **H.E. Maria Castillo-Fernandez**<br>(European Union Ambassador to the Republic of Korea) |
| **Presenters** | **Senem Atvur** (Akdeniz University)<br>"European Union's Perspective on Climate Change and Environmental Security"<br>**Eun-Ah Kim** (National Assembly Futures Institute)<br>"Defining the Supply Chain Risk of Critical Raw Materials and the Strategies of Key Countries"<br>**Heejin Han** (Pukyong National University)<br>"Climate Change and Energy Security as Reconcilable Goals" |
| **Discussants** | **Taedong Lee** (Yonsei University)<br>**Eun Ju Lee** (Korea University)<br>**Young Song** (Yonsei University) |

# European Union's Perspective on Climate Change and Environmental Security

Senem ATVUR[1]

Increasing global temperatures due to anthropogenic activities, especially the use of fossil fuels as a main energy resource since the Industrial Revolution, has degraded natural balance and broken the ecological cycles. As a result, the phenomenon of climate change has accelerated with its devastating impacts on natural, social, economic, and political systems. Climate change has become a global crisis producing several interconnected security problems. The physical impacts of climate change such as droughts and heat waves, flash/torrential rains and floods, wildfires, hurricanes and tornadoes, and sea level rise intensify all around the world. The consequences of these impacts have created new security challenges for states, humans, ecosystems, and international peace and stability. In this regard, this paper aims to reveal the security impacts of climate change through the environmental security approach. After examining the environmental security framework and its nexus with climate change, the climate security approach of the European Union which has an ambitious target to strengthen its role for climate leadership is addressed through the lens of environmental security.

## Environmental Security with Different Assumptions

Environmental degradation has emerged as one of the new security challenges. Deepening ecological problems have influenced national and international security debates. The studies that focused on the redefinition of security and national security highlighted the impacts of environmental degradation on society, economy, and polity due to the interdependency of ecosystems. Furthermore, deepening vulnerabilities and political fragility have been considered as security risks in both developed, developing and less-developed countries. These studies discussing the content of security formed a basis for the development of the environmental security literature.

Environmental security is not a monolithic approach, on the contrary, it includes different perspectives that vary according to their assumptions on the focal point of security, and response to the questions of "the security of who or what?", "how security is provided and by whom?". In this regard, national security, human security, and ecological security are the main perspectives addressing the referent object differently. For instance, the national security perspective of environmental security puts the state at the center and focuses on the environmental problems that pose threats to the state's integrity and stability. In this perspective, natural resource depletion, human-caused pressure, or scarcity are linked to environment-induced migration or conflicts in and/or between states.

Although the nexus of environment and conflict presents an important framework for analysis, it might risk neglecting the underlying factors of environmental degradation as it securitizes the environment. Despite this risk of securitization, environmental security also has

[1] Assoc. Prof., Akdeniz University, Department of International Relations, senematvur@akdeniz.edu.tr

the potential to reverse this approach and desecuritize the environment by focusing on human security or economic inequalities (Dannreuther, 2013: 137-139; Barnett, 2001). Different than the conventional approaches prioritizing state security, the human security perspective of environmental security politicizes environmental problems and their impacts on the human population -the most vulnerable in particular-, focuses on the root causes of the problems, and responds to these root causes with political tools. Therefore, the referent object becomes humans and human welfare, meanwhile revealing the link between environmental crisis, socioeconomic inequalities, and inequity turns out to be the main priority (Matthew et al., 2009). As human life depends essentially on nature and natural resources, the nexus of human and environmental security has a wider focus prioritizing food and water security, the pursuit of economic activities, cultural rituals, or the existence of some communities.

Among environmental security approaches, ecological security is by far the most critical one. To address the root causes of environmental issues, ecological security offers a more holistic and ethical perspective. In terms of protecting the ecological balance and upholding the values of justice and equity, this approach places a strong emphasis on the establishment of legally binding international norms and regimes. The biosphere, or Earth, which consists of the various interconnected ecological, social, and political systems, is the referent object of ecological security. This approach aims to balance ecology and security by holistically considering the needs of ecosystems and all living things. Beyond the human-centered perspectives, ecological security evaluates humans as a part of nature and prioritizes the safety of the planet as a complex living organism comprised of different systems. This perspective focuses on the link between the equitable and just distribution and use of natural resources. It also puts a strong emphasis on the preservation of the environment through international treaties that impose legal obligations and new international regimes that bring binding regulations even to the nation-states and resolve complex issues through cooperation based on common interests. (Pirages and DeGeest, 2004).

Along with environmental security, sustainable security also puts a lens on environmental issues. Sustainable security, which focuses on the intersection of environmental, economic, and security policies, aims to reconcile the collective security needs of states, humans, and nature within the sustainability framework. Different than the conventional security approaches, sustainable security offers a holistic perspective to address the question of "whose security". It has a balancing and dynamic focus in terms of the referent object, which is determined by prioritizing the interconnected relation between states, humans, and the environment (Khagram et al., 2003). Sustainable security highlights the value of nature and the importance of its sustainability. To maintain security, it aims to balance the protection of life support systems for human needs through ecological preservation (Khagram et al., 2003).

Climate change has become one of the most recent debates in security studies. Environmental security with all its aspects examines the multiple impacts of climate change and analyzes how to cope with this crisis.

**Whose security is threatened by climate change?**

By creating complex problems affecting biodiversity and human life as well as political, social, and economic systems, climate change has become a global crisis. The interconnected impacts of climate change create multidimensional risks for states, individuals, ecosystems, and the

global system as well. Especially the physical impacts of climate change pose the most devastating security risk. Environmental security perspectives address differently the security impacts of climate change according to how the referent object is exposed to the existential threat. For instance, sea-level rise directly threatens coastal settlements where population density and economic activities intensify; extreme weather events destroy both people's living spaces and vital economic sectors. Moreover, drought and precipitation anomalies degrade agriculture and livestock farming. All of these impacts might result in displacement and migration flows. The human-centered environmental security approach focuses especially on these issues and considers aggravating vulnerabilities as the most important climate threat.

States have had to face new challenges due to climate change. The impacts of sea-level rise, economic burdens of extreme weather events, migration flows, or political disturbance might create unexpected economic costs and socio-political grievances. The risk of total destruction for small island states is also an imminent existential threat. Furthermore, regarding the ecosystems, loss of biodiversity, deforestation, and desertification are the most complex and crucial problems. These problems threaten not only the functioning of nature but also the sustainability of human systems. Increasing physical, social, psychological, and economic vulnerabilities, pandemics, and displacement are the most fundamental challenges that communities and individuals need to tackle. However, the rights of the next generations and the question of what will be left for them seems as the most existential question regarding the future of the planet and the survival of life on Earth.

Climate change also has the potential to deteriorate global peace and security. The nexus of different security concerns such as global inequalities, regional conflicts, or worsening living conditions requires comprehensive cooperation and more drastic collective measures. In this line, the problems in terms of responsibility and inequality jeopardize the implementation of effective mitigation and adaptation policies. As the climate crisis threatens the whole Planet and the life on it, it requires collective actions based on common interests and common security concerns. In this regard, as one of the most ambitious actors in the global system, the European Union's position in terms of climate policies should be examined.

**European Union Climate Policy**

The European Union has an ambitious plan to transform the continent through a climate-neutral plan by 2050. As the frontiers of the EU have expanded, it has intersected with the climate hotspots. The Mediterranean basin, the Arctic, the North and Baltic Seas, and the Black Sea, where the increasing temperatures threaten biodiversity, local communities, economic activities, and political stability, raise the concerns of the EU. The European Green Deal is the most important strategy and policy adopted in this climate combat process. The European Climate Law adopted in 2021 is the cornerstone of the EU's climate strategy. However, before the climate policies, the European integration had begun to standardize its environmental procedures. According to article 191 of the Treaty on the Functioning of the European Union, the objectives of the environmental policy are based on the following principles (Official Journal 115, 2008):

- *reserving, protecting and improving the quality of the environment,*
- *protecting human health,*
- *prudent and rational utilisation of natural resources,*

- *promoting measures at international level to deal with regional or worldwide environmental problems, and in particular combating climate change.*

Regarding climate policies, the EU is one of the actors successfully applying international commitments. For instance, after the ratification of the Kyoto Protocol in 1998 with a target to reduce emissions by 20% by 2020, the EU redesigned its emission reduction procedures by implementing market mechanisms including carbon trade regulated by the Protocol. Between 1990-2014, the EU reduced its GHG emissions in Europe by 23% (European Environment Agency [EEA], 2015). In 2008, the EU adopted its climate and energy targets for 2020 which were based on cutting greenhouse gas emissions, increasing the share of renewable energy in energy consumption, and improving energy efficiency (Herold et al., 2019: 28-29). In 2009, the Lisbon Treaty made climate change combat a specific goal. After the ratification of the Paris Agreement in 2016, the EU communicated its nationally determined contribution (NDC) that forecasts to reduce GHG emissions by 40% by 2030 compared to 1990. In accordance with this target, European Commission President Ursula von der Leyen presented the European Green Deal plan. In March 2020, the European Climate Law was proposed and in December the European Climate Pact as a part of the Green Deal was launched by the Commission with an aim to integrate all people, communities, and organizations into the climate action.

The European Green Deal is the most comprehensive and ambitious response of the EU to the climate crisis. This transformation process aims to create a carbon-neutral continent by 2050 by considering the well-being of citizens and the needs of industry with a balanced perspective. The main pledge of the EU is to reduce emissions by 55% by 2030 compared to 1990 levels and use the emission trading system to provide new financial resources for climate and energy projects and the social dimension of the transition. In general, the European Green Deal forecasts a comprehensive transition through emissions reduction targets for different sectors, improving natural carbon sinks, updating emission trading systems and pricing pollution, investments for the green transition, and social support for citizens and small businesses (European Commission, n.d.).

**EU's position towards climate security**

When the first Climate Change Program of the EU comprising the period of 2000-2004 was published, the notion of security was not included. While the second program, which started in 2005, highlighted political challenges associated with adaptation, the climate-security link was not mentioned (Youngs, 2015: 40). Whilst the concerns about climate security have fueled by the aggravating impacts of climate change, the EU began to multiply the number of initiatives focusing on the climate-security nexus, including early warning and preparedness, conflict prevention, crisis response and management, early recovery, stabilization, and peacebuilding (European Parliament, 2022: 3).

In 2008, the Secretary General of the Council of the European Union and EU High Representative for the Common Foreign and Security Policy Javier Solana published a paper entitled "Climate Change and International Security." In this paper, climate change was defined as a threat multiplier, and the risks posed by climate change to states, human security, and international security were underlined (Council of the EU, 2008: 3). In this regard, the threats related to climate change are evaluated as resource conflict, economic damage, risk for critical infrastructures, loss of territory and border disputes, environmentally-induced migration,

instability, fragility and radicalization, tension over energy supply, and pressure on international governance. As of this date, the EU's documents on diplomacy, security, and defense have adopted a similar framework to assess the impacts of climate change. The summary of these documents' focus on climate change is as follows:

**European Security Strategy (2009):** along with the other security threats and challenges, climate change was considered with humanitarian and political aspects, and in the context of conflict (related to resource distribution). The strategy document also underlined the impacts of climate change on migration and international trade, and the importance of crisis management, preparedness, and international cooperation was emphasized.

**The EU's Global Strategy (2016):** the document took into consideration the threat-multiplying role of climate change, environmental degradation, and food and water insecurity, and the key role of multilateralism in coping with climate change and other global challenges. Moreover, the importance of inter-institutional cooperation (between member states, EU institutions, third countries, NGOs, and international organizations) was also underlined. Strengthening climate resilience in the EU borders and in third countries has become a priority for the EU, as well as making climate action an integral part of conflict prevention and sustainable security.

**5033/20 Draft Conclusion on Climate Diplomacy (2020):** This document published by the Council of the EU identified climate change as an existential threat to humanity and biodiversity and emphasized the need for an urgent collective response. It defines one of the aims of the European Green Deal as safeguarding prosperity while protecting the planet and underlines the importance of climate diplomacy by drawing attention to climate emergency and enhanced multilateral climate action. Through climate diplomacy and cooperation, the EU presents itself as a *constructive* and *assertive* partner for third parties whose capacity to decrease GHG emissions and strengthen resilience is low. The Council encourages strengthening human rights, gender equality, and women's empowerment and aims to reflect this perspective on cooperation with other regional organizations and partners.

**Climate Change and Defence Roadmap (2020):** prepared by the European External Action Service (EEAS), this document addresses the importance of environmental crimes, and the link between climate change, deforestation, and organized crime. The document claims that mitigation of climate-related risks and alleviation of environmental stress could be addressed more effectively through global cooperation and multilateral channels. New operational challenges posed by climate change are identified with the need for improved equipment resistant to extreme weather events and for more energy-efficient technologies. Reducing emissions and other environmental impacts of CSDP civilian and military missions and operations, particularly among military forces is underlined even though operational effectiveness remains the top priority.

**A Strategic Compass for Security and Defense (2022):** the Council of the EU published this document that defines climate change as a threat multiplier. It emphasizes the link between climate change, environmental degradation and natural disasters, and conflict that might be aggravated due to the competition for natural resources such as farmland and water and the exploitation of energy resources for political purposes.

**Priority of the EU in terms of environmental security**

When the EU's climate policies are examined including the Green Deal and the EU security implications, the reflections of different environmental security perspectives can be found. It is

obvious that the EU prioritizes emission cuts, industrial transformation and innovation, energy security, sustainable development and environmental protection, adaptation strategies enhanced through technology, well-being and prosperity of European citizens, and resilience with strengthening vulnerable communities in the context of climate policies. In this regard, the emphasis on human well-being, vulnerabilities, equity, and equality shows that the nexus of human and environmental security is integrated into climate policies. Furthermore, as the EU is structured through an economic integration process, safeguarding economic sectors, industry, and competitiveness, maintaining energy security, and improving renewable energy become a priority. Therefore, economic security mostly prevails over environmental security.

In this context, the EU's climate security perspective seems to be compatible with the sustainable security approach. As abovementioned, sustainable security provides a balanced framework to assess the risks of climate change and implement more effective and sustainable policies. Although the EU considers protecting economic interests and social welfare, it has adopted detailed environmental procedures and protective regulations. On the other hand, an ecological security perspective is lacking in the EU climate initiatives. Despite its emphasis on collective action, binding regulations, multilateral cooperation, and the planetary risks of the climate crisis, nature and the functioning of ecosystems remain secondary compared to humanitarian and economic needs.

Moreover, the nexus of climate change and conflict, and its relationship with migration flows are another priority of the EU security concerns. Conflict prevention and management, military operations and capabilities, the defense industry and policies are also at focus, and a green transformation for the military sector is also included in the EU climate policies. These targets in terms of the green transition of military and defense have also been compatible with geopolitical and geostrategic expectations of the EU. However, it is still controversial and vague whether the EU can deepen the framework of the common security and defense policy, and common foreign policy to place them to the supranational level. Even though the EU emphasizes collective security and action to fight the impacts of climate change, national governments have their own agendas in terms of security and foreign policy. It is also ambiguous whether national governments easily adopt and apply the requirements of the Green Deal despite its binding mechanisms.

The main challenges regarding the implementation of an environmental security perspective in the EU's climate policies might be summarized through the influence of these factors:

- Lack of supranational foreign and security policies (influence of national governments)
- Priority of economic sectors
- The impact of new sectors (using critical mineral resources) on third countries' environment
- Challenges posed by migration and the EU's controversial border security mechanisms (such as Frontex)
- Far-right governments' anti-climate and anti-EU narratives, and their influences on public opinion
- Unwillingness to contribute climate fund or international aid/funding mechanisms

Thanks to its economic and technological capacity and high awareness, the climate resilience of the European continent is relatively stronger than other regions. However, the instability and risk of conflict in other regions due to the intertwined crises threaten the stability

and security of the EU as well. In this line, the EU's ambitious climate policies might be a key to broadening multilateral cooperation for mitigation and adaptation efforts and accelerating decarbonization, but the planet needs more courageous and significant transformations to cope with these intertwined problems in the age of climate change.

**References**


Barnett, J. 2001. *The Meaning of Environmental Security: Ecological Politics and Policy in the New Security Era*. Zed Books.

Council of the EU. 2008. *Climate change and international security – Paper from the High Representative and the European Commission to the European Council*. https://data.europa.eu/doi/10.2860/50106.

Dannreuther, R. 2013. *International Security. The Contemporary Agenda*. Polity Press.

EEA. 2015. Climate change: EU shows leadership ahead of Paris with 23% emissions cut. https://www.eea.europa.eu/media/newsreleases/climate-change-eu-shows-leadership.

European Commission. n.d. Delivering the European Green Deal. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/delivering-european-green-deal_en.

European Parliament. 2022. Climate change considerations for EU security and defence policy. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/729467/EPRS_BRI(2022)729467_EN.pdf.

Herold, A., et al. 2019. *EU Environment and Climate Change Policies - State of play, current and future challenges*. Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament.

Khagram, Sanjeev et al. 2003. From the Environment and Human Security to Sustainable Security and Development. *Journal of Human Development*, 4 (2), pp.289-313.

Matthew, R. A. et al. (eds.) 2010. *Global Environmental Change and Human Security*. The MIT Press.

Official Journal 115. 2008. Consolidated version of the Treaty on the Functioning of the European Union - Part Three: Union Policies and Internal Actions - Title XX: Environment - Article 191 (ex Article 174 TEC). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12008E191:EN:HTML.

Pirages, D. C., DeGeest, T. M. 2004. *Ecological Security. An Evolutionary Perspective on Globalization*. Rowman & Littlefield.

Youngs, R. 2015. *Climate Change and European Security*. Routledge E-books.

# Defining the Supply Chain Risk of Critical Raw Materials and the Strategies of Key Countries[1]

Eun-Ah Kim

**Abstract**

As global advancements in digital and green-tech industries rapidly increase the demand for critical minerals, ensuring the stability of their supply has emerged as a significant concern. South Korea, heavily reliant on China for these essential raw materials, faces substantial risks, with dependencies on specific minerals exceeding 90%. This dependency presents a potential threat to the stable development of its strategic industries.

The dominance of China in the production and processing of these minerals, notably in lithium, nickel, and cobalt, is a crucial factor. China's strategic control over these resources, essential for green transitions, is evident in its long-term national plans. This scenario poses a significant challenge for other countries, especially considering China's monopolistic position in a context whereas environmental constraints limit mining activities in other regions.

Internationally, the reliance on China for critical minerals is increasingly recognized as a risk, prompting countries like the EU, the U.S., and South Korea to develop strategies and strengthen international cooperation for supply stabilization. The EU's recent Critical Raw Materials Act (CRMA) draft and similar initiatives by the U.S. and South Korea reflect these efforts. The national strategies adopted in these countries share common components: a strategic focus on diversifying the raw material supply chain is essential, alongside development of technologies for recycling to enhance sustainability and to minimize environmental impacts from mining.

In conclusion, the stabilization of raw material supply chains, heightened international cooperation, technological advancement, and proactive engagement in recycling and international standardization are imperative for South Korea to strengthen its position in the global market and secure economic security in the face of escalating U.S.-China technological and influence competition.

## 1. Critical raw materials supply issue: why now?

The emergence of critical raw material issues in recent years can be largely attributed to their foundational role in modern industrial societies and their significant impact on the competitiveness of future industries. Raw materials form the bedrock of production processes, and the stability of their supply is increasingly seen as a determinant of industrial competitiveness.

[1] This paper is based on the report recently published by Eun-Ah Kim, Sung-Jun Park, and Jung-Mi Cha (2023) titled 'Medium- and Long-term Strategies to Ensure the Stable Supply of Critical Raw Materials' National Assembly Futures Institute, Future Agenda 23-08.

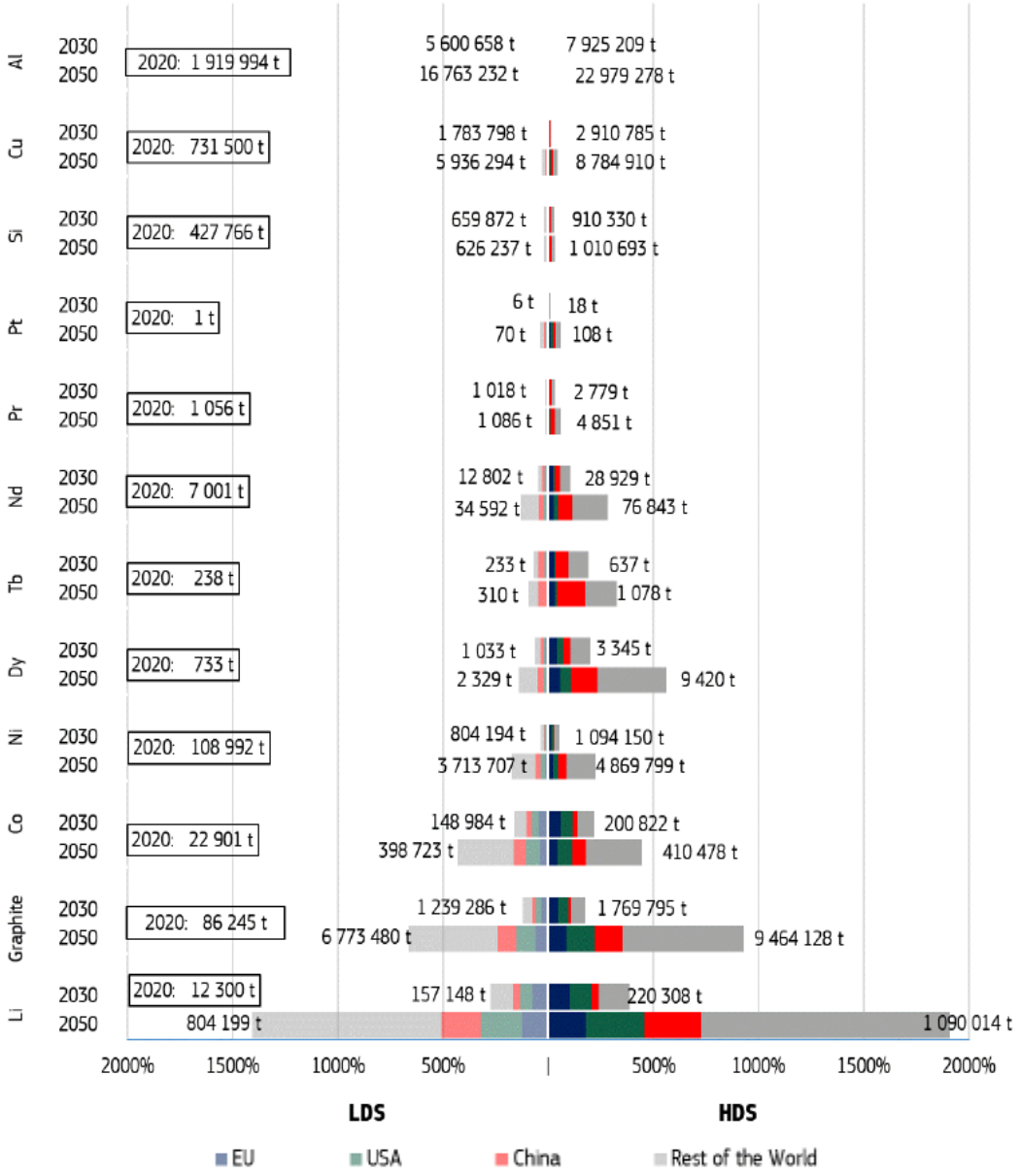



**Figure 1. Global demand forecast for major core raw materials in 2030 and 2050 compared to 2020 (HDS: high demand scenario, LDS: low demand scenario)**
Source: Carrara et al. 2023

According to projections based on the demand in 2020 and industrial growth rates, there is an expected surge in the global demand for critical raw materials by 2030 and 2050. Even in the low demand scenario, the global demand for lithium increases 13-fold by 2030 and 65-fold by 2050 compared to that in 2020.

On top the rising demand of critical raw materials and their imperial roles in the future industries, the ongoing US-China conflict complicates the national strategies to secure enough resources for each nation's competitiveness. China's strategic approach, as outlined in its "Made in China 2025" policy, aims to dominate the global market with essential raw materials, processed materials, and high-tech products. This move by China has been interpreted as the intention to replace the current hegemonic country, the United States.

Currently, China dominates the production of various essential raw materials leading the world not only in mining but also in the processing stages. This monopolistic environment has prompted other major economies, including the European Union and the United States, to develop various laws and policies to ensure a stable supply of critical raw materials and reducing their dependency on China.

## 2. What are the impending and mid-to-long term future supply chain risks in critical raw materials?

The current international landscape and its impact on critical raw materials present significant supply risks, both presently and in the mid-to-long term future. The growing tensions between Western democracies led by the United States and the European Union, and authoritarian states centered around China and Russia, have exacerbated these risks. Critical raw materials, essential for the growth and sustainability of future industries, are increasingly becoming a focal point in economic security and the strategic competition between the U.S. and China.

The primary production countries for these CRMs are listed in Table 1, with data from the United States Geological Survey (USGS) Mineral Commodity Summaries 2023, based on the 2022 production levels. Notably, there are slight discrepancies between data from the USGS and the European Commission. In any case, China holds a dominant position in the production of the entire range of rare earth elements.

**Table 1. Production and reserves of major critical raw materials**

| **Minerals** | | **Production share (mining)** | **Production share (processing)** | **Reserved** |
|---|---|---|---|---|
| Copper | | Chile (24%) | China (42%) | Chile (21%) |
| Niobium | | Brazil (90%) | | Brazil (94%) |
| Nickel | | Indonesia (48%) | China (33%)[1] | Indonesia (21%), Australia (21%) |
| Lithium | | Australia (47%) | China (56%)[1] | Chile (36%) |
| Magnesium | | China (63%) | | Russia (34%) |
| Manganese | | South Africa (36%) | China (58%)[1] | South Africa (38%) |
| Molybdenum | | China (40%) | | China (31%) |
| Vanadium | | China (70%) | | China (37%) |
| Platinum group | Platinum | South Africa (74%) | | South Africa (90%) |
| | Palladium | Russia (42%) | | |
| Strontium | | Spain (38%) | | China [2] |
| Zinc | | China (32%) | | Australia (31%) |
| Antimony | | China (55%) | | Russia (19%), China (19%) |
| Lead | | China (44%) | | Australia (44%) |
| Tin | | China (31%) | | Indonesia (17%) |
| Zirconium | | Australia (36%) | | Australia (71%) |
| Cobalt | | DR Congo (68%) | China (60%)[1] | DR Congo (48%) |

| Minerals | | Production share (mining) | Production share (processing) | Reserved |
|---|---|---|---|---|
| Chromium | | South Africa (44%) | | Kazakhstan (41%) |
| Tantalum | | DR Congo (43%) | | China [2] |
| Tungsten | | China (85%) | | China (47%) |
| Graphite | | China (65%) | | Turkey (27%) |
| Rare earth | | China (70%) | Light rare earth: China (85%)[1]<br>Heavy rare earth: China (100%)[1] | China (34%) |
| Rare earth | Neodymium | | China (85%)[1] | - |
| | Dysprosium | | China (100%)[1] | - |
| | Terbium | | China (100%)[1] | - |
| | Cerium | | China (85%)[1] | - |
| | Lanthanum | | China (85%)[1] | - |
| Gallium | | | China (98%)[1] | - |
| Silicon | | | China (68%) | - |
| Bismuth | | | China (80%) | - |
| Selenium | | | China (41%) | - |
| Aluminum | | Australia (26%)[3] | China (58%) | - |
| Indium | | | China (59%) | - |
| Titanium | | | China (58%) | - |

Source: Kim et al. (2023) based on the data from USGS(2023), European Commission(2023)

[1] The source for the data marked as 1 is the European Commission (2023). There are some differences between the data from the USGS (2023) and the European Commission (2023). The table is based on the USGS (2023) data, and additional information from the European Commission (2023) is indicated separately where available.

[2] No global reserve information available.

[3] Based on bauxite, the raw material for aluminum. Bauxite is the precursor of aluminum, and China accounts for about 54% of the production of alumina (Alumina), which is obtained by processing bauxite.

Regarding the supply stages, the European Commission differentiates between the extraction and processing stages for certain minerals. China's role in the global supply of these materials is significant, particularly in the processing sector. Notably, for strategic minerals like lithium, cobalt, manganese, and nickel, China ranks first in the processing stage. This dominance is a result of China's strategic focus on securing and developing its refining industry. This also reflects the relative underdevelopment of refining industries in advanced countries due to environmental concerns and regulations. It is very recent that these countries started legislating to address these issues.

Furthermore, beyond China's significant share in the supply of critical raw materials, many major producing countries face political instability and institutional challenges (Figure 2). The European Union assesses the vulnerability of supply chains by considering the institutional level of the supplying countries, using the World Governance Indicators (WGI) from the World Bank. This assessment divides countries into four categories based on the average of six governance

indicators. Most CRMs are produced in countries with low institutional levels or political instability, posing potential risks to supply chain stability.

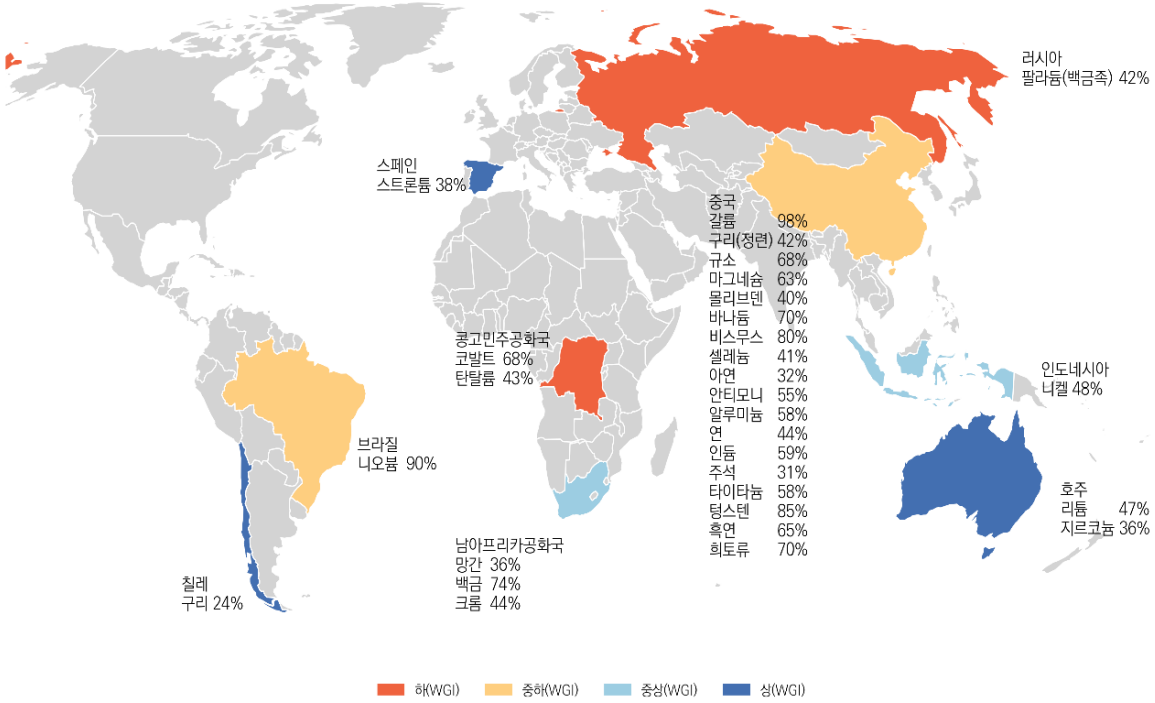



**Figure 2. Major countries producing critical raw materials and their World Governance Indicators (WGI)**

Source: Kim et al. 2023 based on the data from USGS (2023), Kaufmann and Kraay (2023)

## 3. Key countries' response to the supply chain risks in critical raw materials

Key countries around the world have increasingly recognized the dependency on China for critical raw materials as a major risk to future industries. This awareness has led to the formation of policies and systems to address supply risks, particularly focusing on China as the major supplier of these materials. Major importing countries are focusing on legislation to mitigate supply chain risks, developing diversified strategies that include technological development and international cooperation. Countries like Canada, Australia, and Indonesia, as key suppliers of critical raw materials, are revising their strategies in response to global conditions. Canada and Australia are enhancing their ESG (Environmental, Social, and Governance) strategies in mineral exploration and development, and expanding strategic partnerships with countries highly vulnerable in their supply chains.

### EU

The EU has been managing the supply risk of critical raw materials since 2008, indicating a long-standing awareness of the issue. EU has been aware of a high dependency on external sources, especially China, for materials like magnesium and rare earth elements, with import rates of 97% and 100%, respectively. The COVID-19 pandemic and geopolitical issues, such as the Russia-Ukraine conflict, have underscored the urgency of securing supply chains.

Before 2020, the EU's strategy mainly focused on monitoring these risks. Post-2020, the strategy shifted towards forming alliances and implementing practical supply stabilization measures, including shortening permit periods for mining, processing, and recycling projects, and adopting a circular economy strategy to increase recycling rates. The EU recently announced the draft of Critical Raw Material Act (CRMA) to enhance practical responses to these challenges.

**U.S.**

The U.S. Department of Energy identified 13 essential minerals crucial for clean energy technologies. The selection of these minerals reflects the strategic focus of the U.S. on securing materials vital for the transition to a cleaner energy future and reducing dependence on unstable or unfavorable foreign sources.

A significant part of the U.S. strategy is encapsulated in the Inflation Reduction Act (IRA). This act provides tax incentives for electric vehicles assembled in North America, with specific requirements regarding critical minerals and battery components. These components must be produced, processed in the U.S. or in countries with which the U.S. has a Free Trade Agreement (FTA), or recycled in North America.

Moreover, the Defense Production Act empowers the U.S. President to direct the production of essential materials and has been expanded to include minerals used in batteries (such as lithium, nickel, cobalt, graphite, and manganese). This expansion signifies the strategic importance of these materials in national defense and energy security.

**South Korea**

South Korea is also actively enhancing its response to the supply chain risks associated with critical raw materials, a vital move given the monopolization and weaponization of mineral resources by certain countries. The Ministry of Trade, Industry and Energy, in February 2023, identified 33 critical minerals, with a specific focus on 10 strategic minerals crucial for electric vehicles, secondary batteries, and semiconductors industries. These include lithium, nickel, cobalt, manganese, graphite, and five types of rare earth elements (neodymium, dysprosium, terbium, cerium, and lanthanum).

The country is developing a supply and demand map integrating overseas mine information and supply chain analysis of critical minerals. This includes establishing a supply stabilization index and an early warning system to detect risks promptly, formulating country-specific cooperation strategies, selecting strategic partner countries, supporting long-term supply contracts and mine investments, and enhancing supply chain cooperation through Free Trade Agreements (FTAs).

This strategy also includes increasing the proportion of recycled critical minerals to about 20%, emphasizing the importance of a circular economy. This involves expanding financial and tax support, establishing and operating resource recycling demonstration centers for small and medium-sized enterprises (SMEs), creating clusters for collection, recycling, distribution, and storage, introducing certification systems, and providing financial and tax support to recycling companies.

Additionally, South Korea has proposed the "National Resource Security Act" to further strengthen the supply stability of critical raw materials. Common features of the proposed bills include definition of key resources, supply and demand management, crisis response, etc.

**China**

China criticizes the U.S. and Western countries' for framing the vulnerability of its supply chains as a geopolitical risk and forming various resource and supply chain alliances that consequently isolate China. China has defined this international environment as a challenge and recognizes the need to strengthen the integration of its strategic critical mineral supply and industrial networks. This involves analyzing weaknesses and vulnerabilities in processing, refining, material research and development, manufacturing, and resource recycling. China is focusing on identifying the sources, types, and levels of supply risks for strategic critical minerals. It is also concentrating on manufacturing critical equipment, addressing technological bottlenecks and process difficulties, and building a supply chain for strategic critical minerals. This includes tracking, monitoring, analyzing, and evaluating the supply chain and establishing early warning and response mechanisms to handle various complex situations (Wang and Yuan, 2022).

In response to the U.S.'s strategic moves, China has been adapting by investing in and establishing joint ventures with companies in countries that have FTAs with the U.S., such as South Korea. This tactic aims to circumvent production location conditions stipulated by U.S. policies. Additionally, China is actively pursuing expansion into the European market, reflecting a strategic adjustment to the evolving global trade and geopolitical landscape.

On the other hand, after the EU announced the draft of the CRMA, China restricted the export of strategic raw materials like gallium and germanium as of August 2023. China's dominance in the production of these materials (80% of gallium and 60% of germanium globally) means these export restrictions could significantly impact advanced semiconductor production in countries highly dependent on these materials from China.

## 4. Suggestion for Korea's long-term future strategy

In terms of South Korea's dependence on imports for critical raw materials related to future technologies, there is a noticeable reliance on a few countries. For instance, China dominates the imports of lithium and rare earths, while Australia is significant for manganese and nickel. Congo's role in cobalt supply has been rising. In fact, Cobalt imports shifted from China being the largest in 2021 to the Democratic Republic of Congo in 2022. This highlights the possibility of diversification of supply chains.

International cooperation in developing critical raw materials is becoming more vital. Many countries with large reserves have not yet developed them. Countries with significant reserves or mining capacities are incentivized to develop their refining industries, opening opportunities for international cooperation. Initiatives like the Mineral Security Partnership (MSP) led by the United States and discussions under the Indo-Pacific Economic Framework (IPEF) reflect a growing recognition of the need for collaborative efforts to build stable supply chains.

The long-term future scenarios suggest a shift towards green growth, with an emphasis on reducing environmental pollution associated with mineral extraction and processing. The

transition phase to this new model will depend on the development of recycling technologies and industrial competitiveness in the supply of recycled resources. For improved medium- and long-term responsiveness, it is vital to foster advancements in recycling and remanufacturing technologies. Active engagement in the international standardization process, a key element for the commercialization of these technologies, is also critically important.

**References**


Carrara, Samuel, et al. 2023. *Supply Chain Analysis and Material Demand Forecast in Strategic Technologies and Sectors in the EU: A Foresight Study*. Publications Office of the European Union.

Daniel Kaufmann and Aart Kraay. 2023. Worldwide Governance Indicators, 2023 Update (www.govindicators.org)

Eun-Ah Kim, Sung-Jun Park, Jung-Mi Cha. 2023. 'Medium- and Long-term Strategies to Ensure the Stable Supply of Critical Raw Materials' National Assembly Futures Institute, Future Agenda 23-08.

European Commission. 2020. "Critical Raw Materials for Strategic Technologies and Sectors in the EU: A Foresight Study."

European Commission. 2023. "Study on the Critical Raw Materials for the EU 2023"

U. S. Geological Survey. 2023. "Mineral commodity summaries 2023".

Wang Anjian, Yuan Xiaojing. 2022. Thoughts on the security of China's strategic key mineral resources in the context of great power competition (http://cn.chinagate.cn/news/2022-12/02/content_78542546.htm)

# Climate Change and Energy Security as Reconcilable Goals

Heejin Han

## 1. Climate Change

Climate change has become one of the most challenging issues the international community is facing today. Since the first international agreement on climate change was established in 1992 at Rio, governments around the world have been making efforts to reduce their national carbon emissions for the global common objective of stopping a drastic temperature change compared to the industrial revolution period. The Paris Agreement adopted by 196 parties at the UN Climate Change Conference (COP21) in Paris in December 2015 stipulated that the parties would be pursuing the goal of holding the increase in the global average temperature to well below 2℃ above pre-industrial levels and to seek efforts to limit the temperature increase to 1.5℃ above pre-industrial levels. However, limiting global warming to 1.5℃ by the end of this century has become a target as the evidence of negative impact of climate change has accumulated at an accelerating speed and scale. To achieve this goal, greenhouse gas (GHG) emissions must peak before 2025 at the latest and decline 43% by 2030 (UNFCCC). A more recent study published in *Nature Climate Change* argues that given the accelerating climate change, carbon neutrality should be achieved by 2034, not 2050, in order to achieve 1.5℃ goal.

While there has been a growing imperative for drastic carbon emission reduction, the actions of states and non-states actors have remained quite inadequate. Particularly critical and urgent for the rapid reduction of GHG is the energy sector, which accounts for one of the biggest shares of the global emissions. Thus, energy transition to low-carbon or carbon free sources is one of the most important elements in climate change responses. Governments around the world have recognized such urgency and have reformed their energy structure and mix at home and joined various global carbon-free initiatives. For instance, over 50 national governments, together with 110 non-state actors, have joined the Powering Past Coal Alliance, an initiative launched by the UK and Canada at COP23 in 2017. However, there remain many states not participating and retaining their carbon intensive energy structure, generating the problem of carbon leakage. So as to achieve global common climate change goals, more governments need to declare coal phase-out plans and make a genuine energy transition. This means breaking with carbon-intensive social and economic paths and making political commitments for systemic changes (Gambhir 2023).

## 2. Covid-19 and Ukraine War: Energy Security

The Covid-19 and Ukraine War, as a major event in the post-Covid 19 world, can be seen as two focusing events that have unveiled multiple challenges in the global energy system. The global energy system had remained relatively stable since the two oil crises in the 1970s. Since then, the world energy landscape, despite ups and downs, has been relatively stable partially through the US role as the provider of a global public good called energy security, and partially via the

international regime building efforts to stabilize the energy market (e. g. the establishment of the international energy agency).

However, the Covid-19 and the Ukraine War erupted in late 2019 and early 2022 each have unleashed multiple energy-related challenges. While the net effects of Covid-19 on the global energy system are still being studied (Alam et al. 2023), there were some immediate challenges. The global pandemic disrupted the energy system, bringing down the demand for energy, which affected the prices negatively. The energy system experienced a rapid and steady drop in electricity demand as a result of the COVID-19 pandemic and the subsequent lockdown measures. At the same time, the pandemic delayed the deployment of renewable energy related technology and infrastructure as the world went through an unprecedented disruption in the supply chains of parts such as batteries and raw materials such as minerals.

On the other hand, the pandemic has served as a reminder that the world needs a green transition and responses to global environmental challenges to avert another large-scale virus contagion in the future. Thus, some have pointed out the necessity to accelerate the energy transition even faster. In fact, the renewable energy sector recorded a steady growth despite disruptions like the pandemic, and the year 2022 was called a "record year for renewable capacity" as renewable energy capacity was added at an unprecedented scale (Johns Hopkins 2022).

The Russian invasion of Ukraine has deepened the energy-related challenges as Russia, one of the biggest players in the global energy market (3$^{rd}$ largest producer of fossil fuels), announced its cutoff of energy provision including natural gas under ever more stringent comprehensive international sanctions. The gas price, in particular, skyrocketed in Europe as Russia stopped supplying gas through pipelines. Prices of other energy sources spiked to historical highs, threatening businesses and households. The post-Covid-19 supply chain disruptions grew even larger in the context of the war.

Thus, the Covid-19 and Ukraine War served as external shocks to the global energy system. Energy security, a concept that had long been subsided since the 1970s, has once again made its way to the top of the agenda in many countries around the world, especially among those countries with high energy dependence rates.

Energy security has no single definition as it is an umbrella term for many different policy goals. But most of the definitions agree that energy security entails energy supply continuity and the absence of, protection from, or adaptability to threats caused by or have an impact on the energy supply chain (Winzer 2012).

As explained above, the pandemic and Ukraine War posed external threats, disrupting continuous and sustained supply of energy. Thus, governments and media started to emphasize the necessity for drastic recovery of energy security through rapidly securing the energy supply to deal with the blackouts and fuel shortages. This need for an immediate action for energy security, however, raised the question of whether fulfilling the global climate change goal through energy transition should be postponed given the dire energy situations and the sense of insecurity that countries and energy consumers were feeling. That is, the pandemic and the war highlighted the importance of energy security and called for measures for maximizing it.

Faced with the energy insecurity situation, countries including those in Europe have begun to resume the operation of coal-fired and nuclear power plants as quick remedies. Amidst the call to recover energy security, some governments extended the lifelines of old fossil fuel power plants and resumed nuclear energy projects. Such actions and measures for regaining energy

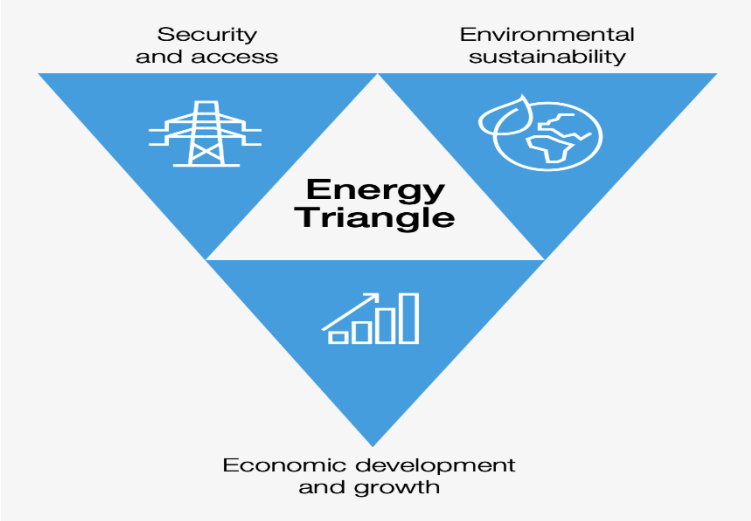
security, however, have raised the question of whether they would delay the energy transition governments around the world had been pursuing to meet climate change goals such as carbon neutrality 2050 (Colgan and Hinthorn 2023; Samandari et al. 2022).

## 3. Climate change and energy security as reconcilable goals

While understandable given the energy crises and their impact, the questions and doubts raised above assume that energy security and climate change are not compatible goals. In particular, such questions assume that renewable energy that constitutes the core of the energy transition is not desirable if energy security is the utmost priority.

However, I would like to argue that energy security and energy transition are reconcilable and compatible and should be reconciled in light of the worsening climate crisis. The World Economic Forum (WEF) already highlighted the importance of reconciling such goals, arguing that successful energy transition needs to have three elements: security and access, environmental sustainability, and economic development and growth (Figure 1). What WEF called "energy triangle" shows that these elements should be pursued together, even though, admittedly, it is not always easy to fulfill them all at the same time (World Economic Forum 2020).

**Figure 1. Energy Triangle**




Source: WEF (2020)

The European Union (EU) is a case in point, illustrating how climate change goals and long-term energy objectives can be pursued together. EU has marked itself as the leader in the global climate change and sustainable development realm. The region has been implementing various programs to achieve carbon neutrality 2050 to meet climate change challenges. EU adopted Green Deal in late 2019 for green transformation of the region and Fit for 55 containing the goal of 55% emission reduction from the 1990 level by 2030, and enacted the European Climate Law which enshrined the goal of achieving carbon neutrality by 2050. All of these EU policies commonly contain energy transition as a core element. EU has been pursuing these goals also as

a measure to make a successful transition to green and digital economy in the post-Covid 19 era and remain competitive vis-à-vis other countries and regions.

EU met challenges in its energy security situation as a result of the pandemic and the Ukraine war. As the fuel prices went up particularly after the outbreak of the Ukraine War, European countries went back to the coal and nuclear as stopgap measures. This move raised the question whether EU's climate change and energy transition goals would be undermined due to the energy security concerns. However, the EU has reinforced its climate commitments and its energy transition goals instead of overturning its long-term existing energy transition goals, and thus reversing the course of action. This move demonstrated that climate change and energy security goals can be pursued jointly if policymakers have strong will.

EU adopted REPowerEU plan in March 2022 with the goal of reducing the dependence on Russian gas by one third of the pre-war level by the end of 2022 and to eliminate the dependence at all by 2030. This is EU's declaration of weaning itself off of the Russian energy (mainly gas) supply as the ultimate and fundamental solution to maximize the region's energy security. The idea was that as long as EU remains reliant on the energy supply from Russia, its energy security will be determined by (in other words will be sensitive to) Russia's EU policy. The interdependence in the energy might be a good idea during the peace time. In fact, EU, particularly Germany believed in such interdependence with Russia as demonstrated by Nordstream 1 and 2. However, as the geopolitical landscape changed, the energy interdependence was weaponized at the expense of the parties at the energy receiving end, raising EU's vulnerability. EU's energy system was devastated by the Russian punitive responses to Western sanctions.

Launched officially in May 2022, REPowerEU aimed to help EU save energy, produce clean energy and diversify energy supplies (European Commission). REPowerEU replies on the deployment of renewables to reduce the demand for natural gas in the power sector in the short to medium term, the electrification of its transport fleet to phase out fossil fuels, and the rollout of heat pumps to significantly reduce its residential and commercial sectors' consumption of natural gas for space heating in the medium to long term (Ah-Voun et al. 2024). The EU Commission states that the program has helped save almost 20% of EU's energy consumption and doubled the new deployment of renewables. In EU 39% of electricity in 2022 came from renewables. Moreover, 80% of Russian pipeline gas was replaced in less than 8 months. These measures intended to reinforce EU's energy security in the face of external threats.

As for the renewables, REPowerEU plan intended to speed up the green transition while strengthening energy security. Within a year or so, the program managed to generate more electricity from wind and solar sources than from gas, reached a record 41GW of new solar energy capacity installed, and increased wind capacity by 16GW. In March 2023, the EU agreed on even stronger legislation to increase its renewable capacity, raising EU's binding target for 2030 to 42.5%, with the ambition to reach 45%. This would double the existing share of renewable energy in the EU region. As for gas, the pipeline imports from Russia were reduced from 132 bcm in 2021 to 62 bcm in 2022 (Ah-Voun et al. 2024).

One might argue that these things are possible given that EU has resources and technology as a regional organization with advanced member states. However, even in other parts of the world countries have been trying to reconcile climate goals with energy security concerns.

Even though there have been setbacks in the wake of the Covid-19 and Ukraine war, countries in Asia seem like they also would not give up on their energy transition policy. Japan, for instance, has been trying to recover its industrial competitiveness through the 2022 Green Transformation (GX) plan, which is also an approach to escape its long-term conundrum created by its dependence on energy impacts. Its long-term goal is to decarbonize while strengthen energy security and resilience. Not just advanced Asian countries, but also developing countries are also on similar track. China and India, whose energy uses have far-reaching implications on climate change, have raised their renewable energy targets and continued to promote green mobilities and clean energy technologies. Indonesia and Malaysia are also closing many of their existing coal fired power plants to obtain international financial support under such programs as the Just Energy Transition Partnership (Herberg 2023).

This trend might be in line with the emerging study that find the relationship between renewable energy and energy security. According to a research based on the data of OECD countries from 1985 to 2016, wind, hydroelectricity, and total renewable energy reduce energy security risk for 23 OECD countries although these positive effects are not valid for all OECD countries. As one of very few empirical studies addressing the relationship between renewable energy and energy security risks, the study shows that renewable energy, overall, can contribute to energy security of countries even though there are variations across countries (Cergibozan 2022).

This argument does not mean that achieving both green energy transition for climate change and energy security is an easy task. Renewable energy, while can be naturally obtained and carbon free, has to obtain scale economy through improved cost competitiveness. Renewable energies such as wind and solar also have to deal with the intermittency and variability challenges through energy storage system (ESS) technology and more efficient grid system management. These kinds of technology require large-scale deployment of financial resources and infrastructure. Moreover, for a successful renewable energy transition, countries, regions and cities are better off by working together and coordinating their energy demand and supply. But it is not easy to establish such a common energy community. EU also has acknowledged a strong necessity to work as an energy community only in the face of energy insecurity conditions. In addition, clean energy technology such as solar cells and batteries require sustained supply of raw materials including critical minerals. The supply chains of such ingredients and parts are at risk of disruption (due to reasons such as geopolitical concerns and resource nationalism) (Shiquan et al. 2023).

However, traditional fossil fuels such as coal, oil, and gas are not any better in terms of these risks and potential threats. Moreover, as responses to climate change become much more urgent, fossil fuel power plants carry the risk of becoming stranded assets. Compared to the renewable energy sources, oil, coal and gas require movement from the originally extracted countries to consuming countries through shipping, which entails risks and costs. Renewable energies in comparison can be deployed in a small scale for energy self-sufficiency of households and villages as can be seen in Europe (Lowitzsch et al. 2020).

Various research suggests that renewables will continue to grow. McKinsey's Global Energy Perspective 2023 states that renewable energy courses are expected to provide between 45 and 50% of global energy generation by 2040 and between 65% and 85% by 2050. While accounting for only 20% of total investments in 2012, power renewables and decarbonization technologies are projected to make up between 40 and 50% of total investments by 2040 (McKinsey 2023).

## 4. Conclusion

The Covid-19 and events like the Ukraine War that took place in the post Covid-19 world raised the question of whether climate change goals such as energy transition and energy security can be reconciled. This short paper has discussed they can be, and should be, reconciled in order the avert the climate crisis.

Energy security, particularly since the pandemic and Ukraine War, has been used as a justification for delaying the clean energy transition, but energy security it not undermined by renewable energy sources. When they reach a scale and are pursued as local projects meeting the local energy needs, they serve as steady and accessible energy sources, maximizing energy security while helping mitigate greenhouse gas emissions.

Energy shocks such as the ones triggered by the Covid-19 and Ukraine war can take place again in the post-Covid 19 world. The international community should build a resilient energy system while pursuing low carbon and carbon free energy transition in the age of deepening climate crisis.

## References


Ah-Voun, D., Chyong, C. K., & Li, C. 2024. Europe's energy security: From Russian dependence to renewable reliance. *Energy Policy*, 184, 113856.

Alam, M. M., Aktar, M. A., Idris, N. D. M., & Al-Amin, A. Q. 2023. World energy economics and geopolitics amid COVID-19 and post-COVID-19 policy direction. *World Development Sustainability*, 2, 100048.

Cergibozan, R. 2022. Renewable energy sources as a solution for energy security risk: Empirical evidence from OECD countries. *Renewable Energy*, 183, 617-626.

European Commission. n.d. "REPowerEU at a glance." https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/repowereu-affordable-secure-and-sustainable-energy-europe_en

Gambhir, A. 2023. "Powering past coal is not enough." *Nature Climate Change*, 13(2), 117-118.

Herberg, Mikkal E. 2023. Forward. In NBR Special Report #105 "The Revenge of Energy Security: Reconciling Asia's Economic Security with Climate Ambitions."

Jeff D. Colgan & Miriam Hinthorn. 2023. "International Energy Politics in an Age of Climate Change," *Annual Review of Political Science*, 26, pp. 3.1-3.18

Johns Hopkins. 2022. How COVID-19 Disrupted the Renewable Energy Transition – and How the World Can Get Back on Track. Dec 12. https://energy.sais.jhu.edu/articles/how-covid-19-disrupted-renewable-energy-transition/

Lowitzsch, J., Hoicka, C. E., & van Tulder, F. J. 2020. Renewable energy communities under the 2019 European Clean Energy Package–Governance model for the energy clusters of the future? *Renewable and Sustainable Energy Reviews*, 122, 109489.

McKinsey. 2023. *Global Energy Perspective 2023*. Executive Summary. November.

Samandari, H., Pinner, D., Bowcott, H., & White, O. 2022. The net-zero transition in the wake of the war in Ukraine: A detour a derailment or a different path? *McKinsey Quarterly*. May 19. https://www.mckinsey.com/capabilities/sustainability/our-insights/the-net-zero-transition-in-the-wake-of-the-war-in-ukraine-a-detour-a-derailment-or-a-different-pa

Shiquan, D., Deyi, X., Yongguang, Z., & Keenan, R. 2023. Critical mineral sustainable supply: Challenges and governance. *Futures*, 103101.

UNFCCC. n.d. "The Paris Agreement." https://unfccc.int/process-and-meetings/the-paris-agreement?gclid=Cj0KCQjw-pyqBhDmARIsAKd9XIMrywJYfChExufSXgF-GmHf-wPjngwSqF4Kiy2O0cjdmbyI1t07YXIaAjdSEALw_wcB

Winzer, C. 2012. Conceptualizing energy security. *Energy policy*, 46, 36-48.

World Economic Forum. 2020. A five-step beginner's guide to the energy transition. July 16. https://www.weforum.org/agenda/2020/07/a-beginners-guide-to-the-energy-transition/

# Session 2

# Health Security and the Global Vaccine Supply Chain

| | |
|---|---|
| **Moderator** | **Yul Sohn** (EAI; Yonsei University) |
| **Presenters** | **Yanzhong Huang** (Council on Foreign Relations)<br>"Pandemic Preparedness in an Era of Geopolitical Rivalries: The Challenges to Global Health Security and China's Response"<br>**Sun-Young Kim** (Seoul National University)<br>"The Global Vaccine Supply Chain after the COVID-19 Pandemic: Prospects and Challenges for Korea from the Global Health Security Perspective"<br>**Taekyoon Kim** (Seoul National University)<br>"Global South's Challenge to Global Health Security: China, India, and the Rest of the Global South" |
| **Discussants** | **Seonjou Kang** (Korea National Diplomatic Academy)<br>**Manki Song** (International Vaccine Institute)<br>**Hyeyoung Chang** (Chung-Ang University) |

# Pandemic Preparedness in an Era of Geopolitical Rivalries: The Challenges to Global Health Security and China's Response

Yanzhong Huang

## Introduction

The Covid-19 pandemic's acute phase is now over, and the issue seems to be quickly fading from public memory, especially as media attention pivots to climate change and the Israel-Hamas war. Global health advocates are striving to push for a new pandemic accord and amendments to the International Health Regulation (IHR). However, the world's level of cooperation over health security seems to be even lower than before the Covid-19 outbreak. With the looming threat of another pandemic, it is crucial to assess the current health security challenges and China's involvement, looking at both past practices and future possibilities. This position paper aims to examine the following questions: How did China respond to the pandemic, and how does this inform its potential reaction to future public health emergencies? How resilient is the global vaccine supply chain, and what role could China play in it? Furthermore, what are the ramifications of the pandemic on the strategic competition between the U.S. and China?

## The Zero-Covid Policy and Beijing's Future Pandemic Response

Zero Covid is a public health strategy that focuses on eliminating Covid-19 cases, as opposed to merely reducing the burden on healthcare systems and mitigating societal and economic impacts. This approach heavily relies on rigorous contact tracing, mass testing, quarantine, and lockdowns. China's implementation of this policy was notably more draconian, widespread, and prolonged compared to other countries that pursued similar approaches.

China's zero-Covid policy originated from its response to the initial novel coronavirus outbreak in Wuhan in early 2020. A stringent lockdown in the city led to a sharp decline in cases by mid-February. By early April, China had seemingly disrupted domestic transmission and emerged as an early victor in the battle against Covid-19. This success coincided with a rapid socio-economic recovery, contrasting with the struggles of other countries still grappling with the pandemic. In this context, the zero-Covid policy was adopted to sustain China's success. The strategy was first implemented in Beijing during the Xinfadi outbreak in summer 2020 (Campbell 2020). It was enforced through a Maoist mobilization regime and supported by high-tech means, including big data, AI, and QR codes, and the introduction of pooled testing that enabled China to test hundreds of millions of people within days.

For the first one and a half years, this approach enabled China to reduce local Covid cases to zero in short periods and maintained an extremely low infection rate. However, is enforcement came with significant costs, including economic disruption, human rights violations, and limited access to routine healthcare. Over time, the high cost of maintaining such a stringent policy became increasingly apparent. Starting in the summer of 2022, as the highly transmissible Delta variant reached China, the policy began to encounter significant diminishing returns. Moreover, it contributed to a huge immunity gap between China and the rest of the world, leaving China

particularly vulnerable to the impending Omicron wave (Huang 2022a). Unlike other zero-Covid nations such as Australia, Singapore, and New Zealand, which began transitioning away from this strategy, the Chinese government intensified its anti-Covid-19 measures. For instance, in spring 2022, China imposed its largest lockdown in Shanghai since early 2020, resulting in major economic and social disruptions in the city and beyond (*Associated Press* 2022). In May 2022, then-Premier Li Keqiang highlighted the need to fix China's battered economy by convening an emergency meeting with 100,000 government officials (Yeung 2022).

By November 2022, the uncontrollable spread of the Omicron variant in China had become evident, leading even former proponents of the zero-Covid policy to voice criticisms. At the end of the month, a series of anti-lockdown protests erupted across Chinese universities and cities (Schifrin and Aranda 2022). These protests, the largest in over three decades, demanded not only an end to zero Covid but also the step-down of Xi Jinping. In early December, Xi abandoned the zero-Covid strategy. However, this policy shift occurred without adequately preparing the country for the transition. The ensuing surge in infections swiftly impacted over 90 percent of the population, resulting in at least 1.4 million deaths shortly after the stringent measures were lifted (Du et al. 2023).

China's Covid-19 response has deeply scarred its society and economy, while also damaging its international reputation and soft power. The close association of the Chinese Communist Party (CCP), and Xi himself, with a policy that ultimately proved catastrophic, and their subsequent shift to a previously derided approach, has eroded their legitimacy. However, the implementation of the zero-Covid policy also provided a proof of concept for a surveillance state, allowing for increased government intrusion into people's daily lives. In the post-Covid era, although itinerary codes have been discarded, health codes — which assess an individual's risk level based on travel history, residence, and medical records — remain. Massive datasets containing such information are still stockpiled by the government, ready to be reactivated in the event of another outbreak. This is especially concerning given the lack of strong public opposition and ongoing efforts to enhance the infrastructure and organization of digital governance in post-Covid China. Indeed, on December 1, 2023, health codes were reintroduced in some Chinese provinces in response to the upsurge of pediatric respiratory illnesses in the country. It is not difficult to envision that, faced with a new, dangerous pathogen for which no treatments or vaccines exist, China could readily revive its surveillance apparatus, relying heavily on non-pharmaceutical methods to identify, track, quarantine, and isolate carriers and their close contacts.

In the aftermath of the Covid-19 pandemic, Chinese lawmakers are drafting a revision to the infectious disease prevention and control law. This draft, however, appears to legitimize many aspects of the zero-Covid policy. Key zero-Covid measures, such as quarantines, lockdowns, PCR testing, and health codes, are included in the proposed amendment. While the revision attempts to introduce the principle of proportionality — ensuring that measures are in line with the level of threat — it also grants local governments the authority to implement these measures without obtaining prior approval from higher authorities. However, the draft does not adequately safeguard civil liberties and human rights in the implementation of these measures.

China's future pandemic response is also marked by additional areas of concern. The proposed amendments to the infectious disease prevention law emphasize enhancing China's epidemic surveillance, early warning, and reporting systems. However, there are no significant

strides toward improving transparency and international cooperation. While the revisions incentivize whistleblowers to report potential outbreaks, they are barred from sharing this information on social media or through any channels not sanctioned by the government. Moreover, these revisions do not offer sufficient protection for whistleblowers' safety. The responsibility to publicize potential outbreaks remains solely with local governments, which could hinder a timely and effective response. Equally concerning, in the post-Covid context, there has been no public discourse on drawing lessons from the Covid-19 pandemic. This continued opacity and lack of cooperation might explain why the WHO has publicly sought information from the Chinese government regarding the recent undiagnosed cluster of respiratory illnesses among children in northern China. In the absence of significant reforms in its political system and public health infrastructure, the events experienced in China during the Covid-19 pandemic could recur.

**The Global Vaccine Supply Chain Challenge and China's Position**

One major challenge in the global vaccine supply chain is the inequity in vaccine distribution, a consequence of uneven R&D and manufacturing capacities, particularly between the Global North and South. Vaccine production is concentrated in a few countries, exacerbating disparities. The Covid-19 pandemic intensified these issues as wealthy countries stockpiled vaccines, leaving poorer nations struggling for access. Actions by some countries, such as export bans and restrictions on vaccines and ingredients to prioritize their populations, worsened the situation. The vaccine nationalism, combined with a surge in demand, scaling-up challenges, and cold chain logistics, led to global supply-chain disruptions, shortages, and delays, impeding equitable vaccine access. Initially hampered by vaccine nationalism and later by unstable supply and inefficient delivery, the COVAX initiative fell short of its goal of global vaccine equity.

The pandemic met the criteria for a Trade-Related Aspects of Intellectual Property Rights (TRIPS) waiver under the World Trade Organization (WTO). In fall 2020, India and South Africa led a call for a TRIPS waiver from the WTO, aiming to suspend intellectual property rights for COVID-19 medical countermeasures. However, it took nearly two years for WTO members to agree on limited terms for a COVID-19 vaccine waiver. This was compounded by the hesitance of companies, significantly funded by public money for vaccine development, to share vaccine rights with governments. But the assumption that a TRIPS waiver would rapidly increase vaccine access in low-income countries ignores the complexity of the issue (Huang and Katz 2023). The waiver did not address the essential expertise needed for Covid-19 vaccine development and distribution, and the WTO's decision came too late in the pandemic to be significantly effective. As vaccines became more available, the main challenge shifted to adoption rates rather than availability or cost.

In response to heightened supply chain bottlenecks during the pandemic, enhancing supply chain resilience has become a priority in the post-Covid era. To secure their supply chains for the future, many countries are moving towards onshoring – bringing production back within national borders, or friend-shoring – diversifying supply chains among allied countries. On November 29, 2023, U.S. President Joe Biden led the inaugural meeting of the White House Council on Supply Chain Resilience, announcing over 30 initiatives to strengthen America's supply chains (The White House 2023). These include utilizing the Defense Production Act to bolster domestic production of essential medicines. A Presidential Determination will expand

the Department of Health and Human Services' authority to invest in domestic manufacturing of crucial medicines, medical countermeasures, and vital inputs critical to national defense. Supply chain resilience is also a central topic in diplomatic talks between the U.S. and its allies and partners. This includes ongoing bilateral and multilateral efforts, like the Supply Chain Agreement under the Indo-Pacific Economic Framework for Prosperity (IPEF), initiated by the U.S. with the Republic of Korea and 12 other countries in May 2022 (Office of the United States Trade Representative 2022).

Meanwhile, countries that suffered from vaccine disparity or with limited decision-making influence in the global vaccine development and distribution are reevaluating their reliance on global systems for their population's safety and security. They are contemplating whether developing health-related infrastructure should be prioritized as a national security concern. Countries are also exploring regional cooperation agreements, either as a complement to or, in some cases, a replacement for global cooperation, focusing on mutual assistance with neighboring nations in vaccine access.

The pandemic highlighted China's important role in the global vaccine supply chain. In early 2020, China emerged as a leader in the race to develop a Covid-19 vaccine. President Xi pledged to make Chinese vaccines a "global public good" upon their availability (Wheaton 2020). Until fall 2021, China was the world's biggest Covid vaccine exporter. By the end of 2022, Beijing had distributed 2.18 billion doses to 119 countries, either through sales or donations (*Bridge* 2022). Beyond exporting vaccines, China also collaborated with several developing countries to enhance their vaccine production capabilities, including the construction of vaccine filling and finishing facilities. Amidst enormous global demand and disruptions in the vaccine supply chain, China's vaccine diplomacy played a key role in lessening global vaccine access disparities. It also enabled Beijing to gain a foothold in a market traditionally dominated by Indian and Western pharmaceutical companies.

Evidence nonetheless challenges the view of Beijing as a leader in providing global public goods. By definition, a public good should be non-rivalrous and non-excludable. In its vaccine diplomacy, only 15 percent of China's overseas vaccine shipments – 328 million doses – were donations, with the rest sold commercially. Moreover, China's inactivated vaccines were less effective than mRNA vaccines against highly transmissible variants. As the U.S. increased its vaccine supply, Chinese vaccines quickly lost their competitive edge in the global market. This decline became evident in fall 2021 when China's global vaccine deliveries plummeted. By January 2022, with the rapid spread of the Omicron variant, China's share in the global vaccine supply dropped to its lowest point since December 2020.

Despite the reduced effectiveness of its vaccines, Beijing has persistently refused to authorize foreign-made mRNA Covid-19 vaccines. China's efforts to develop a domestic mRNA vaccine against Covid-19 was not very successful. It was only in September 2022 that Indonesia granted emergency use approval to a Chinese company's mRNA Covid-19 vaccine (Widianto and Liu 2022). China approved its first mRNA Covid vaccine in March 2023, which was too late given the waning Omicron wave in the country by that time (*Reuters* 2023).

Given its vast vaccine R&D and manufacturing capacity, China could still play a significant role in the future global vaccine supply chain. The extent of this role hinges on developing new collaboration mechanisms for technology transfer and R&D in preparation for future pandemics. In July 2023, U.S. vaccine producer Moderna agreed to build its first mRNA

manufacturing facility in China, in partnership with the Shanghai municipal government (Silver 2023). To facilitate prompt access to effective vaccines in emerging and developing countries, OECD nations should bolster compulsory licensing provisions at the WTO. The resilience of the global vaccine supply chain also depends on whether China can be encouraged to integrate its bilateral health assistance into a COVAX-like multilateral framework. Such a framework should not only empower LMICs in decision-making regarding global vaccine development and distribution but also facilitate cooperation between geopolitical rivals as contributors to global public goods in a non-confrontational way. Naturally, fostering multilateralism in the absence of trust among geopolitical competitors requires these nations to engage in confidence-building measures, including scientific collaboration and the establishment of shared multilateral norms and principles. In addition, the Pandemic and Influenza Preparedness framework for the sharing of influenza viruses and access to vaccines and other benefits could be retrofitted for future pandemic readiness and response. Discussions are already in progress to incorporate such a framework for accessing medical countermeasures into the new pandemic treaty and the amended IHRs.

## The Covid-19 Pandemic and U.S.-China Strategic Competition

The pandemic has shaped the dynamics of U.S.-China strategic competition. For the first time, ideological competition was introduced into epidemic and pandemic response. Both nations framed their pandemic response as a contest between authoritarianism and liberal democracy. China touted its early success in controlling the virus as proof of its political system's superiority, while the U.S. began to view the CCP regime as a major adversary, posing a threat to the liberal international order. China intensified its criticism of the U.S. pandemic handling, labeling it as the worst globally (Zheng 2021). In the U.S., perceptions of China as the pandemic's origin, its initial missteps, and disruptions to global supply chains fueled calls among politicians for a hard decoupling from China (Michta 2020).

The antagonism, once predominantly economic and technological, now extends to public health and personal interactions. Concerns about dependency on Chinese pharmaceutical products spurred the U.S. to diversify its sources to allied countries, bring some production back home, and increase stockpiles. China's actions and rhetoric regarding Hong Kong, Taiwan, Xinjiang, and the South China Sea, along with the American response, have escalated tensions further. The pandemic, along with persistent travel restrictions, the ongoing trade war, and escalating geopolitical tensions, is also contributing to a decline in U.S.-China cultural exchanges, evidenced by reduced tourism and academic interactions (Goodier and Hawkins 2023).

Furthermore, both countries sought to leverage the provision of vaccines and medical supplies to vie for strategic influence. Beijing engaged in "mask diplomacy" and "vaccine diplomacy," using the Health Silk Road and Belt and Road Initiative's networks to distribute medical supplies, especially to BRI participants (Huang 2022b). China used its role as a key vaccine supplier to pressure countries with ties to Taiwan into reconsidering their diplomatic stances. In return for Chinese vaccines, many countries expressed support for Beijing's policies towards Hong Kong, Taiwan, Tibet, and Xinjiang (Lew et al. 2021). In response, the U.S. launched its Covid diplomacy, offering bilateral assistance and collaborating with Quad countries (Australia, India, and Japan) to counter China's influence in Asia (Ruwitch and

Kelemen 2021). In a strategically hostile and heavily securitized context, the bilateral or minilateral approach encouraged competitive dynamics that not only exacerbated global inequity in public health resources distribution but also undermined mutual trust for effective international health cooperation.

During the pandemic, both nations also sought to shape the global health agenda. Beijing initially used the WHO to validate its pandemic response narrative. The Trump administration, accusing the WHO of being "China-centric," suspended funding and terminated the U.S. relationship with the organization. Beijing countered with a $30 million pledge to the WHO's Covid-19 efforts (Shih 2020). Since March 2020, China has contested the pandemic's origin, influencing the WHO-China joint study findings, which supported Beijing's theory and rejected the lab-leak hypothesis. In the U.S., China's perceived opacity regarding the pandemic's origins fueled mistrust and skepticism, while China viewed US accusations and focus on the lab-leak theory as attempts to contain its rise. Amid allegations and conspiracy theories, the U.S. and China became entangled in a vortex of suspicion, disinformation, and diplomatic disputes, politicizing the scientific quest for the pandemic's origins.

US-China strategic competition has eroded trust and cooperation, particularly in health security. During the pandemic, there was minimal government-to-government dialogue on joint efforts to address the pandemic. In the post-Covid era, despite the clear need for collaboration, political will is lacking. Health security was not a key topic at the recent Biden-Xi summit in San Francisco (Huang 2023). In the U.S., Covid-19's link to China remains politicized, with the Biden administration focusing on partnerships with allies rather than engaging with geopolitical rivals.

Paradoxically, by affecting China's domestic economy and its ability to project power overseas, the pandemic has altered the global power balance, potentially reducing the intensity of US-China competition. China's stringent zero-Covid strategy has slowed its economic growth, with revised forecasts that China's GDP overtakes the U.S.'s only by 2035, if at all (*The Economist* 2023). Even if China becomes the largest economy, its advantage over the U.S. might be modest, insufficient for significant competitive edge. Moreover, survey data indicate China's limited effectiveness in gaining lasting soft power or substantial clout during the pandemic (Silver et al. 2023). The latest Lowy Institute Asia Power Index records the largest decline in China's power (Lowy Institute 2023). While it is premature to declare China's ascent at its peak, especially as the U.S. is facing its own daunting challenges, China's trajectory to a power on par with the U.S. is likely to be prolonged. The altered power dynamics will shape both nations' strategic preferences and choices. Hopefully, it might generate additional incentives for both sides to work together in pandemic prevention and preparedness.

**References**


*Associated Press*. 2022. “Shanghai starts China’s biggest COVID-19 lockdown in 2 years.” March 29. https://apnews.com/article/covid-china-locking-down-shanghai-b406df3a0113b9be99273324fec2c12e

*Bridge*. 2022. “China COVID-19 Vaccine Tracker.” https://bridgebeijing.com/our-publications/our-publications-1/china-covid-19-vaccines-tracker/

Campbell, Charlie. 2020. “China Appears to Have Tamed a Second Wave of Coronavirus in Just 21 Days with No Deaths.” *Time*. July 2. https://time.com/5862482/china-beijing-coronavirus-second-wave-covid19-xinfadi/

Du, Zhanwei, Yuchen Wang, Yuan Bai, Lin Wang, Benjamin John Cowling, and Lauren Ancel Meyers. 2023. “Estimate of COVID-19 Deaths, China, December 2022–February 2023.” *Emerging Infectious Diseases*. 29, 10: 2121-2124.

Goodier, Michael, and Amy Hawkins. 2023. “US-China cultural exchange at low point after tensions and Covid, data shows.” *The Guardian*. July 22. https://www.theguardian.com/world/2023/jul/22/us-china-cultural-exchange-at-low-point-after-tensions-and-covid-data-shows

Huang, Yanzhong. 2022a. “China’s Immunity Gap: The Zero-COVID Strategy Leaves the Country Vulnerable to an Omicron Tsunami.” *Foreign Affairs*. January 26. https://www.foreignaffairs.com/articles/china/2022-01-26/chinas-immunity-gap

_____. 2022b. “The Health Silk Road: How China Adapts the Belt and Road Initiative to the COVID-19 Pandemic.” *American Journal of Public Health*. April 2022.

_____. 2023. “Two Geopolitical Rivals, One Health.” Think Global Health. November 29. https://www.thinkglobalhealth.org/article/two-geopolitical-rivals-one-health

Huang, Yanzhong, and Rebecca Katz. 2023. “Negotiating Global Health Security: Priorities for U.S. and Global Governance of Disease.” https://www.cfr.org/report/negotiating-global-health-security

Lew, Jacob J., Gary Roughead, Jennifer Hillman, and David Sacks. 2021. “China’s Belt and Road: Implications for the United States.” CFR Independent Task Force Report No. 79.

Lowy Institute. “Lowy Institute Asia Power Index 2023 Edition: China.” https://power.lowyinstitute.org/countries/china/

Michta, Andrew A. 2020. “The Wuhan Virus and the Imperative of Hard Decoupling.” *The American Interest*. March 17. https://www.the-american-interest.com/2020/03/17/the-wuhan-virus-and-the-imperative-of-hard-decoupling/

Office of the United States Trade Representative. 2022. “Indo-Pacific Economic Framework for Prosperity (IPEF).” https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef

*Reuters*. 2023. “China OKs its first mRNA vaccine, from drugmaker CSPC.” March 23. https://www.reuters.com/business/healthcare-pharmaceuticals/china-approves-its-first-mrna-vaccine-domestic-drugmaker-cspc-2023-03-22/

Ruwitch, John, and Michele Kelemen. 2021. “Biden And ‘Quad’ Leaders Launch Vaccine Push, Deepen Coordination Against China.” *NPR*. March 12. https://www.npr.org/2021/03/12/976305089/biden-and-quad-leaders-launch-vaccine-push-deepen-coordination-against-china

Schifrin, Nick, and Teresa Cebrián Aranda. 2022. “Thousands in China protest zero-COVID policy in largest demonstrations in decades.” *PBS*. November 28. https://www.pbs.org/newshour/show/thousands-in-china-protest-zero-covid-policy-in-largest-demonstrations-in-decades

Shih, Gerry. 2020. “China pledges additional $30 million funding for World Health Organization.” *The Washington Post*. April 23. https://www.washingtonpost.com/world/asia_pacific/china-pledges-additional-30-million-funding-for-world-health-organization/2020/04/23/24f9b680-8539-11ea-81a3-9690c9881111_story.html

Silver, Andrew. 2023. “Moderna begins work on China mRNA manufacturing site.” *Reuters*. November 28. https://www.reuters.com/business/healthcare-pharmaceuticals/moderna-begins-work-china-mrna-manufacturing-site-2023-11-28/

Silver, Laura, Christine Huang, and Laura Clancy. 2023. “China’s Approach to Foreign Policy Gets Largely Negative Reviews in 24-Country Survey.” Pew Research Center Report. July 27. https://www.pewresearch.org/global/2023/07/27/chinas-approach-to-foreign-policy-gets-largely-negative-reviews-in-24-country-survey/

*The Economist*. 2023. “How soon and at what height will China’s economy peak?” May 11. https://www.economist.com/briefing/2023/05/11/how-soon-and-at-what-height-will-chinas-economy-peak

The White House. 2023. “FACT SHEET: President Biden Announces New Actions to Strengthen America’s Supply Chains, Lower Costs for Families, and Secure Key Sectors.” November 27. https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/27/fact-sheet-president-biden-announces-new-actions-to-strengthen-americas-supply-chains-lower-costs-for-families-and-secure-key-sectors/

Wheaton, Sarah. 2020. “Chinese vaccine would be ‘global public good,’ Xi says.” *Politico*. May 18. https://www.politico.com/news/2020/05/18/chinese-vaccine-would-be-global-public-good-xi-says-265039

Widianto, Stanley, and Roxanne Liu. 2022. “A Chinese mRNA COVID vaccine is approved for the first time - in Indonesia.” *Reuters*. September 30. https://www.reuters.com/business/healthcare-pharmaceuticals/indonesia-drug-agency-approves-chinas-walvax-mrna-vaccine-emergency-use-2022-09-29/

Yeung, Jessie. 2022. “100,000 Chinese officials attend emergency meeting to revive Covid-hit economy.” *CNN Business*. May 26. https://edition.cnn.com/2022/05/26/business/china-state-council-economic-meeting-intl-hnk/index.html

Zheng, Sarah. 2021. “‘US leads world in pandemic failure’: Chinese report takes aim at American coronavirus response.” *South China Morning Post*. August 9. https://www.scmp.com/news/china/diplomacy/article/3144400/us-leads-world-pandemic-failure-chinese-report-takes-aim

# The Global Vaccine Supply Chain after the COVID-19 Pandemic: Prospects and Challenges for Korea from the Global Health Security Perspective

Sun-Young Kim

## The Context - Global Health Security (GHS)

**Health security** is a field within human security that emerged after the Cold War. It encompasses activities and measures that take place across national borders to mitigate all kinds of public health threats to ensure the health of the people (UNDP, 1994). Examples of ***public health threats*** include infectious diseases, antimicrobial resistance, foodborne diseases, chemical accidents, nuclear accidents, and environmental disasters (including climate change) (WHO 2007).

Extending the concept of health security, **Global Health Security (GHS)** refers to a shared responsibility that requires a coordinated effort from countries around the world to protect the health of all people. More specifically, the WHO defines GHS as activities that encompass both preventive and reactive aspects to minimize the risk and impact of ***acute public health events*** that endanger people across geographic regions and national borders.

With rapid globalization, the mobility of people and goods has increased, and economic interdependence has grown. As a result, among the various types of global health security threats, ***infectious disease-related threats*** are becoming increasingly important in terms of frequency and scale. For example, the emergence of infectious diseases (EIDs) such as COVID-19, is threatening the health of people around the world and causing significant socioeconomic losses.

## Importance of Vaccines in the Context of GHS

Vaccines, beyond their health and life-saving benefits against vaccine-preventable infectious diseases, can also yield societal benefits in terms of global economy and security, particularly during a pandemic.

## Features of Global Vaccine Supply Chains

Generally, **Supply chains**, are networks of organizations and business processes that work together to deliver a product or service from its inception to the end-user. They connect suppliers, manufacturers, warehouses, retailers, and customers, facilitating the flow of products and services from source to consumption. In the supply chains, materials, information, and payments flow in both directions. Supply chains represent complex systems that can be challenging to manage. However, it is essential for businesses or industries to effectively manage their supply chains in order to be successful. Effective management of supply chains is crucial for businesses to enhance efficiency, reduce costs, and boost customer satisfaction.

Similarly, **vaccine supply chains** can be thought of as the organization and processes that are used to develop, produce, distribute, and administer vaccines. Vaccine supply chains are equally complex, necessitate meticulous planning, coordination, and collaboration between

various stakeholders, including suppliers, manufacturers, distributors, wholesalers, immunization providers, and public health agencies.

However, it should be noted that vaccine supply chains have some characteristics that differ from the general supply chains:

- Rigorous safety and quality control: Vaccines have a direct impact on the health of populations, so strict safety and quality control are required throughout the supply chain. In particular, they often require specific low-temperature conditions to maintain their stability;
- Difficulty in forecasting and planning for production and distribution: The nature of infectious disease outbreaks and epidemics makes it difficult to forecast and plan for production and distribution;
- Limited number of vaccine developers and producers: Due to high entry barriers, the number of vaccine developers and producers is often very limited;
- Long distribution chain: Vaccines often require a long distribution chain that crosses borders, from the manufacturing facility to the local healthcare facility or vaccination site;
- Strict regulations and certification: Each stage of the vaccine supply chain must comply with strict regulations and certification. This process is more stringent and complicated than for other products or services. Most developing countries do not have the infrastructure to comply with these regulations, so WHO's prequalification (PQ) system or the emergency use listing (EUL) system are needed to provide vaccines and medicines to these countries;
- The need for public education and campaigns: To achieve sufficient levels of herd immunity, specialized knowledge dissemination through public education and campaigns is crucial, going beyond mere marketing. This necessitates the collaboration of healthcare professionals;
- The need for data management system: The vaccine supply chain must have a data management system to collect, manage, and report important data such as the production and distribution of vaccines and vaccination rates; and,
- The need for international cooperation: International cooperation is essential for the delivery of vaccines, as many middle- and low-income countries are not involved in the development, production, or distribution of vaccines, and are often unable to purchase them directly.

**Importance of Vaccine Supply Chains**

Given that vaccines can play a vital role in reducing morbidity and mortality rates, promoting public health and well-being, and achieving global health goals, investing in and strengthening the global vaccine supply chains that can ensure effective and efficient vaccine production is also essential for ensuring equitable access to life-saving vaccines.

Notably, the ***'global supply chain of pandemic-related products***' has emerged as a key issue for the Intergovernmental Negotiating Body (INB), established in late 2022 to deliberate on a pandemic treaty.

**Current Challenges with Global Vaccine Supply Chains**

While vaccines have been pivotal in combating the COVID-19 pandemic, the pandemic also exposed several shortcomings in current vaccine supply chains. These challenges necessitate global-level efforts and actions for resolution:

1. Production capacity and distribution inequalities:
    - Limited production capacity: The initial focus on developed nations led to bottlenecks in vaccine production, limiting access for low- and middle-income countries (LMICs).
    - Unequal distribution: High-income countries continue to hold a disproportionate amount of vaccine doses, exacerbating inequities in global vaccination coverage.
    - Logistics and infrastructure gaps: LMICs often lack the infrastructure and logistics networks needed for efficient vaccine distribution, particularly in remote regions.

2. Raw material and supply shortages:
    - Dependence on specific suppliers: The reliance on a few key manufacturers for critical vaccine components creates vulnerabilities to disruptions in their supply chains.
    - Competition for resources: Competition for essential raw materials, such as vials, syringes, and filters, can drive up prices and limit access for LMICs.
    - Geopolitical tensions: Political tensions between countries can disrupt the flow of essential vaccine components and finished products.

3. Regulatory and bureaucratic hurdles:
    - Complex regulatory frameworks: Different countries have varying regulatory requirements, which can delay the approval and distribution of vaccines.
    - Bureaucratic delays: Complicated administrative procedures can slow down the procurement and distribution of vaccines, hindering timely vaccination efforts.
    - Lack of data harmonization: Inconsistent data collection and reporting across countries make it difficult to track vaccine rollout and identify areas needing support.

4. Lack of funding and investment:
    - Inadequate financing: LMICs often lack the financial resources needed to purchase vaccines and invest in robust health systems for vaccine administration.
    - Unpredictable funding flows: Donor fatigue and fluctuating funding commitments can hinder long-term planning and sustainable vaccine programs.
    - Competing priorities: Funding allocated to vaccine programs can be diverted to other pressing healthcare needs, impacting vaccination efforts.

5. Vaccine hesitancy and misinformation:
    - Public distrust of vaccines: Misinformation and mistrust of vaccines can lead to vaccine hesitancy and lower vaccination rates, undermining global efforts to reach herd immunity.

- Limited access to information: Lack of access to accurate and timely information about vaccines can fuel misinformation and vaccine hesitancy, particularly in underserved communities.
- Need for tailored communication strategies: Effective communication strategies that address diverse cultural contexts and concerns are crucial to overcoming vaccine hesitancy and promoting vaccination uptake.

Addressing these challenges will require a multi-pronged approach, such as:

- Strengthening production capacity and expanding access to vaccines in LMICs;
- Diversifying the supply chain for critical vaccine components;
- Harmonizing regulatory frameworks and streamlining bureaucratic processes;
- Mobilizing additional funding and ensuring predictable funding flows; and,
- Combatting misinformation and promoting vaccine confidence through effective communication strategies.

**Realignment of Global Supply Chains after the COVID-19 Pandemic**

The COVID-19 pandemic has led to the following changes in global supply chains:

- **Regionalization of supply chains:** The COVID-19 pandemic has increased the instability of global supply chains, prompting many companies to pursue regionalization, which can simplify processes and enhance stability.
- **Diversification of supply chains:** To mitigate the risks associated with a single-sourced supply chain, companies are pursuing diversification of supply chains, which can also help to improve stability.
- **Digitalization of supply chains:** The increased demand for non-face-to-face services during the COVID-19 pandemic has accelerated the digitalization of supply chains to improve the efficiency and transparency of supply chains.

Considering the trends in the realignment of global supply chains, the following changes and trends are expected for future vaccine supply chains:

- **Improvement of vaccine supply chains for future emergencies:** The importance of vaccine supply chains has been highlighted more than ever before, even though the limitations of vaccine supply chains were revealed during the COVID-19 pandemic. Therefore, efforts will be made to improve the current supply chain to prepare for future emergencies.
- **Regionalization of vaccine supply chains:** As the instability of global supply chains has increased since the COVID-19 pandemic, vaccine supply chains will also be pursued to improve stability through regionalization and diversification. For example, efforts are underway to establish vaccine production facilities in Africa. In addition, it is expected that vaccine production facilities will be expanded in developing countries.
- **Digitalization and automation of vaccine supply chains:** Similarly, digital technologies and automation technologies will be applied more actively in vaccine supply chains along with the digitalization of global supply chains in general. This is expected to help improve production efficiency, ease of monitoring production and distribution status, and so on.

• **Strengthening of international cooperation:** While the trend of decoupling global supply chains may impact the short-term outlook, there is an expectation for heightened international cooperation in the long term. This collaboration will span the development, production, distribution, and vaccination processes, informed by the lessons of COVID-19. However, achieving effective global cooperation will present challenges, such as overcoming 'vaccine nationalism.'

Note that the activities being carried out by international organizations such as the United Nations and WHO through various partnerships to prepare for future pandemics are also expected to affect the form of future vaccine supply chains and contribute to strengthening international cooperation.

For example, COVAX, which aimed to contribute to the distribution of vaccines to middle- and low-income countries but had limitations due to the AMC mechanism design, will end its activities within 2023, and the new C19 program will start activities to prioritize the supply of vaccines to countries that did not receive vaccines under the COVAX mechanism.

In addition, the pandemic treaty (Pandemic Treaty) announced through an intergovernmental consultation body and the pandemic fund (Pandemic Fund), which was launched in the form of an intermediary fund of the World Bank to secure funding for pandemic preparedness and response last year, are also expected to affect vaccine supply chains for developing countries.

On the other hand, WHO announced that it is designing a more comprehensive medical response platform to replace ACT-A, which served as the main pandemic response platform during the COVID-19 pandemic. However, only the name MCM (Medical Countermeasures Platform), which aims to develop and accelerate access to medical countermeasures for infectious diseases and non-infectious diseases, has been announced so far.

**Challenges and Tasks for Korea**

Korea has world-class competitiveness in the field of vaccine production and supply, but it faces several challenges under the current situation of realignment of global supply chains. In this regard, the following basic directions are suggested:

• First, Korea should focus on establishing and improving its domestic vaccine supply chain, leveraging its competitiveness in vaccine production and supply. Additionally, developing and implementing proactive plans to address potential future crises in the vaccine supply chain is crucial.

• Leveraging its established expertise and experience in vaccine supply chain development, Korea should play a key role in contributing to the production and supply of COVID-19 vaccines, while also supporting the enhancement of supply chains and infrastructure in developing countries. Furthermore, Korea should strive for a leadership role in enhancing global vaccine accessibility through active international cooperation.

It is also necessary to aim for a leading role in improving global vaccine accessibility through active international cooperation.

# Global South's Challenge to Global Health Security: China, India, and the Rest of the Global South

Taekyoon Kim

## Introduction: The Global Pandemic, COVID-19 Vaccine Inequity, and Global Supply Chains

It is now a cliché to note that the global pandemic of COVID-19 results in not simply degenerating vulnerabilities to complex, often traversing risks such as infectious diseases, climate disasters, or protracted conflicts, but also paralyzing the global supply chain, thereby hampering the vaccine equity between the Global North and the Global South. The challenge before states and international organizations, particularly the World Health Organization (WHO), is to build or restore long-term, systemic resilience into the global health supply chain, as all public health activities and operations depend on an effective supply chain which globally leads resilience- and capacity-building to be vital for health outcomes in low- and middle-income countries (LMICs) of the Global South. Indeed, managing risks to health supply chains at the global level is essential to safeguarding public health, filling gaps in commodity access and quality, facilitating inclusive growth and socioeconomic stability in fragile states.

Since the COVID-19 pandemic was officially ended by the WHO, drawing on lessons learned about the conditions needed to ensure resilient health supply chains will be crucial to enabling greater health system access and equity for the Global South, improving pandemic preparedness, and more broadly achieving the Sustainable Development Goals (SDGs). It is therefore critical to examine the characteristics of resilient health supply chains and identify opportunities for effective multi-sectoral partnerships to transform health systems in LMICs.

However, the coronavirus pandemic verifies global health governance did not work properly and the distribution of vaccines as well as the global health supply chain were dominated totally by a few vaccine-producing states, including the Global North and China and India within the Global South. Vaccine diplomacy was aimed to improve a country's diplomatic relationship and influence to the target countries by using vaccines. In particular, both China and India pose a growing threat to global health security via vaccine diplomacy not only for sustaining hegemony over the Global South, but also for challenging the Global North-centered structure of global health governance by claiming alternative mechanisms of the global supply chain of vaccine doses for the Global South. While confronting the current landscape of the global health supply chain that the Global North rules, India and China also have been competing with each other to secure itself as a hegemon to govern the Global South. Moreover, China and India show the variation of challenges against the West's global health governance: China is more likely to take its own line of vaccine diplomacy in bilateral forms, whereas India's stance is a sort of mixed bag between bilateral vaccine diplomacy and multilateral cooperation with the EU and UN agencies.

**Malfunctioned Global Health Governance and the Fragility of Health Supply Chains**

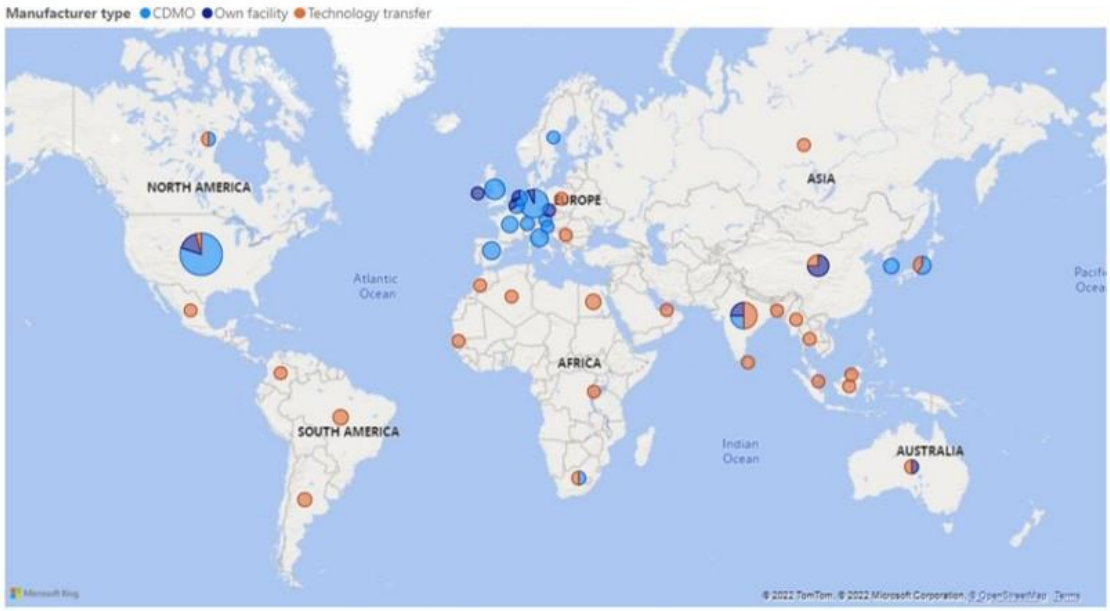
COVID-19 vaccine inequity would have a lasting and profound impact on socio-economic recovery in LMICs without urgent action to boost supply and assure equitable access for every country, including through dose sharing. Emerging infectious diseases (EIDs) pose a real threat to global health security, given the fact that the costs of EIDs are vast in both human and economic terms: in terms of the devastating death toll and disruption to societies, COVID-19 could cost the global economy $4.1 trillion, or almost 5% of global gross domestic product. In response to this total disaster, however, the WHO failed to take a proper and responsive action to tackle the outbreak of COVID-19, thereby providing a reason for the Trump administration to criticize WHO's pro-China tendencies and withdraw US membership from the WHO. Strong states in the Global North, which are fully equipped to produce and distribute vaccines for their own citizens as well as LMICs, have focused on their capacities and preparedness of vaccine supply chains at the domestic level, rather than contributed to multilateral collaborations with WHO and other international health initiatives.

Nevertheless, the international community has endeavored to set up some new health security initiatives which were designed to engage global epidemic or pandemic for the South's affected countries during outbreaks. Firstly, the Coalition for Epidemic Preparedness Innovations (CEPI) was launched at Davos 2017 as the result of a consensus that a coordinated, international, and intergovernmental plan was needed to develop and deploy new vaccines to prevent future epidemics. CEPI is an innovative global partnership between public, private, philanthropic, and civil society organizations working to accelerate the development of vaccines against emerging infectious diseases and enable equitable access to these vaccines for affected populations. In this regard, CEPI supports coordinating activities to improve our collective response to epidemics, strengthening capacity in countries at risk, and advancing the regulatory science that governs product development. Secondly, the COVID-19 Vaccines Global Access (COVAX) was formed in April 2020 as a worldwide initiative aimed at equitable access to COVID-19 vaccines directed by the Gavi, the Vaccine Alliance, CEPI, and WHO, alongside key delivery partner UNICEF.

Furthermore, recognizing the urgency of turning vaccine doses into vaccinated, protected communities, WHO, UNICEF and Gavi, the Vaccine Alliance launched the COVID-19 Vaccine Delivery Partnership (CoVDP) in January 2022. CoVDP was built on existing resources to support the AMC 92 and focused on the 34 countries with or below 10% coverage. Working closely with countries to understand bottlenecks to vaccination, CoVDP offered access to urgent operational funding, technical assistance and political engagement to rapidly scale up vaccination and monitor progress towards targets.

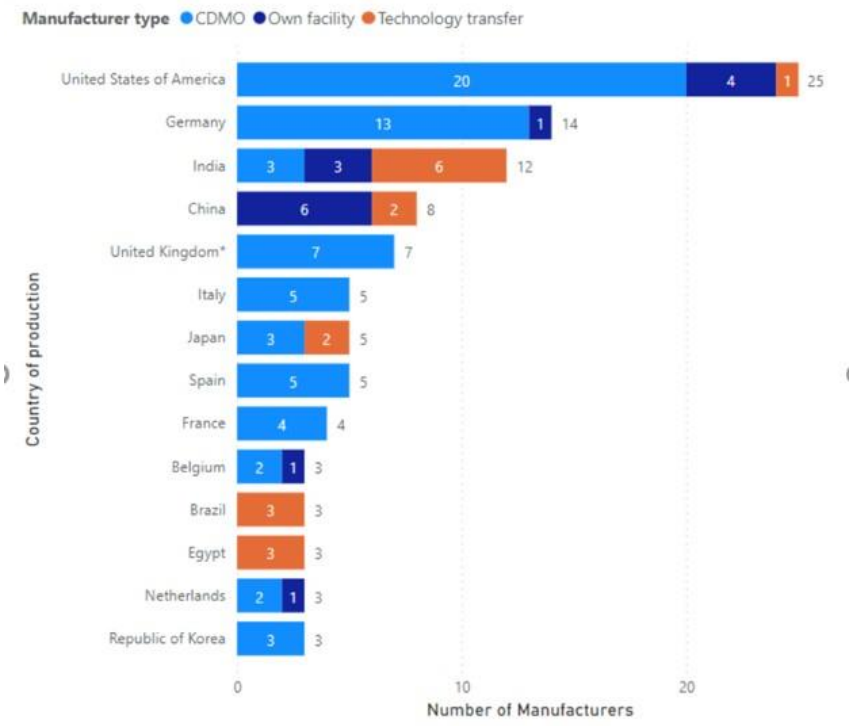
Although the abovementioned global health initiatives contribute to sustaining global health supply chains transferring vaccine doses into fragile states of the Global South, global health governance is easily collapsed or malfunctioned in the face of national interest first strategies which major vaccine-producing countries strategically pursued for. As figure 1 and 2 illustrate, around 30 states take the lead of the COVID-19 vaccine production whose type of manufacturer consists of the three kinds – Contract Development and Manufacturing Organization (CDMO), own facility, and technology transfer. The spoiler, affecting negatively global health security,

**Figure 1. Geographical Locations of Vaccine Production by Type of Manufacturer, February 2022**




Source: Created using data from UNICEF COVID-19 Vaccine Market Dashboard.
Disclaimer: The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations

**Figure 2. Top 10 Vaccine Production Locations, Type and Number of Manufacturers, February 2022**




Source: Created using data from UNICEF COVID-19 Vaccine Market Dashboard.
Abbreviations: CDMO: Contract development and manufacturing organizations.
United Kingdom* includes United Kingdom of Great Britain and Northern Ireland

comes from just 9 countries which have their own facilities for vaccine production, rather than the other countries producing vaccines through the CDMO or transferring technology only. Within top 10 vaccine production locations, only 6 countries, such as the United States (4), Germany (1), India (3), China (6), Belgium (1), Netherlands (1), operate vaccine production facilities for the domestic needs and vaccine diplomacy beyond their national uses of vaccines (see figure 2).

Considering the fact that vaccine production remains geographically concentrated, lead developers and activities in the vaccine value chains have been concentrated in 13 economies of the Vaccine Club. The data clearly point to high concentration and self-reliance in COVID-19 vaccine production among a group of 13 countries[1] that we refer to as the "COVID-19 Vaccine Producers' Club" or simply the "Vaccine Club." These countries are not only where the headquarters of the companies currently producing COVID-19 vaccines are found—they are also where 91% (783 out of 857 subsidiaries worldwide) of the subsidiaries of these companies are located. They also account for 60% of total confirmed advance purchasing agreements with pharmaceutical companies for vaccine doses.

A 2020 survey on vaccine manufacturing capacity by CEPI revealed geographical concentration of vaccine production: Europe had the largest production capacity for RNA-based drug substances; India had the largest production capacity for active ingredient production, followed by Europe and North America; and China had the largest production capacity for drug bulk production, followed by North America and the rest of Asia and Oceania.

As the fragility of health supply chains has become increasingly apparent, global public health stakeholders have acknowledged the need to rethink traditional supply chain management approaches, such as the "just-in-time" model for inventory. This approach, which dominated health supply chains leading up to the COVID-19 pandemic, prioritized supply chain efficiency through cost-cutting and waste-reduction measures, encouraging suppliers to eliminate redundancy and replenish inventory only when reserves ran low.

In this sense, vaccine production as well as the global supply chain would be *securitized* by some members of the Vaccine Club – particularly, members equipped with own facilities for vaccine production. Advancing vaccine diplomacy, the EU, US, China, and India are easily ready to strategize their own production capabilities in order to maximize their own national interests and influences by impeding global health supply chains. The issue of vaccine inequity plus supply chain resilience to safeguard health in fragile states of the Global South is extremely vulnerable to both North's return to nationalistic protection, and South's challenge to the existing platform of global supply chains. It is timely and critical to review China and India's strategic moves for vaccine diplomacy in a comparative perspective.

## China's Strategies for Vaccine Diplomacy

China's recent moves on its own way for a new international order have been solidified on the cornerstones of Xi's 3Gs – Global Development Initiative (GDI), Global Security Initiative (GSI), and Global Civilization Initiative (GCI) – as well as the Health Silk Road of the Belt and

[1] The countries are Argentina, Australia, Brazil, Canada, China, European Union, India, Japan, Korea, Russian Federation, Switzerland, United Kingdom, United States.

Road Initiative (BRI). China categorizes its vaccines as public goods which can be used as vaccine aid to developing countries in the Global South, but reflects its strategic roadmap – increasing influences through BRI and GDI – into vaccine diplomacy.

Eight vaccines have been approved for use in China: Anhui Zhifei Longcom Zifivax (approved in 4 countries, 21 trials in 5 countries); Livzon Mabpharm Inc V-01 (approved in 1 country, 7 trials in 3 countries); CanSino Convidecia (approved in 10 countries, 14 trials in 6 countries); CanSino Convidecia Air (approved in 2 countries, 5 trials in 4 countries); Shenzhen Kangtai Biological Products Co. KCONVAC (approved in 2 countries, 7 trials in 1 country); Sinopharm (Beijing) Covilo (approved in 93 countries, 39 trials in 18 countries); Sinopharm (Wuhan) Inactivated (Vero Cells) (approved in 2 countries, 9 trials in 7 countries); Sinovac CoronaVac (approved in 56 countries, 42 trials in 10 countries). The bulk of Chinese vaccines are produced domestically by its own facilities, as mentioned before. With the help of the government, manufacturers started ramping up production capacity as vaccines were being developed and tested. As early as April 2020, Sinopharm established production lines in Beijing and Wuhan with an annual capacity of 300 million doses, with plans to eventually export 300 to 500 million doses to over twenty countries. This expanded capacity allows China to meet domestic demand as well as fulfill orders from abroad.

Chinese vaccine diplomacy has been overwhelmingly bilaterally conducted to date, and has been a significant factor to forge China's own supply chains of vaccine distributions to the Global South. As China has delivered 5 million doses to 13 countries, with more on the way, its bilateral donations could exceed its contribution to COVAX, a global initiative to ensure equitable access to vaccines, which China joined on October 2020. The Sinopharm BIBP vaccine and CoronaVac are Chinese developed vaccines approved by WHO for distribution through COVAX. By July 2021, Gavi had signed advanced purchase agreements for 170 million doses of the Sinopharm BIBP vaccine, 350 million doses of CoronaVac, and 414 million doses of SCB-2019, another vaccine in Phase III trials. As China's Xi pledged 2 billion vaccines globally through the end of 2021 as part of BRI, particularly the Health Silk Road project.

In a nutshell, China's vaccine diplomacy has rested mostly upon the bilateral channels of vaccine distribution through its global vaccine supply chain, rather than multilateral supports via COVAX and other channels. China's direct engagement into the global supply chain that the Global North has been heavily governing causes a challenging risk to the existing global health governance system.

**India's Competition for Health Security**

India is among the world's largest pharmaceutical manufacturers, producing around 60% of the world's vaccines by volume. While India has developed several vaccine candidates in different stages of clinical trials, the main vaccine it uses for vaccine diplomacy is Covishield, the adapted version of the British vaccine developed by AstraZeneca and Oxford University. The Serum Institute of India (SII), the world's largest vaccine manufacturer, signed a deal in April 2020 to produce 1 billion AstraZeneca-Oxford vaccine doses, half for domestic use and half for other low- and middle-income countries, charging only production costs. With limited domestic inoculation capacity, India has excess vaccines for diplomatic purposes.

India has actively engaged in bilateral and, to a lesser extent, multilateral vaccine diplomacy. Being a lower-middle-income country itself, India is a recipient as well as a contributor to the COVAX initiative. India's vaccine diplomacy focuses on donations to its neighboring countries in South Asia and partners in Southeast Asia and Africa. Under its "neighborhood first" policy, India donated 2 million doses to Bangladesh, 1.5 million to Myanmar, 1 million to Nepal, 500,000 each to Sri Lanka and Afghanistan, 150,000 to Bhutan, 100,000 each to Cambodia and Maldives, and 50,000 to Seychelles in January. In February, India extended its donations to Caribbean countries, offering 570,000 doses to fifteen countries. These countries have a substantial Indian diaspora. So far, India has supplied 6 million doses of vaccine aid and 29.4 million doses as commercial exports, including to major economies such as Brazil, Algeria, South Africa, and Egypt, as well as some countries that received vaccine donations, such as Myanmar and Bangladesh.

India joined COVAX through a membership with the Gavi alliance. The SII is the main producer for the Oxford-AstraZeneca vaccine, up to 700 million doses were expected for 2021. After initial deliveries to North Africa, West Africa, Eastern Europe and the Middle East in March and April 2021, India began to limit vaccine exports until the end of 2021, due to high domestic demand. Based on the high infection rates in India, COVAX was projected to deliver only 145 million doses instead of 240 million by May 2021. Vaccine production was also negatively affected because of a ban by the U.S. on the export of key raw materials. In September 2021, the Government of India announced the resumption of vaccines exports from October 2021 onwards since it had quadrupled its production and only excess supplies would be exported.

**Competition or Complementarity? Global Supply Chain for the Rest of the Global South**

By and large, there are two approaches of Global South's participation in vaccine value chains. First, the Indian case – particularly, SII – demonstrates local companies joining with pharmaceutical multinationals to be part of their global vaccine production, through CDMO and technology transfer contracts. Along with CDMO and technology transfers, India also has own COVID-19 vaccine production facilities – for example, Bharat Biotech. Second, the Chinese case shows the government took initiative of launching research institutes and companies developing own COVID-19 vaccines – Sinovac or Sinophram. Despite increasing vaccine manufacturing capacity through participation in global vaccine value chains to ensure access to vaccines, it may not solve issues of equitable vaccine distribution, simply because vaccine supply chains conducted by China and India are not fully integrated with the existing global supply chains. Rather, they would be conflicting or competing without complementarities.

China's and India's approaches to vaccine diplomacy vary in terms of objective, strategy, and operational practicality. Any pure sense of philanthropic aid cannot be applicable to the two powers, thereby making vaccine aid being a small portion of the exported volume of vaccine doses. Both countries prioritize bilateral channels to conduct vaccine diplomacy. China has a global ambition to provide vaccines to developing countries across the Global South as it aspires to become an economic and technology hegemon with manufacturing capabilities of vaccines. To achieve this goal, it has invested heavily in vaccine development, transnational clinical trials, and its own platform for global supply chain, which ultimately won orders for hundreds of

millions of doses. China's vaccine diplomacy, aligned with its BRI and GDI, is more likely to aim to export jobs, technology, and supply chains.

India's objective, on the other hand, is more regional, compared to that of China. With no self-developed vaccine just like China, India's vaccine diplomacy is built on its role as the main manufacturer for AstraZeneca, which allows it to produce vaccines at low cost and distribute them with little resistance. This means that the country's vaccine diplomacy is conducted through aid to its neighboring states and the Global South as opposed to commercial sales.

India and China do not always implement vaccine diplomacy in a separate way without the strategic calculation of the other player's ambitions. Although differing in geopolitical ambition and diplomatic tactics, they compete for international recognition and influence over developing countries. Unlike traditional security-based competition, however, this vaccine competition to provide public goods offers more opportunity than risks to regional countries. Neither China's nor India's vaccine aid is exclusively confrontational, and smaller countries are able to enjoy selecting a better supplier by playing with one power against the other, thereby hedging between powers to secure more doses.

However, this competition in vaccine diplomacy has its own risks. Even though China and India differ in their strategies and tactics, they do operate in the same region, and their vaccine diplomacy can intersect with other dimensions where they are more competitive or even confrontational. The dynamics between the two countries are also influenced by major powers within the region of Indo-Pacific. Through the Quad, the United States, Japan, and Australia are grouped with India and decided to supply about 1 billion COVID-19 vaccine doses across the Indo-Pacific region by the end of 2022 to counterbalance China's growing influence. If competition intensifies to the point that smaller countries must take sides, that will bring new uncertainties to the Indo-Pacific.

Unlike the 'just-in-time' model for vaccine supply chains, maintaining stockpiles of critical medicines and raw materials, or 'just-in-case' supply chain models that are anchored in preparedness, has shown to be more resilient to price volatility, geopolitical instability, and climate-related disruptions. This is important because supply chains are situated within, and shaped by, a country's health system, socioeconomic conditions, and political institutions. Significant functional challenges – for example, underdeveloped transportation networks, shortages of skilled labor, obscure regulatory environments, and weak governance mechanisms – demonstrate the need for a systems-approach to building resilience. Strategies to strengthen supply chain resilience therefore need to be informed by contextually relevant evidence and inclusive of the specific needs of local populations. This is especially true in LMICs of the Global South, where vast inequities persist between rural and urban settings, and across religious, racial, ethnic, and gender divides, thereby shaping communities' quality of, and access to, health systems and commodities.

**References**


Access to Medicine Foundation. 2023. *Amsterdam Session on Global Health Security – Meeting Report*. Retrieved from https://accesstomedicinefoundation.org/resource/amsterdam-session-on-global-health-security-meeting-report.

Evenett, S. J., B. Hoekman, N. Rocha, and M. Ruta. 2021. "The Covid-19 Vaccine Production Club: Will Value Chains Temper Nationalism?" *Policy Research Working Paper* 9565. Washington, D. C.: World Bank. Retrieved from https://openknowledge.worldbank.org/server/api/core/bitstreams/0365d859-c722-5baf-a7d8-821b9dc5eaca/content.

Frisch, M. F., K. W. Scott, and A. Binagwaho. 2021. "An Implementation Research Approach to Reorient Health Supply Chains toward an Equity Agenda in the COVID-19 Era," *Annals of Global Health* 87(1).

Reproductive Health Supplies Coalition. 2021. *Building Resilient Sexual and Reproductive Health Supply Chains During Covid-19 and Beyond*. Retrieved from https://www.rhsupplies.org/uploads/tx_rhscpublications/BUILDING_RESILIENT_Sexual_and_Reproductive_Health_SUPPLY_CHAINS_DURING_COVID-19_AND_BEYOND.pdf.

Subramanian, L. and J. Nayler. 2021. *Africa's Covid-19 Vaccine Supply Chain and Logistics Readiness*. London: Pamela Steele Associates Ltd. Retrieved from https://www.pamsteele.org/wp-content/uploads/2021/03/20210308_Africa_Covid_Vaccine_Logistics_Final.pdf.

Yang, S. 2021. "Rising-Power Competition: The Covid-19 Vaccine Diplomacy of China and India," *Emerging Voices on the New Normal in Asia.* Washington, D. C.: National Bureau of Asian Studies. Retrieved from https://www.nbr.org/publication/rising-power-competition-the-covid-19-vaccine-diplomacy-of-china-and-india/.

# Session 3

# Conflicts and Cooperation in Cybersecurity

| | |
|---|---|
| **Moderator** | **Won Gon Park** (EAI; Ewha Womans University) |
| **Presenters** | **Motohiro Tsuchiya** (Keio University)<br>"Japan's Response to Cyber Threats in East Asia"<br>**So Jeong Kim** (Institute for National Security Strategy)<br>"Malicious Cyber Threat from DPRK: Implication for ROK"<br>**Minwoo Yun** (Gachon University)<br>"The Future of Cyberwarfare: An Emphasis of Cyber Cognitive Warfare" |
| **Discussants** | **In Tae Yoo** (Dankook University)<br>**Yonghan Park** (Korea Institute for Defense Analyses)<br>**Jungmi Cha** (National Assembly Futures Institute) |

# Japan's Response to Cyber Threats in East Asia

Motohiro Tsuchiya

## 1. Introduction

The United States government has named China, Russia, Iran, and North Korea as sources of cyberattacks; the cyberattacks surrounding the 2014 film *The Interview* gave a strong impression of North Korea's cyber capabilities. The Japanese government does not often attribute cyberattacks, but in the 2017 WannaCry incident, it made an exception and attributed the attack to North Korea.

As North Korea repeatedly conducts missile launch tests and nuclear tests, it has become a well-known fact that cybercrime by North Korea is being used as a source of funding for such tests. In its interim report, the United Nations Panel of Experts, which examined the implementation of sanctions against North Korea, announced that North Korea stole 1650.5 million USD in crypto assets through cyber attacks in 2022.[1]

In Japan, the Japan Aerospace Exploration Agency (JAXA) was hit by another cyber attack at the end of November 2023. But it is better to say that the agency has been continuously hit by cyber attacks and one of them was successful this time. It was later discovered that when the Japan Pension Service was cyber-attacked in 2015 and pension and other records were taken, more than 1,000 government ministries, companies, universities, and other organizations in Japan were simultaneously cyber-attacked. It should be considered that Japan is constantly exposed to cyber-attacks, and only a further fraction of those successful attacks are reported.

When it comes to cyber security, there is no longer contingency or peacetime. Cyber defense must be conducted 24 hours a day, 7 days a week, 365 days a year. Active Cyber Defense (ACD) is the approach that should be taken by those involved in cyber defense, which never rests. In this paper, we would like to discuss how to improve Japan's cyber security capability, focusing on ACD in the National Security Strategy announced by the Japanese government in December 2022.

## 2. Active Cyber Defense

The term "active defense" began to be used in the cybersecurity world as late as 2011, to the author's recollection. He remembers one Japan Self-Defense Forces (SDF) officer asking him what he thought of the U.S. active defense. At that time, the word "cyber" was not between "active" and "defense". Perhaps it had been discussed in the U.S. military before that, and it came to Japan through the SDF.

The author participated in the "Council on Security and Defense Capabilities[2]" to discuss the "National Defense Program Guidelines for FY 2019 and Beyond." At the second meeting of the council on September 21, 2018, the author reported on "Cyber Security Challenges" and included the line "Examining Active Defense: Attack and Defense are Two Sides of the Same

[1] https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/dprk_open_briefing_13_nov_2023_chair_statement_poe_briefing_1_3.pdf

[2] https://www.kantei.go.jp/jp/singi/anzen_bouei2/index.html

Coin" in his presentation material.[3] This means that by that time, active defense was already being discussed among cybersecurity stakeholders in Japan.

In the 2018 NDPG approved by the Cabinet in December 2018,[4] active defense and similar terms were not included. However, the so-called "capability to disrupt" was incorporated. In other words, "SDF will fundamentally strengthen its cyber defense capability, including capability to disrupt, during an attack against Japan, the use of cyberspace by an attacker."

What this "capability to disrupt" means was not specified. However, the fact that Japan is allowed to maintain the ability to disrupt its opponent's cyber capabilities, rather than being forced to defend itself against attack, is a step forward in improving Japan's cybersecurity capabilities.

On June 5, 2020, Chief Cabinet Secretary Yoshihide Suga was asked at a press conference following a cabinet meeting whether Japan needed to review its National Security Strategy in response to the spread of the new coronavirus, to which he replied, "The basic policy does not easily change, and I do not think it is necessary to review the strategy at this time."[5] However, in mid-June, Prime Minister Shinzo Abe began to express his intention to review the National Security Strategy in order to consider the so-called "counter-strike capability," and at a press conference on June 19, Chief Cabinet Secretary Suga said, "I would like to discuss it firmly within the scope of the Constitution and under the concept of exclusive defense," and the move toward a review began.[6] And Prime Minister Suga, who took office in September 2020 following Prime Minister Abe's resignation, also indicated his intention to review the national security strategy. In June 2021, the government was considering simultaneously reviewing not only the National Security Strategy but also two other documents: the National Defense Program Guidelines and the Medium Term Defense Program.[7]

When Prime Minister Suga stepped down in October 2021, his successor, Prime Minister Fumio Kishida, stated in his first policy speech, "We will work on the revision of the National Security Strategy, the National Defense Program Guidelines, and the Medium Term Defense Program." The debate over the revision of the three documents began here, but it was Russia's invasion of Ukraine, which began on February 24, 2022, that shook up the debate.

Russia had launched cyber attacks about a month before invading Ukraine with ground troops. They were perceived as a precursor to a military invasion, and the Ukrainian side quickly increased its defensive posture. Since Russia's unilateral annexation of the Crimean Peninsula in 2014, Ukraine had been preparing for such an eventuality in cybersecurity, and since President Wlodimir Zelensky took office in May 2019, the information technology (IT) industry has been working with the president and Mikhail Fedorov, Deputy Prime Minister and Minister Digital Transformation, and measures were taken to protect critical infrastructure industries. Thanks to these measures, in 2022, Russian hybrid warfare, including cyberattacks, did not achieve the expected results, but rather Ukraine's anti-hybrid warfare did.

[3] https://www.kantei.go.jp/jp/singi/anzen_bouei2/dai2/siryou3.pdf
[4] https://www.mod.go.jp/j/policy/agenda/guideline/2019/pdf/20181218_e.pdf
[5] 「国家安全保障戦略『見直す必要ない』　菅官房長官」『日本経済新聞』2020年6月5日電子版。
[6] 「国家安保戦略、多角的に改定　日米安保発効60年」『日本経済新聞』2020年6月19日電子版。
[7] 「日米防衛指針、自民に改定論　台湾・南シナ海対処を検討」『日本経済新聞』2021年6月4日電子版。

## 3. Japan's National Security Strategy

This situation had a significant impact on the revision of Japan's three documents, particularly the emphasis on improving cybersecurity capabilities. Among the three documents adopted by the cabinet in December 2022, there are some eye-opening points in cybersecurity, especially in the National Security Strategy.[8]

First, the term "cyber national security (サイバー安全保障)" was used instead of "cyber security (サイバーセキュリティ)" in Japanese katakana characters, which emphasizes the national security aspect. It also says, "In order to ensure secure and stable use of cyberspace, especially the security of the nation and critical infrastructures, the response capabilities in the field of cybersecurity should be strengthened equal to or surpassing the level of leading Western countries." The phrase "surpassing the level of leading Western countries" is very ambitious considering Japan's cybersecurity capabilities up to that point. Although it is not easy to achieve cybersecurity capabilities surpassing those of the U.S., a politician from the ruling party responded to the author's question that it is not a bad thing to have high goals.

Second, "active cyber defense" was written in. It says, "Japan will introduce active cyber defense for eliminating in advance the possibility of serious cyberattacks that may cause national security concerns to the Government and critical infrastructures and for preventing the spread of damage in case of such attacks, even if they do not amount to an armed attack."

The phrase "eliminating in advance" is particularly noteworthy. This is because in the 2018 NDPG it was assumed that an attack would take place first, and then the "capability to disrupt" could be exercised as a counterattack. However, "eliminating in advance" means eliminating cyber-attacks before they are launched, which implies the ability to detect cyber-attacks. This would represent a significant and revolutionary shift in Japan's cyber security capabilities.

The government will consider the following three measures to realize this active cyber defense.

(a) Japan will advance efforts on information sharing to the Government in case of cyberattacks among the private sector including critical infrastructures, as well as coordinating and supporting incident response activities for the private sector.
(b) Japan will take necessary actions to detect servers and others suspected of being abused by attackers by utilizing information on communications services provided by domestic telecommunications providers.
(c) For serious cyberattacks that pose security concerns against the Government, critical infrastructures, and others, the Government will be given the necessary authorities that allow it to penetrate and neutralize attacker's servers and others in advance to the extent possible.

To "detect servers and others suspected of being abused by attackers," it is essential to have the cyber intelligence capability to find out what the attacker is really doing, and to "penetrate and neutralize the attacker's servers and others in advance" means not only detecting what the attacker is doing, but also taking some measures against the attacker's system. The conventional interpretation of the law is that such measures violate Article 21 of the Constitution, the secrecy

[8] https://www.mod.go.jp/j/policy/agenda/guideline/pdf/security_strategy_en.pdf

of communications under Article 4 of the Telecommunications Business Law, or the Unauthorized Computer Access Prohibition Law. Introducing active cyber defense means overcoming these legal restrictions.

Third, it says, "In order to realize and promote these efforts, including active cyber defense, the Cabinet Cyber Security Center (NISC) is to be reorganized and a new organization is to be established to coordinate policies in the field of cyber security in a unified and comprehensive manner." The NISC was originally called the "National Information Security Center," but was reorganized in 2015 with the passage of the Cybersecurity Basic Act. It is envisioned that it will be further reorganized and become an organization with national security at the forefront. It is not clear at this stage who will be in charge of active cyber defense, but the new NISC will be involved in some way.

Some have expressed uncertainty about the definition of "active cyber defense," but at this stage there is no formal definition by the Japanese government. In the United States, the Department of Defense released a summary of its Cyber Strategy in September 2018[9] that drew attention to the use of the term "defend forward." It is "to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict" and "to stop threats before they reach their targets." The U.S. Cyber "Defend Forward" Strategy may serve as a reference case. However, the Japanese government should define its own active cyber defense.

For such discussions, the Japanese government is expected to set up an expert panel for active cyber defense. It was scheduled in summer 2023, but it is delayed. On October 25, 2023, Prime Minister Kishida was asked by Yuichiro Tamaki, representative of the Democratic Party of Japan, at a plenary session of the House of Representatives about the delay in the submission of the Basic Act on Cyber Security to the Diet, and he replied, "We will continue to work on it so that we can present a bill as soon as possible. Asked about the delay in the government's consideration, Hidetoshi Iijima, Deputy Director General of the Cyber Security System Preparatory Office, Cabinet Secretariat, said, "The entire government is now vigorously studying the issue," and further stated, "We are studying the issue while sorting out the relationship with the Constitution and other existing laws, as well as the necessity from a national security standpoint." As for the expert panel, he said, "We will make a decision based on the progress of the panel.

## 4. International Cooperation

If Japan can improve its cybersecurity capabilities, it will be able to cooperate with and further enhance those of leading countries.

Japan has long been allied with the United States under the Japan-U.S. Security Treaty. In recent years, the U.S. has been frustrated with Japan's cybersecurity capabilities and has sought to improve and support them, and according to U.S. National Security Agency (NSA) documents exposed by Edward Snowden in June 2013, the U.S. and Japanese governments cooperate in many ways, with the NSA in particular actively cooperating with Japan's Ministry of Defense and Self Defense Forces.

[9] https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

In the Guidelines for Japan-U.S. Defense Cooperation, released on April 27, 2015, the U.S. and Japanese governments "called for continued progress in cooperation on cyberspace issues, particularly in the areas of threat information sharing, mission assurance, and critical infrastructure protection, through the whole-of-government Japan-U.S. Cyber Dialogue and the Cyber Defense Policy Working Group." [10] In March 2014, Japan's Self-Defense Forces established a Cyber Defense Unit, which has been gradually expanded since then, and cooperation and collaboration with the U.S. is ongoing.

The Joint Declaration of the QUAD, a framework for Japan-U.S.-Australia-India cooperation, states that " The Quad partners will coordinate capacity building programs in the Indo-Pacific region under the Quad Cybersecurity Partnership."[11] Under the partnership, it says, "As partners, we seek to cooperate to enhance the development of: critical infrastructure cybersecurity, supply chain risk management, software security, workforce development."[12]

On August 18, 2023, the leaders of the United States, Japan, and South Korea held a summit meeting at Camp David in the United States and issued a joint statement. It stated, " We express concern regarding the DPRK's illicit cyber activities that fund its unlawful WMD and ballistic missile programs. We announce the establishment of a new trilateral working group to drive our cooperation, including with the international community, to combat DPRK cyber threats and block its cyber-enabled sanctions evasion."[13] In response, in November 2023, it was announced that the three countries would establish a new high-level "Cyber Consultative Body." The body will meet regularly on a quarterly basis to discuss countermeasures against cyber-attacks, which are a major source of funding for North Korea's nuclear and missile development.

In November 2023, the first Japan-NATO Cyber Dialogue was held in Brussels, and a wide range of issues were discussed, including the cyber policies of both NATO and Japan and future Japan-NATO cooperation in the cyber field. The participants confirmed that they would continue to work closely together in the cyber field, taking advantage of the Japan-NATO Cyber Dialogue and other opportunities.[14]

A multilayered framework of international cooperation, including Japan-US, Japan-US-Australia-India, Japan-US-ROK, and Japan-NATO, will help improve Japan's cyber security capabilities, which have been limited in the past. However, even though information sharing is important, it is not enough for Japan to simply receive information unilaterally. It is most necessary to improve its own cyber security capability and expand its cyber intelligence capability to collect a large amount of information, analyze it by itself, and use it for policy making. Active cyber defense capability is at the core of this capability.

## 5. Conclusion

Improving cyber security capabilities is an urgent issue for Japan that needs to be addressed as soon as possible. At the same time, however, it is certain that this requires careful discussion in relation to the protection of citizens' privacy. Security and privacy are sometimes a trade-off,

[10] https://warp.da.ndl.go.jp/info:ndljp/pid/11591426/www.mod.go.jp/e/d_act/us/anpo/pdf/js20150427e.pdf
[11] https://www.mofa.go.jp/fp/nsp/page1e_000401.html
[12] https://www.mofa.go.jp/mofaj/files/100347892.pdf
[13] https://www.mofa.go.jp/mofaj/files/100541771.pdf
[14] https://www.mofa.go.jp/mofaj/press/release/press4_009859.html

but they are not completely zero-sum either. We must avoid a situation in which the emphasis on privacy becomes so great that cyber-attacks on critical infrastructure are allowed to threaten the lives of citizens. We would like to see the establishment of a legal system that responds to the threat of global cyberspace, which is approaching a lawless zone, after exhaustive discussions.

On top of that, we should establish and develop cooperative and information-sharing relationships in a multi-layered international partnership, and improve our capability to respond to state and non-state actors that conduct cyber attacks. Japan's cybersecurity capabilities were assessed by the International Institute for Strategic Studies (IISS) as Tier 3, the lowest of the three tiers, shocking all concerned.[15] However, Japan has managed to thwart cyber attacks against mega events such as the G20 Osaka Summit in June 2019, the Rugby World Cup from September to November 2019, new emperor's coronation ceremony in October 2019, the Tokyo Olympic and Paralympic games in summer 2021, and the G7 Summit in May 2023. Despite the legal restrictions, the cyber defense capability is not necessarily low. We should promote the development of a legal system to further improve it.

## References


Kaplan, Fred. 2016. *Dark Territory: The Secret History of Cyber War*, New York: Simon & Schuster.

Perlroth, Nicole. 2021. *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race,* London: Bloomsbury.

Sanger, David E. 2018. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, New York: Crown.

White, Geoff. 2023. *The Lazarus Heist: From Hollywood to High Finance: Inside North Korea's Global Cyber War*, London: Penguin Business.

土屋大洋『サイバーグレートゲーム―政治・経済・技術とデータをめぐる地政学―』千倉書房、2020 年。


[15] https://www.iiss.org/research-paper/2021/06/cyber-power---tier-three/

# Malicious Cyber Threat from DPRK: Implication for ROK

So Jeong Kim

## 1. Key challenges South Korea seeks to address in cyberspace

The Republic of Korea has a double exposure to cyber threats: Firstly, as a highly developed and one of the best-connected countries in the world it is vulnerable to criminal cyberattacks and cyber espionage. Secondly, it is one of the prime targets of North Korean hackers, as part of its grey zone war fare. For North Korea (DPRK) cyber criminality is an important source of income and contributes significantly to its budget on which the stability of the regime depends. The recently released Mandiant Report on North Korea illustrates the scope of cyberattacks and cryptocurrency theft against a diverse range of targets (Mandiant 2023). These activities are part of the intensive efforts to evade traditional sanctions and secure funds for the North's nuclear weapons program (Kim 2022a).

Concerning North Korea, the US Office of the National Intelligence is very clear in its 2023 threat assessment not only for South Korea but also for the United States: "North Korea's cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat. Pyongyang's cyber forces have matured and are fully capable of achieving a range of strategic objectives against diverse targets, including a wider target set in the United States. Pyongyang probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States. North Korea's cyber program continues to adapt to global trends in cybercrime by conducting cryptocurrency heists, diversifying its range of financially motivated cyber operations, and continuing to leverage advanced social engineering techniques." (Office of the Director of National Intelligence 2023) This makes the US with which South Korea has an 'iron-clad' security alliance, an important partner for cyber diplomacy.

North Korea's emergence as a cyber threat stems from its strategic use of cyber operations to generate funds, evade sanctions, and advance its political goals. The nation has invested heavily in building a sophisticated cyber warfare capability, and several key characteristics make its cyber activities particularly dangerous:

North Korea's cyber operations are orchestrated and supported by the state. It is known that the Reconnaissance General Bureau (RGB) oversees these activities, utilizing specialized units like Bureau 121 and state-sponsored hacker groups like Lazarus Group. These characteristics distinguish it slightly from other countries that utilize mafia or voluntary hackers to attack other nations, as the vast majority of its cyber activities are backed by state sponsorship.

With international sanctions limiting its access to global financial systems, North Korea turned to cybercrime to obtain funds. They have engaged in various cyber activities like hacking banks, cryptocurrency theft, and conducting ransomware attacks to generate revenue estimated in billions.

North Korean hackers exhibit advanced capabilities, utilizing techniques like spear-phishing, malware deployment, and social engineering to infiltrate targets. APT Groups: APT (Advanced Persistent Threat) groups are known for their persistence, advanced techniques,

and targeting of critical infrastructure, governments, financial institutions, and cryptocurrency exchanges. Thus, North Korea's cyber activities have caused significant economic damage globally.

Recently, North Korean cyber operations transcend borders, posing a threat to institutions and individuals worldwide. Their ability to conduct operations from remote locations allows them to remain elusive and difficult to track.

The combination of state support, advanced technical expertise, financial motivations, and global reach makes North Korea's cyber threat particularly dangerous. Their activities not only target financial systems but also pose a broader risk to international security, stability, and critical infrastructure. Moreover, the shift towards cryptocurrency-enabled crime has provided them with a decentralized means to finance their agenda while evading traditional financial restrictions and monitoring.

Concerns have arisen also regarding the emergence of a new political alignment and potential escalation of competition, as North Korea demonstrates a closer alignment with countries such as Russia, Iran, and China (Lee 2023). North Korea supported Russia during the Russo-Ukraine War (*Financial Times* 2023) while concurrently hacking into a Russian missile development firm (Pearson and Bing 2023). Also, North Korean IT workers help spy from UAE and Russia (Stone 2023). Various threats, including the securing of technological competitiveness through intellectual property theft and influence operations capable of inducing societal unrest, are being observed.

## 2. Recent cyberattack from North Korea (cases)

North Korea, while directly and indirectly operating hacking groups like Lazarus, utilizes the proceeds from these hacks as a new source of funds. Through this, they amass a substantial amount of illicit foreign currency continuously. Previous attacks by North Korea on the financial sector were primarily direct assaults on the financial system. In February 2016, the North Korean hacker group 'Lazarus' hacked $951 million (approximately 1.812 trillion won) from the Central Bank of Bangladesh, which was stored in the Federal Reserve Bank of New York. Due to an error during the hacking attack, the actual damage amounted to $65 million (approximately 74 billion won), significantly less than the initially targeted amount. While traditional hacking into established financial systems, like the Central Bank of Bangladesh incident, requires intricate processes, including money laundering, even after system penetration, the theft and laundering of virtual currency in the cryptocurrency market are comparatively easier. Experts predict that North Korea's theft and exploitation of virtual assets will persist due to this ease of use compared to attacking physical cash.

North Korea is increasingly leveraging cutting-edge technology by shifting its focus from attacks on physical cash to transferring targets to cryptocurrencies and other virtual assets. Law enforcement agencies, starting to trace and recover stolen assets through cryptocurrencies, as seen in the Colonial Pipeline incident, prompted hackers to make it more difficult to track by converting and trading assets across different cryptocurrencies. Consequently, the rise of 'mixer' services, enhancing anonymity, has been in vogue, with North Korea actively exploiting this trend (Kim 2022a).

North Korea continues to pose persistent threats in cyberspace. It was confirmed that suspected North Korean forces hacked the email account of a key figure within Sejong Institute, a prominent domestic think tank specializing in inter-Korean relations and diplomatic security. Considering the substantial relevance of Sejong Institute's research findings in actual policy formulation, it's difficult to rule out the possibility that hackers accessed significant research and analytical data related to the Korean Peninsula from this director's mailbox. Amid reinforced sanctions against North Korea, resulting in increased difficulty in earning foreign currency, North Korean actors persist in their attempts to either pilfer data from major domestic companies through hacking or engage in ransomware activities (김성훈, 안정훈 2023).

It has been revealed that there was an attempt to manipulate a mobile application used by over 20 million Koreans for e-commerce, intending to distribute malware. This malicious code was transmitted through an e-commerce app, 'Coupang,' and was traced back to the North Korean hacking group known as 'Kim Su-ki.' The manipulated app intercepted by the National Intelligence Service in October was a variant of malware derived from Kim Su-ki's disguised app, 'Hancom Viewer,' created last year. Kim Su-ki is also among the hacking organizations recently added to the exclusive sanctions list by the U.S. Treasury Department (문재연 2023).

Richard Haass, a prominent figure in U.S. foreign and security policy and the President of the Council on Foreign Relations (CFR), during his visit to South Korea, emphasized the necessity of regulating cyber technologies for global progression toward order rather than chaos. He highlighted the imperative to prevent countries like Russia, North Korea, and China from disrupting democratic processes through cyber technologies, specifically mentioning upcoming elections in Taiwan, South Korea, and the United States (조재연 2023).

In a recent police investigation, it was uncovered that following multiple instances of North Korea's hacking organization 'Lazarus' breaching the court computer network and extracting information, another group known as 'Andariel' hacked dozens of domestic defense companies, IT firms, technology institutes, and research centers from December last year to March this year, siphoning off 1.2TB of data. This cache reportedly included plans for advanced laser anti-aircraft weapons developed by the South Korean military along with weapon production blueprints (「이데일리」 2023).

There have been instances where hackers collaborated with ransomware 'Magniber' from October 15, 2018, to July 26, 2022, infiltrating victims' computers, rendering them unusable, and extorting approximately 2.66 billion won from victims under the guise of computer recovery costs. Magniber, a type of ransomware, encrypts all files on the victim's computer and demands money in exchange for decryption. It primarily infects users with Korean-language operating systems and Korean IP addresses, altering the file extension after encrypting the targeted computer files (송원형 2023).

### 3. How does South Korea exercise diplomatic influence

Overall, the South Korea’s cyber diplomacy has been strongly driven by broader national interests caused by its relations with the DPRK. The bilateral cyber dialogue with the US is the

most important one, given the South Korea's dependence on US security guarantees, the US stakes in the stability of the Korean peninsula and the high sophistication of US cyber capacities.

The United States tracks cryptocurrencies to prevent North Korea's theft and unlawful use, employing measures such as prosecution and criminal justice cooperation, including asset seizures. Additionally, actions encompass travel bans, asset freezes, trade restrictions, cessation of development aid and security support, arms export prohibitions, financial transaction bans, diplomatic measures like protests, condemnations, pursuing international organization sanctions, diplomatic expulsions, or embassy closures. To facilitate this, the Countering America's Adversaries Through Sanctions Act (CAATSA) was enacted. Executive Orders 13694 (2015) and 13757 (2016) designate malicious cyber activities as a national emergency and authorize sanctions, while Executive Order 13722 (2016) specifically outlines comprehensive prohibitions and sanctions on dealings with the North Korean government (김소정 2023).

Following these laws and executive orders, the U.S. Department of the Treasury consistently announces sanction measures to thwart North Korea's theft of virtual assets. The Office of Foreign Assets Control (OFAC) within the Treasury has even prohibited the use of 'Tornado Cash,' a cryptocurrency mixing service. Moreover, individuals violating the U.S. government's ban on travel to North Korea and engaging in cryptocurrency-related academic conferences in North Korea or providing cryptocurrency-related knowledge to help North Korea circumvent sanctions have faced imprisonment sentences imposed by the U.S. government (함지하 2020).

Following the 2022 ROK-US Summit which addressed North Korea's malicious cyber activities, both nations made substantial commitments to counter North Korea's illicit gains from its foreign IT personnel and to prevent sanctions evasion through cryptocurrency theft. They prevented North Korea acquiring resources necessary for its nuclear and missile programs. This resulted in a joint government advisory by the Ministry of Foreign Affairs and the National Intelligence Service on December 8, 2022 urging domestic companies to exercise prudence and enhance identity verification measures when engaging IT personnel who may conceal their North Korean nationality and identity. Concurrently, North Korean individuals and seven entities have been singled out as the initial independent sanction targets in the realm of cyber activities. South Korea and the United States have jointly designated a North Korean national as sanctions target due to their involvement in North Korea's financing of weapons of mass destruction (WMD) through illegal cyber activities.

The 2022 ROK-US Summit brought a further deepening of the cooperation in cyber security leading to the declaration of a "strategic cyber security cooperation framework" in 2023. This Framework confirms the principles articulated during the 2022 ROK-US Summit, underscoring the significance of cybersecurity as a national policy and strategic priority. Its primary objective is to advance an open and collaborative approach aimed at ensuring the security and integrity of the internet and cyberspace (Kim 2022b).

Building upon these initiatives, the 2023 "Strategic Cybersecurity Cooperation Framework" distinguishes itself by its commitment to enhancing cooperation across technology, policy, and strategic domains while fostering trust. Moreover, it articulates South Korea's position within the competitive landscape. Ensuring the execution of follow-up actions is imperative to consolidate the achievements of this framework.

The 2023 trilateral summit in Camp David committed the three to plan, “to coordinate regional capacity-building efforts to ASEAN and Pacific Island countries to ensure that they are mutually reinforcing and maximally beneficial to our valued partners, including through capacity building efforts in cybersecurity and financial integrity and our new Trilateral Maritime Security Cooperation Framework.” “We express concern regarding the DPRK’s illicit cyber activities that fund its unlawful WMD and ballistic missile programs. We announce the establishment of a new trilateral working group to drive our cooperation, including with the international community, to combat DPRK cyber threats and block its cyber-enabled sanctions evasion.” (The White House 2023)

The inaugural meeting of the 'Trilateral Working Group among the United States, Japan, and South Korea on Countering North Korean Cyber Threats' took place in Tokyo in last July. Representatives from the three nations evaluated the collaborative achievements in curbing illegal cyber activities, identified as primary funding sources for North Korea's major nuclear and missile development. They anticipated that the formation of this working group would further strengthen the coordination among the diplomatic authorities of the three countries.

**4. Implication for ROK for future efforts**

Through the Russo-Ukraine and the Israel-Hamas war, the potential for non-state actors to engage in cyber warfare has emerged, with the cashing out of stolen virtual assets taking place in friendly North Korean countries such as China and Russia. Given these factors, considerable imagination is required to anticipate how North Korea will persist in its attacks moving forward. As a new business model, North Korea's potential to conduct hacking operations not only causing financial damage but also engaging in activities such as espionage and proxy warfare remains high.

Experts from diverse fields need to convene to develop predictions and scenarios for North Korea's next threatening activities. It's imperative to devise corresponding strategies and contemplate educational and training programs tailored to respond effectively to these threats. This necessitates collaboration between private sectors and international partners.

Governments worldwide should collaborate and coordinate efforts to track and counter North Korean cyber operations. Establishing joint task forces or coalitions dedicated to addressing these threats could enhance global responses. In this regard, our 2 year long efforts from both South Korea and US to have joint cyber working group on IT personnel, and cryptocurrency heist has been successful. Engaging in diplomatic dialogues and applying diplomatic pressure on North Korea can encourage the nation to adhere to international norms in cyberspace.

The international community should consider rigorously enforcing targeted sanctions on North Korean entities engaged in cybercrimes and cryptocurrency theft. This will restrict their access to global financial systems and hinder their illicit activities. The shift of cash conversion points to areas untouched by the traditional financial sector causes another restriction on this approach, now.

Providing support to countries with less developed cybersecurity infrastructures can strengthen their resilience against North Korean cyber threats. This could involve sharing expertise, providing technical assistance, and enhancing cybersecurity capabilities.

South Korea recognizes the global remit of cyber and is therefore working with the World Bank and Interamerican Development Bank. The enhancement of South Korea's cyber capabilities not only serves to fortify the capabilities in a tangible sense but also aligns with the country's security objectives. Less developed and developing nations in Southeast Asia have actively sought Korea's expertise in various facets, including policy formulation, legal framework development, training, and capacity building. These countries are eager to leverage Korea's extensive experience and knowledge sharing. By extending support for cyber capacity building through avenues like development cooperation or Official Development Assistance (ODA) programs, South Korea can make a meaningful contribution to raising the nation's cybersecurity standards. Focusing efforts on capacity-building activities targeted at Southeast Asian countries and other nations where North Korea exploits IT infrastructure and deploys personnel is likely to yield particularly effective results for both sides (Kim 2023).

The collaboration between the private sector and the international community is pivotal in mitigating North Korea's cyber activities. By combining efforts, sharing information, enforcing regulations, and applying diplomatic pressure, there's a greater chance of reducing the success of North Korean cybercrimes and deterring their malicious activities.

## References


Cho, Sungbaek. 2022. National Cybersecurity Organisation: Republic of Korea (2022) https://ccdcoe.org/uploads/2022/12/ROK-Country-report.pdf

*Financial Times*. 2023. "Kim Jong Un pledges support for Russia's 'sacred fight' in Ukraine." September 13. https://www.ft.com/content/6b8935e8-c6ad-44ce-922a-673e48d9935f

Kim, So Jeong. 2022a. "Considerations for ROK-US Cybersecurity Cooperation in Response to North Korea's Cryptocurrency Thefts", Institute for National Security Strategy, Issue Brief summaries, vol.80, No.53, Nov. 01, 2022.

_____. 2022b. "The 2022 ROK-US Summit and Cybersecurity: Strategic Challenges to Strengthen Deterrence", Institute for National Security Strategy, Issue Brief, Vol.51, No.24, June 23, 2022.

_____. 2023. "Future of ROK-US Cybersecurity: past and future considerations", *Journal of International Community of Korea Studies*, October 2023

Kim, So Jeong, and Sunha Bae. 2021. "Korean Policies of Cybersecurity and Data Resilience", The Korean Way With Data, CEIP.

Lee, Christy. 2023. "North Korea Using Ties With Russia to Boost Standing With China." *Voice of America*. October 26. https://www.voanews.com/a/north-korea-using-ties-with-russia-to-boost-standing-with-china/7329191.html

Mandiant. 2023. "첩보 활동을 위해 사이버 범죄로 자금을 조달하는 북한의 공격 그룹 APT43." https://www.mandiant.kr/resources/reports/apt43-north-korea-cybercrime-espionage

Ministry of Foreign Affairs. 2022. "Indo-Pacific Strategy of Freedom, Peace and Prosperity", December 2022; at https://www.mofa.go.kr/eng/wpge/m_26382/contents.do

*Nikkei Asia*. 2023. “South Korea asks cyber firms for advice on North’s crypto crimes.” 20 July 2023; https://asia.nikkei.com/Spotlight/Cryptocurrencies/South-Korea-asks-cyber-firms-for-advice-on-North-s-crypto-crimes

Office of the Director of National Intelligence. 2023. Annual Threat Assessment (2023); at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

Pearson, James, and Christopher Bing. 2023. “Exclusive: North Korean hackers breached top Russian missile maker.” *Reuters*. August 8. https://www.reuters.com/technology/north-korean-hackers-breached-top-russian-missile-maker-2023-08-07/

Stone, Jeff. 2023. “North Korean IT Workers Help Spy from UAE and Russia, UN Says.” *Bloomberg*. May 31. https://www.bloomberg.com/news/newsletters/2023-05-31/north-korean-it-workers-help-spy-from-uae-and-russia-un-says

The White House. 2023. “The Spirit of Camp David: Joint Statement of Japan, the Republic of Korea, and the United States”, August 2023; at https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/18/the-spirit-of-camp-david-joint-statement-of-japan-the-republic-of-korea-and-the-united-states/

김성훈, 안정훈. 2023. “세종연구원장 이메일 해킹… 北에 외교자료 유출됐나.” 「매일경제」. 12 월 7 일. https://www.mk.co.kr/news/politics/10893425

김소정. 2023. “미국의 사이버공격 대응정책과 한국에의 시사점: 솔라윈즈 해킹 대응사례를 중심으로.” 국가안보전략연구원 연구보고서 2022-04.

문재연. 2023. “’쿠팡 앱’ 위장 공격은 ‘김수키’ 소행… 활개 치는 北 해킹 조직.” 「한국일보」. 12 월 7 일. https://www.hankookilbo.com/News/Read/A2023120612060002841

송원형. 2023. “해커와 짜고 랜섬웨어 유포… 복구비 26 억 챙긴 데이터복구업체.” 「조선일보」. 11 월 20 일. https://www.chosun.com/national/court_law/2023/11/20/EYEDVVZKYVD7LFETKRPNFMOOPE/

「이데일리」. 2023. “[사설] 北 사이버 공격, 전방위 확산… 보안 태세 안심할 수 있나.” 12 월 6 일. https://www.edaily.co.kr/news/Read?newsId=01187366635835896

조재연. 2023. “사이버 기술 통제 필요… 北, 4 월 총선 방해 가능성.”「문화일보」. 12 월 6 일. https://www.munhwa.com/news/view.html?no=2023120601072930103001

함지하. 2020. “미 암호화폐 전문가, 북한 제재회피 조력 정황 추가로 드러나.” 「Voice of America」. 6 월 12 일. https://www.voakorea.com/a/korea_korea-politics_virgilgriffith-nk-cryptocurrency/6032040.html

# The Future of Cyberwarfare: An Emphasis of Cyber Cognitive Warfare

Minwoo Yun[1]

## I. Intersection of cyberwarfare and geopolitics of Northeast Asia

Cyberwarfare has grown increasingly significant as a battleground in both present-day conflicts and presumably those of the future. It has expanded its scope to encompass multiple dimensions, thereby enhancing its strategic importance. To begin with, it encompasses not only cyber technological warfare but also cyber cognitive warfare. Furthermore, it has become an integrated domain that merges cyberwarfare, electronic warfare, information warfare, and cognitive warfare. Lastly, it interconnects with various other realms of warfare, including land, sea, air, space, and human cognition.

The strategic significance of the cyber domain is also crucial in shaping the outcome of the hegemonic struggle in Northeast Asia, as well as globally. Northeast Asia holds a pivotal role in the ongoing global conflict due to the underlying contest between the US and China-contrasting with the earlier Cold War era, which primarily featured the US-USSR rivalry. The victor of the geostrategic competition in Northeast Asia is poised to exert considerable influence over the larger New Cold War across the entirety of Eurasia.

## II. Advancement of cyberwarfare

Formerly cyberwarfare predominantly referred to hostile cyber technological acts through malicious codes. Examples encompassed hacks, DDoS attacks, malware infiltrations, cyber espionage, and more. Yet, it has now evolved into more inclusive and amalgamated manifestations, undergoing progression through various avenues.

Primarily, cyberwarfare increasingly encompasses not just conventional cyber technological actions but also cyber cognitive operations. Presently, cyberwarfare embodies a concept that intertwines cyber-technology warfare and cyber-cognitive warfare. Cyber-technology warfare pertains to technical strategies for attacking and safeguarding hardware and software within computer networks, utilizing malicious software as a tool. Cyber-cognitive warfare entails a sequence of maneuvers targeting the manipulation of thoughts, emotions, and psychology of human users in the cyber realm, using malicious information as a means to this end.

Cognitive warfare aims to alter or influence people’s perceptions. Perception results from cognition, the mental process of acquiring and understanding knowledge, encompassing information consumption, interpretation, and perception. Consequently, the cognitive domain encompasses the awareness and rationality required for executing military maneuvers, utilizing information that shapes the interconnected beliefs, values, and cultures of individuals, groups, and the public. Cognitive warfare predominantly unfolds in cyberspace in the contemporary world, yet it extends beyond cyberspace to offline realms.

[1] Ph.D. in International Politics and Criminal Justice, Professor, Gachon University, Researcher, Future Warfare Research Center, Institute of International Studies, Seoul National University, Visiting Researcher, Asia Center, Seoul National University, South Korea

Examples of cyber cognitive warfare encompass not only traditional forms of military confrontation but also low-intensity conflicts such as terrorism, insurgency warfare, influence operations, FIMI (Foreign Information Manipulation and Intervention), disinformation campaigns, propaganda of violent extremism, and various others. Cyber cognitive warfare knows no domestic or international boundaries, and it often intertwines and overlaps with both times of war and peace. It merges military and non-military domains, as well as governmental and civilian sectors.

More and more, cyber-technology warfare and cyber-cognitive warfare have converged. DDoS attacks or website defacement, despite their relatively low technological sophistication, can mobilize a wide range of participants with lower levels of computer skills. These low-level cyberattacks can generate political and social movements through the involvement of a multitude of participants. Therefore, these attacks are utilized for psychological influence operations or achieving strategic goals through mass mobilization. Another instance of integration, called "hack-n-leak," involves hacking and the dissemination of malicious code to exfiltrate sensitive information. Zombie PCs and botnets are then used as intermediaries to publish sensitive news about the targeted subject. These tactics are ultimately executed through comment manipulation using human trolls, recommending likes, and other means to orchestrate public opinion, propaganda, and narrative warfare. In this case, cyber technological attacks are used as a means to achieve the strategic goal of cyber cognitive warfare.

Secondly, cyberwarfare merges with electronic warfare. In contemporary times, the convergence of cyber warfare and electronic warfare has grown stronger due to the interconnectivity of various wireless combat systems, human command centers, AI-assisted control mechanisms, satellites, data storage facilities, and other components within communication networks on the internet. This interdependence has heightened the overlap between cyberwarfare and electronic warfare.

As a result, electronic warfare has made it possible to influence cognitive warfare in the cyber realm. For instance, through electronic intrusion and theft, it is now feasible to install malicious software on devices like smartphones, tablets, and PCs connected via Wi-Fi. These compromised devices can then serve as launching points for conducting cognitive warfare, such as disseminating fake news, disinformation, and manipulation. The further challenge lies in the development of Brain-Machine Interface (BMI) technology, which connects the brain and computer. This advancement has enabled the integration of human behavior, the brain, and computer software programs and mechanical devices into a single, interconnected network. Human and machine can be totally interconnected and integrated via cables and wireless networks. Both computers and human brains can be hacked.

Thirdly, cyberwarfare becomes increasingly intertwined with warfare in other domains. Future warfare takes place in a multi-domain environment encompassing not only the traditional domains of land, sea, and air but also cyber, space, and the human cognitive domain. This shift in paradigm is propelled by changes in how the results of war are determined. The essential features of future warfare involve the diversification and integration of war domains, erasing the lines between various domains, and ushering in an era of hyper-connected warfare that fuses all domains.

In the context of multi-domain integrated warfare, the cyber domain holds significant strategic importance. In the past, the seas served as massive highways with strategic importance, and those who controlled maritime space held global dominance. This was because controlling

sea communication routes allowed for the freedom of access, movement, and communication essential for successful military operations. This capability could be defined as strategic flexibility. Today and in the future, the cyber domain is expected to provide the same strategic flexibility as the seas did in the past. Thus, the controller of the cyber domain can gain a significant advantage in terms of freedom of access, movement, and communication necessary for military victory.

Lastly, cyberwarfare tends to blur the boundary between war and peace. It establishes a state of constant peaceful war (or warlike peace) as the norm. Peace and war are no longer strictly dichotomous concepts; instead, they need to be understood as part of a continuous spectrum. The current situation lies somewhere along the spectrum between absolute peace and absolute war, and this position is always shifting.

## III. Cyberwarfare in South Korea today

While subject to debate, cyberwarfare remains a persistent threat to South Korea in the present day. China and North Korea pose continuous dangers to South Korea as they engage in active cyber espionage, cyber theft, and influence campaigns. Given its circumstances, South Korea becomes an exceptionally viable target for these cyber operations, aligning with the strategic objectives of these actors.

### 1. China

China's capabilities in the realm of cyberwarfare are regarded as highly menacing. Ever since Xi Jinping assumed leadership, China has dedicated itself to becoming the preeminent global cyber superpower. Over the past decade, Xi Jinping has placed significant emphasis on augmenting cyber prowess. China's strides in cyber capabilities are projected to intensify, particularly with the commencement of its space station missions in 2021. The anticipated full operational status of China's space station, forecasted to occur between 2022 and 2024, is poised to provide a significant boost.

China's hacking endeavors and influence operations are integral components of its all-encompassing information warfare initiatives, harmonizing both physical and cyber domains. This interconnection signifies that China's cyber activities are closely interwoven with its information campaigns in the tangible world. These information activities align with an overarching national strategic objective: the pursuit of regional dominance.[2]

Furthermore, China's involvement in the 5G information and communication network supply chain have engendered apprehensions within South Korea, paralleling the concerns of its Western counterparts. These concerns stem from the profound implications for information security. Considering the intricate interplay between 5G technology and a plethora of internet of Things (IoT) devices, China's sway over the information and communication technology (ICT) supply chain transcends mere hardware provision. This influence spans critical domains like cybersecurity and cyberwarfare, extending into realms of intellectual property, economic interests, and industrial advancement. As a consequence, South Korea finds itself voicing

[2] Interviews with a South Korean security personnel.

escalating worries regarding China's sway over IT networks, materials, components, and equipment.[3]

China's overarching, seamlessly integrated, and medium- to long-term information activities, both in the digital realm and the physical world, are steered by core strategy known as "Unrestricted Warfare" or "Chao Xian Zhan." This strategic framework is anchored in the belief that information activities serve as instrumental tools for achieving China's geopolitical objectives. In essence, Unrestricted Warfare signifies a departure from conventional notions of warfare, encapsulating a multifaceted approach that ventures beyond the boundaries of norms, ethics, and conventional reasoning. This strategy employs an extensive spectrum of unorthodox and non-normative methods, spanning organized crime, bribery, cyber technology appropriation, manipulation of political processes and elections, propagation of disinformation, economic reprisals, cultural maneuvering, and manipulation of public opinion. The ultimate aim is the establishment of a regional order centered around China.

China's information activities can be broadly divided into two primary domains. The first pertains the acquisition of scientific and technological advancements, which in turn supports ongoing economic growth and the modernization of national defense capabilities. The second domain involves influence operations targeted at specific countries, such as South Korea. Both of these domains encompass a blend of offline and online endeavors, working in tandem to accomplish their individual objectives.

Firstly, China conducts cyber espionage and cyber theft, alongside various offline methods, to acquire scientific and technological advancements for the purposes of economic development and defense modernization. Its objective is to attain cutting-edge knowledge, skills, and capabilities in industries and defense sectors. To achieve this, China focuses its efforts on advanced countries like the United States and other Western nations. Within Northeast Asia, South Korea and Japan are key targets for the China's cyber operations aimed at pilfering industrial and defense science and technology.

Secondly, for years, China has been engaged in cyber influence operations as part of its "unrestricted warfare," directed at South Korean elites and the general public. These operations are designed to sway South Korea's orientation toward a more pro-Chinese and anti-American (as well as anti-Japanese) stance. Cyber cognitive operations, coupled with offline influence efforts like Confucious Institute, have been utilized to reshape the opinions of both elites and the public, ultimately influencing election outcomes within South Korea. China's influence campaign in South Korea follows a multifaceted approach, encompassing both online and offline dimensions. This strategy involves a range of activities, such as social and cultural infiltration, financial investments, the establishment of covert overseas police stations, exertion of economic and diplomatic pressure, exacerbation of historical tensions between South Korea and Japan, and numerous other tactics.[4]

[3] CISA. NSA. ODNI. 2021. Potential threat vectors to 5G infrastructure. www.odni.org.

[4] Interviews with a South Korean security official.

### 2. North Korea

North Korea is another significant source of cyber threats against South Korea. The country's capabilities in cyberattacks and espionage activities are currently considered among the highest in the world. According to Andrew Grotto, who was responsible for cybersecurity at the White House during the Obama and Trump administrations, North Korean hackers did not possess such advanced skills just a few years ago. However, they have rapidly developed their capabilities within a short span of time, making them one of the most significant cyber threats globally.

North Korea harnesses its cyber capabilities for diverse purposes, encompassing cybercrime, cyberattacks, cyber espionage, and preparation for cyberwarfare in the event of full-scale war. Firstly, within the realm of cybercrime, North Korea leverages its cyber prowess for financial gains through activities such as cryptocurrency hacking and ransomware attacks. Secondly, in the context of cyberattacks, North Korea deploys its cyber capabilities to execute retaliatory strikes in response to perceived provocations, as well as to install fear and uncertainty among enemy governments and populations. This involves launching malware attacks against pivotal government institutions, financial organizations, critical infrastructure, and communication or broadcasting networks. Thirdly, in the realm of cyber espionage, North Korea employs its cyber capabilities to pilfer defense technologies, medical-pharmaceutical data, and other valuable scientific and technological information. Fourthly, the nation engages in cognitive warfare activities, encompassing the dissemination of propaganda, psychological operations, and the propagation of misinformation, with a particular focus on South Korea. Lastly, North Korea is bolstering its cyber power to cultivate capacities for potential cyberwarfare, especially as a means of supplementing its comparatively inferior conventional military capabilities vis-a-vis South Korea and the United States.

## IV. Cyber cognitive warfare: strategic goals and tactical principles

### 1. Strategic goals

The strategic goals of cognitive warfare are accomplished through the dominance of friendly narratives over enemy narratives. In the cognitive battleground, friendly and enemy narratives collide. The outcome of the battle is determined by whose narratives win the hearts and minds of combatants and civilians via the superiority of intellectual, emotional, and moral persuasiveness.

Narratives are essential tools in cognitive warfare. Narratives are often interchangeable with stories (or story-telling) but are much broader concepts than that. Narratives include story-telling, texts, myths and legends, fables, tales, short-stories, novels, history, dramas, comedies, pantomimes, gestures, paintings, stained glass windows, murals, movies, photographs, news, conversations, lectures, online contents, and online games. They can appear in infinite numbers of forms.

Once narratives enter the realm of cognitive warfare, they become important weapons to achieve strategic goals, namely seizing cognitive dominance. Narratives have many functions in cognitive battle. They mobilize the friendly side, provide direction to friendly combatants, sustain the friendly troops' solidarity, control dissidents, and provide strategic guidance to the

friendly fighting force. To do so, the formulation and diffusion of narrative epics are carefully designed to instigate victim awareness and humiliation, to urge the inevitability of resistance by reconstructing the present that recalls situations from the past, to link their frustrations with the public call for a great cause, and to endow individuals with a sense of authority (self-esteem or self-efficacy) as meaningful actors in a decisive cognitive battle. Through this process, narratives awaken individuals who feel dispersed, frustrated, and helpless, functioning as glue that binds individuals with disparate interests and concerns together as an organized force according to strategic guidance.

Meanwhile, the other important functions of narratives are to disintegrate and disunite the enemy side. Narratives alienate the populace from the government by promoting cynicism, distrust, and hatred of the government, dividing enemy combatants and civilians by fostering confusion and fear, undermining the enemy combatants' and civilians' confidence in their values, institutions, and leadership, and finally obstructing the adversary's decisions and acts.

The attribution of narratives is "strategic communication." Episodes and events should necessarily be translated into stories and then interpreted. A well-crafted strategic narrative connects seemingly unrelated events and actions with those that are related, making such events and actions understandable. According to Freedman, strategic narratives leverage the narrative crafters to embody how the target audience should feel and understand particular events and issues, thereby influencing their behavior. In its earliest stages, the strategic narrative frames the problem and suggests appropriate responses to it. Strategic narratives do not necessarily have to be rational. They may be grounded in empirical evidence, but also rely on emotion, questionable metaphors, and dubious historical reasoning. For these strategic narratives to be successful, they must be relevant to the target audience's deep-rooted culture, historical experiences, prejudiced beliefs, and genuine interests.

Strategic narratives should survive and overcome the attacks of the counter-narratives crafted by the enemy. In this regard, the Russian narrative has not been so successful in the recent Russia-Ukraine war, because the initial Russian "Zelensky government as Nazi" narrative could not be sustained before the overpowering US-West narrative that depicts Putin and the Russian forces as authoritarian criminal aggressors disregarding the liberal democracy and sovereignty of Ukraine. The triumph of the US-West narrative can be evidenced in a South Korean newspaper editorial where a columnist portrays Putin as evil. Strategic narratives may be continually arbitrated, rejected, or impeded by other hostile actors. Thus, the narratives that have been told once are continually referred to, interpreted, applied, and retold by many friendly actors, and passed on to a large audience, including friendly, enemy, and neutral spectators. Through this process, once a narrative enters the realm of the masses, it goes through a process that can make it self-sustaining.

## 2. Tactical principles

Strategic goals and methods are actualized through tactical-level operations. Via the application of strategic methods, the core narrative can be constructed and applied to achieve strategic goals at the level of the long-term theater of war. Such a core narrative is implemented through tactical principles and applications in relatively short-term combat operations. The vertical integration of strategic planning with tactical operations in cognitive warfare is equivalent to

that in conventional kinetic warfare. To execute tactical operations, three key tactical principles need to be kept constantly in mind: preemptive strike, offensive-defense, and striking the messenger. First, a preemptive strike is key to winning a cognitive battle. In narrative clashes, offense always has an overwhelming advantage over defense. This is why preemptive strikes are so important. This process is called anchoring bias. Disinformation could be effectively used for this purpose. A preemptive strike should be combined with intelligence estimates and proactive reconnaissance-surveillance to search for the vulnerabilities of the enemy. Cyber cognitive campaign combined with cyber technological attack, such as hack-n-leak, could be a formidable initial strike.

Second, offensive-defense is a key to defending against the enemy's first strike. Sometimes, it is inevitable to counteract the enemy's first strike. Counter-arguments or rational clarification are often ineffective to unravel or remove anchored bias. Rather, they backfire because they address the same topics or issues and thus reinforce already anchored bias. Factual truth, reasoning, and sound evidence have very limited effects. Rather, counterarguments only make the target population cognitively alert and indoctrinated in favor of the enemy. Thus, striking the enemy's other vulnerabilities is more effective because a new anchored bias against the enemy cancels out the existing anchored bias against the friendly side.

Third, striking the messenger is more likely to be effective than the message (piece of narrative or information). If the messenger gets corrupted or contained, its messages have little destructive power. Striking the messenger can be done either by corruption and degradation or by containment and alienation. Messengers can be persons, communities, or institutions.

## V. Future of cyberwarfare in Northeast Asia

South Korea occupies a central position as a major battleground for cyberwarfare, both during times of peace and in the event of a full-scale war in Northeast Asia. The significance stems from South Korea's positioning along the spectrum of pro-Chinese and pro-American alignment, which has the potential to sway the outcome of geopolitical rivalry between two opposing camps in the region. Therefore, it is imperative for the US, Japan, and South Korea to remain resilient against cyber aggressions from China and North Korea, whether during periods of peace or the potential outbreak of full-scale conflict. This centrality is due to the fact that Northeast Asia has become the epicenter of the new wave of global conflict between the United States and China, in contrast to the previous iteration of the Cold War between the US and the USSR. The victor in the geostrategic competition within Northeast Asia is more likely to emerge triumphant in the broader New Cold War across the entire Eurasian continent. In this critical battle, cyber cognitive domain assumes paramount importance, given that all regional players possess advanced information technology, scientific capabilities, and cyberwarfare expertise. As such, in the Northeast Asia, cyberwarfare stands out as a pivotal factor that could decisively influence the outcome of the geostrategic conflict, exerting a profound impact for years to come.

# Session 4

# U.S.-China Strategic Competition and Economic Security

| | |
|---|---|
| **Moderator** | **Chaesung Chun** (EAI; Seoul National University) |
| **Presenters** | **Kuik Cheng-Chwee** (National University of Malaysia)<br>"Southeast Asian Hedging amid U.S.-China 5G Competition: Explaining the Economy-Security Tradeoffs"<br>**Seungjoo Lee** (EAI; Chung-Ang University)<br>"High Technology and the Evolution of South Korea's Economic Security Strategy"<br>**Yongshin Kim** (Inha University)<br>"South Korea's Experiences of Different Economic Coercions from China and Japan and Lessons for Countering Economic Coercion" |
| **Discussants** | **Wang Hwi Lee** (Ajou University)<br>**Yong Wook Lee** (Korea University)<br>**Ryo Sahashi** (University of Tokyo) |

# Southeast Asian Hedging amid U.S.-China 5G Competition: Explaining the Economy-Security Tradeoffs

Kuik Cheng-Chwee

In an era of intensified U.S.-China competition, geoeconomics *is* geopolitics. On one hand, economic and geoeconomic means are used to pursue political and geopolitical ends. On the other, geopolitical activities are shaping, limiting, and complicating geoeconomic processes. As the U.S.-China rivalry intensifies, geoeconomics and geopolitics are increasingly inseparable. While the links between geoeconomics and geopolitical are not new, the widening big-power rivalries on both military and non-military chessboards are making them an increasingly salient trend across the globe, especially in Asia.

Such dynamics are perhaps most profound in Southeast Asia, a region where the big powers' interests converge. Over the past decade, Southeast Asia has been the center of big-power courtships and competitions across the twin chessboards. Virtually all powers prioritize Southeast Asia for the exercise of military statecraft. Southeast Asia is also a targeted area for the non-military chessboards, where big powers compete to win support from regional countries not only over public health and other non-traditional security cooperation, but also over infrastructure-building, 5G networks, and semi-conductor supply chains. Southeast Asian states are "middle states" sandwiched between the competing powers.

This paper focuses on Southeast Asian responses to the U.S.-China 5G competition as an instance of middle states' responses to big-power competition on the second chessboard. The responses reveal a puzzling pattern: the small- and medium-sized states' have pursued different policies vis-à-vis Huawei and other Chinese tech firms.[1] Vietnam has excluded Chinese vendors from their 5G telecommunication networks but allowed Chinese tech companies to expand operations in its digital economy. Singapore has excluded Chinese tech firms from its major 5G networks but included Huawei in its smaller 5G network. However, other member states of the Association of Southeast Asian Nations (ASEAN) have adopted a more open and receptive stance: welcoming Chinese 5G providers and viewing Chinese firms as sources of opportunities that can benefit their own economy and technology capacity.

Why do Southeast Asian states respond differently vis-a-vis hi-tech competition? I argue that the former approach (i.e., Vietnam and Singapore's approach) is best understood as "heavy hedging", whereas the latter approach (i.e., the other ASEAN states) "light hedging" in digital connectivity cooperation. They represent two distinct approaches to *economy-security tradeoffs*. Vietnam and Singapore are both vigilant on the tradeoffs: prudent about security risks and watchfully seeking ways to minimize those risks, even at the expense of *paying some economic price* or *foregoing* some economic benefits. By contrast, most other ASEAN states take the opposite outlook: prioritizing economic benefits and willingly exploring opportunities to maximize these benefits, while *downplaying* potential risks of digital insecurity, developmental dependency, and other problems.

[1] The remainder of the paper is extracted from Cheng-Chwee Kuik, "Southeast Asian Responses to U.S.-China 5G Competition: Hedging and the Economy-Security Tradeoffs", *Journal of Chinese Political Science* (forthcoming).

**Making Sense of Economy-Security Tradeoffs**

"Tradeoff" is fundamental to policy processes. Literature across disciplines highlight that all policy choices involve tradeoffs. These manifest in multiple forms: compromising one thing in exchange of something else; getting x by giving up y; choosing between two competing goals or alternative actions; (Tetlock et al. 2000) "choosing one solution means foregoing another"; (Winter 2013) privileging one yardstick comes at the expense of another important one; (Skinner 1969) etc.

In the context of inter-state cooperation (e.g., digital connectivity cooperation), tradeoffs occur when a state's pursuit of a prioritized goal exposes the state to some risks, potential harms, and opportunity costs. There are three types of tradeoffs: *sectoral* (e.g., economy versus security), *spatial* (internal versus external), and *temporal* (now versus future/ short- versus long-terms). This paper deals with sectoral tradeoffs, focusing on the nexus between economy and security.

Building upon the "hedging" paradigm in international relations, I explain how and why states make risk-benefit tradeoffs across domains the ways they do. The hedging school's emphasis on risk-mitigation and return-maximization under uncertainty makes it a pertinent paradigm to unpack the dynamics underpinning the tradeoff calculations and choices (Kuik 2008; Lim and Cooper 2015; Haacke 2019). Hedging is defined here as an insurance-seeking behavior aimed at mitigating risks and cultivating a fallback position, while pursuing return-maximizing acts under the conditions of high-stakes and high uncertainties (Kuik 2016). Risks and returns are two sides of the same policy coin. In the policy world, returns are gained side-by-side with risks; benefits are accrued alongside unavoidable downsides. All acts seeking to maximize benefits inevitably come with risks, drawbacks, and dangers. The deeper and wider the uncertainties, the greater the risks, and the higher the tendency for rational actors to hedge against the perceived risks even when they seek to maximize prioritized benefits for as much and as long as possible.

Risks are *omni-present*: they cannot be eliminated, but only mitigated, managed, and offset. Risks are *omni-dimensional*: they manifest not only in security domains (both traditional and non-traditional), but also in economic and political realms (Heng 2022; Kuik and Tso 2022). Risks are *omni-directional*: they are fluid, relative and subjective. Risks are neither fixed nor static, but are constantly evolving, with changing magnitudes, manifestations, and ramifications. Because the meanings and consequences of risks are perceived differently across actors and times, there will always be a process of "riskification", where risks are being *decoded varyingly*—either being perceived and responded to proportionately, or being played up, or down—by policymakers based on prevailing internal and external circumstances (Clapton 2011; Corry 2012; Haacke and Ciorciari 2022; Kuik 2022).

Varying riskification leads to varying choices of risk-mitigation measures, manifesting in varying hedging behavior. That is, different countries hedge in different degrees (and forms). Heavy hedgers are those who: (a) see darker shades of risks from uncertainties; (b) display a greater determination to invest in risk-mitigation measures; and (c) exhibit a greater readiness to forego potential benefits. Light hedgers, by comparison, see lighter shades of risks, prioritize return-maximization over risk-mitigation, and display a greater readiness to defer than defy the stronger partners. In digital connectivity cooperation, countries make *different sectoral tradeoffs*:

heavy hedgers prioritize security over economy, while light hedgers emphasize economic gains over potential security risks.

What explains these distinctive approaches to economy-security tradeoffs? Why do some countries stress security risks, while others prioritize economic benefits? The sectoral tradeoff model treats *elite legitimation*—the imperative of justifying and enhancing the elite's political authority to rule—as the principal determinant, and driver, of tradeoff calculations. Specifically, it postulates that elite legitimation is an intervening variable that filters and decodes the meanings of a given connectivity cooperation (or any external partnerships), assessing its *relative acceptability* in terms of elites' domestic political base (i.e., do the risks *politically* outweigh the benefits) and then responding (including playing down or playing up) accordingly (the riskification process).

### *How* Do States Hedge in Tech Competition?

How do states hedge in the face of big-power 5G competition? Both heavy- and light-hedgers have sought to mitigate *multiple* risks by concurrently pursuing three interrelated approaches: (a) actively signaling their neutrality position (aimed at mitigating the geopolitical risks of being entrapped in big-power conflicts as the U.S.-China rivalry intensifies); (b) inclusively diversifying their partnerships as much as possible (aimed at minimizing the twin economic risks of dependence and downturn); and (c) prudently pursuing mutually-counteracting measures to cultivate a fallback position for as long as possible (with an eye to avoiding the wider, multifaceted risks of external uncertainties and internal resentments). Each of these hedging elements is discernible in the weaker states' policies toward 5G rollouts, some more persistent and consistent than others, as discussed follows.

- **Active neutrality:**

Neutrality—an impartial position where a state insists on not taking sides between the competing big powers—has been the hallmark of Southeast Asian states' alignment. This is true not only for their overarching macro-level postures, but also true of their micro-level choices across domain-specific cooperation. On 5G and broader digital infrastructure domain, no ASEAN state has completely embraced the U.S. Clean Network or China's Digital Silk Road (DSR). The presence of European and Korean tech firms in the digital landscapes of most Southeast Asian states provides them with additional choices of prospective partners. The multiplicity of tech players thus provides space for Southeast Asian states to actively signal their neutral position vis-à-vis the competing powers.

Hence, despite U.S. efforts to persuade its allies and partners to ban China's 5G technology providers, Southeast Asian states have insisted on *making their own decisions*. The ASEAN states have cautiously avoided taking sides with either power over digital connectivity, while stressing their own policy autonomy. Indeed, instead of aligning with the U.S.-led alliance of techno-democracies, the ASEAN states, including *democratic* Indonesia, Malaysia, and the Philippines, have chosen to make their 5G decisions primarily on commercial and technological grounds rather than political ones.

Even though Vietnam, and to some extent Singapore, have excluded Chinese tech firms in their respective 5G networks, the exclusions are *selective* (only limited to highly sensitive areas over cybersecurity concerns) and *not* across-the-board.[2] They did not bar Huawei in their digital ecosystem (unlike U.S. allies across the Indo-Pacific), and they continue to actively engage China in other areas of economic and functional cooperation (Vietnam and Singapore are, respectively, China's top and third largest trading partners in the ASEAN region). More importantly, the two countries, like other ASEAN states, have insisted on impartiality vis-à-vis the competing powers. Having excluded Huawei from its 5G rollout, Vietnam took pains to emphasize that its decision was neither about siding with Washington nor succumbing to external pressures. Similarly, Singapore's 5G policy was made out of its own national considerations, and not about choosing sides. Even the Philippines and Thailand, the two treaty allies of the United States, have adopted an impartiality approach.

- **Inclusive diversification**:

Central to Southeast Asian hedging is a persistent effort to diversify a state's developmental and strategic partnerships beyond any one big power (or any one coalition) across domains. As for digital connectivity, as well as other realms of connectivity-building, the key ASEAN states have all pragmatically sought *to diversify their partnerships as inclusively as possible*, avoiding putting all their eggs in one basket. Inclusive diversification complements the intended goals of active neutrality, i.e., mitigating the risks of entrapment and alienation, minimizing the dangers of dependency, and potential technological vulnerabilities, while maximizing autonomy, bargaining capacity, and developmental opportunities, thereby boosting the elites' internal legitimation.

The inclusive diversification approach is evidenced in Singapore, Southeast Asia's technology leader. Even though the city-state did not include Chinese tech firms in its two primary 5G networks, the IMDA, Singapore's sector regulator, made it a point to include Huawei as a partnering vendor in the smaller 5G network run by TPG Telecom. Significantly, there are also other nuanced, selective arrangements in Singapore's major 5G networks: while the StarHub-M1 consortium has selected Nokia to supply the core components of its network, StarHub is also exploring using both Nokia *and* Chinese firms (Huawei and ZTE) for non-core elements of the 5G networks, while M1 is reviewing Ericsson, Nokia and Huawei. Muhammad Faizal Abdul Rahman, a research fellow based at Singapore's RSIS, points out that such arrangements are indicative of Singapore "vendor diversify", a form of "risk management", aimed at minimizing "cybersecurity risks that could arise from over-reliance on a single supplier." (Rahman 2020)

[2] 5G infrastructure raises concerns over national security and cyber-surveillance because its architecture uses technologies that allow providers "to access and analyse the chain of networks from users to data storages." See Martinus, Melinda. "The Intricacies of 5G Development in Southeast Asia." *ISEAS Perspective*, no. 130 (2020): 1–9.

- **Fallback cultivation:**

The ASEAN states' impartial and inclusive approaches have been pursued side-by-side with efforts to cultivate independent "fallback" options. Fallback is defined here as backup plans or safety measures aimed at addressing potential challenges or losses that might arise in undesired but possible scenarios (e.g., in the event the present arrangement falters or the primary option fails). Under uncertainties, states—like other rational actors—are inclined to possess and develop as many fallback options as possible (Khong 2004). The imperatives of coping with uncertainties *and* hedging against the associated risks tend to push states to pursue one or more of the following: (a) developing contingency options (the just-in-case "plans B") to minimize possible losses in case any unexpected scenario occurs; (b) enhancing domestic capacity (including technological capability); and (c) adopting multiple mutually-counteracting measures (e.g., simultaneously enhancing relations with the competing powers; concurrently displaying selective defiance and selective deference toward both powers) for offsetting multiple risks and keeping options open.

Southeast Asia's fallback-cultivation efforts on 5G technology is perhaps best illustrated by Singapore's "vendor diversify" strategy, a contingency plan aimed at addressing possible risks. As observed by RSIS's Muhammad Faizal, Singapore's decision to have its telcos M1 and StarHub allow Huawei provide non-core elements of the 5G networks, in addition to Singapore's main networks involving Ericsson and Nokia, is "a strategic step" to pre-empt "plausible supply chain disruptions to national infrastructure if the United States is effective in severing Huawei's global access to semiconductors." (Rahman 2020)

While other ASEAN states have displayed a similar tendency to cultivate fallback options, they have done so in a *much lighter and more limited* manner. These states, as light hedgers, hold a more sanguine outlook of economy-security trade-offs: prioritizing concrete economic benefits, avoiding over-emphasize security risks, and preferring to maximize long-term maneuverability by cultivating and keeping as many options open as possible. Malaysia is a case in point. In 2021, Malaysia under the Muhyiddin Yassin government decided to go with the single wholesale network (SWN) route to develop its 5G network, entrusting the state-owned Digital Nasional Bhd (DNB, owned by Ministry of Finance) as the network owner, while awarding Ericsson a contract to design and build its 5G telecommunications network. In 2023, Malaysia's Anwar Ibrahim government (November 2022-present) announced the transition of the 5G implementation model from the SWN to "a dual network" with such justifications as, increasing competition, ending the current 5G monopoly, and reducing the financial implication for the government on a large scale (Bernama 2023; Carrozza and Bruni 2023). Other light hedgers like Cambodia and Laos, due to their limited internal capabilities and limited external alternatives, have focused more on enhancing their own domestic digital connectivity capacity than investing in contingency measures.

### *Why* Do States Make Different Economy-Security Tradeoffs?

While a state's insistence on fallback cultivation is driven more by the necessity to hedge against the risks of external uncertainty, the approaches it *chooses* (including the types of contingency options, the priorities of self-capacity enhancement, as well as the extent and manner of

counteractive actions) are motivated, shaped, and constrained more by its elite's *internal* legitimation needs. Specifically, the elite's varying pathways of legitimation lead to varying patterns of a state's riskification process, in turn leading to different choices of economy-security tradeoffs, and by extension, different degrees and approaches of hedging (including the manner of counteractive actions). Legitimation defines which types of returns *are prioritized* (based on political desirability) and which perceived risks *are taken more seriously than others* (based on political acceptability and unacceptability). This process, accordingly, determines the *range* and *ranking* of both prioritized returns and perceived risks, and ultimately, the trade-offs between them.

Vietnam and Singapore, the heavy hedgers, have opted to trade *some* levels of potential economic gains for security-maximization, primarily because the relative salience of *identity-based legitimation* pushes their respective elites to prudently prioritize policy independence, autonomy and maneuverability over commercial interests vis-à-vis the big powers, especially China. The two Southeast Asian states have thus declined or distanced themselves from collaborating with China on 5G, viewing such digital connectivity collaboration as risking their national security *and* regime authority.

In Vietnam, the ruling Communist Party of Vietnam (CPV) elites draw their political legitimacy not only from delivering economic growth (performance justification) and conforming to socialist ideological narratives (procedural justification), but also from projecting and mobilizing the party's image as the defender of Vietnamese sovereignty and territorial integrity (identity-based particularistic justification). The relative importance of such identity-based legitimation dictates that no Vietnamese leader can afford to play down China-related risks. This is especially so considering the Vietnamese people's enduring memory of thousands of years of Chinese domination, as well as growing anti-China sentiments, in the face of China's increasingly aggressive actions over the South China Sea.

In Singapore, the ruling People's Action Party (PAP) elites justify their right to rule by the party's ability to cope with the island state's inherent vulnerabilities (Leifer 2000; Acharya 2008). They derive their authority primarily by ensuring continuous economic growth (performance legitimation), alongside winning elections (procedural legitimation) and maintaining Singapore's identity as a multicultural society (particularistic legitimation). Singapore is a multi-ethnic country with 76 percent of its population ethnic Chinese, 15 percent ethnic Malays and 7.5 percent ethnic Indians. While China's rise as an economic powerhouse has been a boon to the PAP's performance legitimation, Beijing's increasing attempts to "influence", "manipulate" and "foist a Chinese identity on multiracial Singapore" are regarded by Singapore elites as "invidious and dangerous." (Kausikan 2023) The elites see China's "influence operations" as a profound political challenge and risk because it may threaten Singapore's "multiracial meritocracy" socio-political fabric. Such political concerns thus push the elites in Singapore, like their counterparts in Hanoi, to take China-related digital security and political risks seriously.

Hence, in Singapore and Vietnam, the elites' legitimation-driven priorities prompt ruling elites to be more vigilant than the elites of regional countries about the economy-security tradeoffs, viewing the prospect of partnering with Chinese tech firms on 5G as politically risky, undesirable, and even unacceptable. In both cases, *political* maximization requires *security* maximization. Such serious and stern *riskification* thus push Vietnam and Singapore to hedge against the perceived political and security risks more heavily by excluding Huawei from their 5G networks, investing more on self-capacity enhancement, and widening their diversification

efforts. Both governments choose to defy Beijing on 5G for their own interests, not about siding with Washington. Indeed, driven in large part by the needs to underscore their neutrality while pursuing inclusive diversification and keeping options open, both Vietnam and Singapore have sought to *counteract* their selective defiance by selective deference and pragmatic engagement. This is because defiance without deference invites suspicion, hostility and entrapment, while deference without defiance risks subservience and dependency. Both countries, hence, have simultaneously forged closer ties with China on different channels or platforms: the CPV continues to strength its party-to-party ties with the CPC, while Singapore has widened its economic and functional cooperation with China.

Singapore and Vietnam's heavy-hedging approaches on 5G technology are in stark contrast to other ASEAN states' light-hedging stance, which manifests in a persistent inclination to trade potential security risks for economic-maximization. Such a tradeoff is chiefly attributable to their respective elites' emphasis on different principal pathways of legitimation. From Indonesia to Malaysia, and from Thailand to Cambodia, the relative salience of *development-based legitimation* pushes their elites to prioritize concrete partnerships capable of boosting their growth prospect and bringing economic gains, over potential digital insecurity. For these countries, political maximization necessitates economic maximization. These states have thus engaged and even embraced China on 5G and DSR more broadly, viewing Chinese tech firms as opportunities to be leveraged (instead of dangers to be distanced from) for enhancing the governing elites' performance in delivering economic fruits, creating jobs, developing new growth engines, raising domestic technological capacity, and tackling cyber security issues.

This is not to say that these ASEAN states are not concerned about security risks. Rather, these countries, the light hedgers, are more inclined to *play down* longer-term security concerns, chiefly because the imperative of performance legitimation requires the elites to place greater attention to the *now-and-here* developmental gains. Besides, they can afford to play down the China-related digital security risks—as projected by some in the West—in part because these risks have remained *potential or possible* risks, rather than clear-and-present dangers. In the eyes of these states, China-related security harm may or may not take place in the future. Such *sanguine* riskification (as opposed to Vietnam and Singapore's serious and stern riskification, as discussed above) leads these ASEAN states to hedge more lightly. That is, while these states have similarly insisted on active neutrality and inclusive diversification (like the heavy hedgers), they have pursued a much lighter degree of fallback cultivation, i.e., fewer contingency options and counteractive measures (compared to Vietnam and Singapore's heavier investments on such options). The light hedgers are also less inclined to defy China and more inclined to display deference to their giant neighbor.

Of course, such sanguine riskification notwithstanding, there are variations among the light hedgers: Indonesia, Malaysia, and Thailand have been demonstrating a greater tendency and efficiency of diversification, contingency, and capacity enhancement efforts than Cambodia and Laos. These variations are a result of two factors: higher/lower level of internal resilience (including political systems, domestic technological base, resource endowment) and wide/limited range of external alternative partners.

## Conclusion

To conclude, the variations in the Southeast Asian approaches to economy-security tradeoffs are attributable to the ruling elites' legitimation-driven calculations of optimizing the prioritized benefits and perceived risks. Vietnam and Singapore both hedge heavily because the relative salience of identity-based legitimation in both countries prompt the respective elites to see more security risks than economic benefits from China-related digital connectivity. By contrast, the other ASEAN states can afford to adopt a light-hedging approach, primarily because their elites rely more heavily on development-based legitimation as the principal pathway of inner justification, which motivates them to prioritize economic benefits, play down the risks of digital insecurity and dependence but highlight the dangers of polarization, entrapment, and economic downturn. The lack of self-capabilities and external alternatives also play a role in some of the light hedgers' responses.

The preceding discussions have important policy implications. Instead of considering any of the big-power initiative from an either-or dichotomy, middle states often see a spectrum of policy options, prompting them to respond to the initiative in a selective, partial, and mixed manner based on elite domestic needs. Regardless of their degrees of hedging and types of tradeoffs, ASEAN states' policy choices toward 5G digital connectivity are *not* about siding with or against any power, but about maximizing their own domestic political and development needs. Hedging is about *avoiding* a binary choice; it is about insistence on neutrality, diversification, and fallback cultivation. Technological neutrality is still feasible under the current circumstances in part because of the availability of alternative partners (primarily the European players), and in part because of some level of self-capacity development (in the cases of Vietnam and Singapore). Technological neutrality is desirable because of the high, unacceptable tradeoffs associated with the taking-sides approach.

## References


Acharya, Amitav. 2008. *Singapore's Foreign Policy: The Search for Regional Order*. Hackensack, NJ: Institute of Policy Studies/World Scientific.

*Bernama*. 2023. "PM Anwar: Transition to 5G Network Reduces Financial Implications for Govt." May 23. https://www.malaymail.com/news/malaysia/2023/05/23/pm-anwar-transition-to-5g-network-reduces-financial-implications-for-govt/70562

Carrozza, Ilaria, and Giacomo Bruni. 2023. "China's Digital Silk Road and Malaysia's Technological Neutrality." *The Diplomat*, August 22. https://thediplomat.com/2023/08/chinas-digital-silk-road-and-malaysias-technological-neutrality/.

Clapton, William. 2011. "Risk in International Relations." *International Relations* 25, no. 3: 280–95.

Corry, Olaf. 2012. "Securitisation and 'Riskification': Second-Order Security and the Politics of Climate Change." Millennium: *Journal of International Studies* 40, no. 2: 235–58.

Haacke, Jürgen. 2019. “The Concept of Hedging and Its Application to Southeast Asia: A Critique and a Proposal for a Modified Conceptual and Methodological Framework.” *International Relations of the Asia-Pacific* 19, no. 3: 375–417.

Haacke, Jürgen, and John Ciorciari. 2022. “Hedging as Risk Management: Insights from Works on Alignment, Riskification, and Strategy.” IPC Working Paper Series Number 124, 2–44.

Heng, Yee-Kuang. 2022. “Japan in the Gulf: Hedging between Washington and Tehran?” *The International Spectator* 57, no. 4: 20–34.

Kausikan, Bilahari. 2023. *Singapore Is Still Not an Island: More Views on Singapore Foreign Policy*. Singapore: Straits Times Press.

Khong, Yuen Foong. 2004. “Coping with Strategic Uncertainty: The Role of Institutions and Soft Balancing in Southeast Asia’s Post-Cold War Strategy.” In *Rethinking Security in East Asia: Identity, Power, and Efficiency*, edited by J. J. Suh, Peter J. Katzenstein, and Allen Carlson, 172–208. California: Stanford University Press.

Kuik, Cheng-Chwee. 2008. “The Essence of Hedging: Malaysia and Singapore’s Response to a Rising China.” *Contemporary Southeast Asia* 30, no. 2: 159–85.

_____. 2016. “How Do Weaker States Hedge? Unpacking ASEAN States’ Alignment Behavior towards China.” *Journal of Contemporary China* 25, no. 100: 500–14.

_____. 2022. “Shades of Grey: Riskification and Hedging in the Indo-Pacific.” *The Pacific Review*: 1–34.

Kuik, Cheng-Chwee, and Chen-Dong Tso. 2022. “Hedging in Non-Traditional Security: The Case of Vietnam’s Disaster Response Cooperation.” *The Chinese Journal of International Politics* 15, no. 4: 422–42.

Leifer, Michael. 2000. *Singapore’s Foreign Policy: Coping with Vulnerability*. Politics in Asia. New York: Routledge.

Lim, Darren, and Zack Cooper. 2015. “Reassessing Hedging: The Logic of Alignment in East Asia.” *Security Studies* 24, no. 4: 696–727.

Rahman, Muhammad Faizal Abdul. 2020. “Singapore Decides on 5G Networks: Is Huawei Banned?” *The Diplomat*, July 2. https://thediplomat.com/2020/07/singapore-decides-on-5g-networks-is-huawei-banned/.

Skinner, Wickham. 1969. “Manufacturing-Missing Link in Corporate Strategy.” *Harvard Business Review* 47, no. 3: 136–45.

Tetlock, Philip E., Orie V. Kristel, S. Beth Elson, Melanie C. Green, and Jennifer S. Lerner. 2000. “The Psychology of the Unthinkable: Taboo Trade-Offs, Forbidden Base Rates, and Heretical Counterfactuals.” Journal of Personality and Social Psychology 78, no. 5: 853–70.

Winter, Harold. 2013. *Trade-Offs: An Introduction to Economic Reasoning and Social Issues*. 2nd ed. Chicago, Ill.: University of Chicago Press.

# High Technology and the Evolution of South Korea's Economic Security Strategy

Seungjoo Lee

## Introduction

This paper aims to explain the origins and evolution of South Korea's economic security strategy. The origins of South Korea's economic security strategy can be traced back to its industrialization strategy in the 1960s. In implementing its industrialization strategy, South Korea as a late developer pursued the geoeconomic goal of catching up to the advanced countries. South Korea simultaneously sought the geopolitical goal of responding to growing security threats. Compared to the traditional one, South Korea's economic security strategy in the 21st century displays continuity and change in terms of its geopolitical and geoeconomic nature. The U.S.-China strategic competition has been a decisive trigger for the change in South Korea's economic security strategy. In the course of the strategic competition, the United States and China quickly broadened the scope of competition from trade to advanced technology. Recognizing the potential as the nexus between economy and security, South Korea established and promoted an economic security strategy utilizing high technology. First, South Korea actively explored the possibility of utilizing high technology as a means to counter economic coercion. Second, South Korea has focused on mitigating structural vulnerabilities in order to increase the utility of advanced technology as a tool in its economic security strategy. Third, South Korea has also utilized its technological capabilities to induce international cooperation.

## The Emergence of Traditional Economic Security Strategy in Korea

South Korea's economic security strategy has gone through several phases of transformation. The primary nature of the traditional South Korea' economic security strategy was its strong mercantilist traits. South Korea relied on the United States for aid and a security umbrella in the cold war period. The industrialization strategy that began in 1962 with export-oriented industrialization (EOI) can be considered the origins of South Korea's economic security strategy. South Korea, as a late developer, pursued a catch-up strategy to adopt export-oriented industrialization as a means to achieve it. On the surface, it was liberal in the sense that it sought to integrate into the global economy by fostering export industries. However, it was mercantilist in that it demonstrated the explicit goal of catching up. The completion of industrialization through catch-up was a survival strategy in response to geoeconomic challenges, and thus the genesis of South Korea's economic security strategy.

Since the late 1960s, South Korea has attempted to upgrade its industrial structure through heavy chemical industrialization (HCI) drive, industrial policy became the central feature of its economic security strategy. It was an industrialization strategy that sought to upgrade from labor-intensive industries to capital- or technology-intensive industries. The geoeconomic challenge of keeping up with the advanced countries and fencing off the late-late developers was a key theme in South Korea's economic and security strategy during this period. The economic

security strategy with industrial policy at the core was established and implemented as a response to geoeconomic challenges.

Meanwhile, the HCI drive was also an industrial policy response to geopolitical challenges. The pursuit of heavy chemical industrialization was an economic security strategy in response to geopolitical challenges in that it aimed to strengthen industrial capabilities in order to strengthen military capabilities to counter the North Korean security threat. In other words, it was an industrial policy response to the geopolitical challenge of the North Korean security threat by focusing on the development of defense industries or industries that directly or indirectly help to build up defense capabilities. In particular, the development of the defense industry was not only a response to the geopolitical challenge, but also implied a geoeconomic response of upgrading the industrial structure, as industrial policy occupied a key position in South Korea's economic and security strategy.

## High Technology as a Nexus between the Economy and Security

### *U.S.-China Strategic Competition and High Technology*

The fact that the U.S. and China have expanded the front from a trade war to a technology competition underscores the long-term and structural nature of the U.S.-China conflict. The escalation of U.S.-China competition has led to the emergence of linkages between the economy and security. The modes of economic-security linkages can be categorized into "tactical linkages," which utilize asymmetries in national power, and "substantive linkages," which are based on a cognitive consensus on the creation of functional synergies when two or more issues are linked (Aggarwal 2013). Recognizing that technological competition is embedded in strategic competition, the U.S. and China simultaneously employ a very wide range of instruments in technology competition, from protectionism and export controls to industrial policy and innovation capacity building.

High technology is the nexus between the economy and security, not only because it is key to securing future competitive advantage, but also because it affects the ability of the defense industry to innovate. Because advanced technologies have such a significant impact on the security as well as the competitiveness of key industries in the future, the United States and China have tended to consider both economics and security as an integral part of their technological competition, rather than as an either/or proposition (Navarro 2018). 21st century high technologies have the potential for dual use, which further emphasizes the role of the economic-security nexus.

China is faced with the need to cultivate its own high-tech capabilities in order to gain an advantage in strategic competition. This is why the Chinese government has prioritized the development of domestic self-sufficiency in high-tech capabilities by promoting the Made in China 2025. Furthermore, the Chinese government actively promotes military-civilian convergence as a means to create a virtuous cycle of exchange and cooperation between the military and civilian sectors in order to strengthen indigenous innovation capabilities (Laskai 2018). Civil-military fusion is an integrated national strategy in China that aims to integrate the innovation capabilities of the military and civilian sectors so that military technologies can spin

off commercial technology and, conversely, commercial technologies can be spun on to enhance military capabilities.

The high-tech as a nexus between the economy and security helps us understand the domestic political origins of the strategic competition. The Biden administration is pursuing a "small yard, high fence" strategy, moving away from the all-encompassing pressure of the Trump administration. The Trump administration expanded the scope of sanctions, putting pressure on China from all sides. However, in the face of criticism that these measures are "self-defeating" and undermine the interests of U.S. companies, the Biden administration was forced to approve temporary export licenses, demonstrating that the all-out offensive has shown limited success in achieving the desired outcomes. The Biden administration has shifted to a strategy of targeting sanctions to increase their effectiveness while minimizing harm to U.S. businesses.

Recognizing the importance of high-tech as a nexus between the economy and security, the U.S. has expanded its entity list to include not only Huawei and ZTE, but also SMIC and DJI, in response to China's pursuit of civil-military fusion, which tightly combines civilian and military innovation capabilities. The Trump administration's perception that "economic security is national security" is reflected in the technology competition (The White House 2017). The Biden administration has also recognized that technological competition affects not only future industrial competitiveness, but also national security as the potential for dual-use technologies increases. The Biden administration has further expanded the scope of export controls and restrictions on China, while expanding and strengthening international cooperation with allies and partners.

In addition, economic security strategies in the 21st century are shifting from a narrowly defined geoeconomic response to a more comprehensive approach, as they also encompass responses to geopolitical challenges. Economic security strategies based on strategic ambiguity focused primarily on responding to geoeconomic challenges. As U.S.-China strategic competition has intensified, the difficulty of maintaining a separate economic and security approach between the United States and China has been highlighted. The U.S.-China strategic competition, which began with a trade war in 2018, quickly expanded to include high technology and key industries. In the process, the United States sought to strengthen cooperation with allies and partners to increase the effectiveness of its deterrence against China, while China responded by attempting to isolate weak links in the U.S.-led cooperation network. South Korea faced a double-edged challenge: the pressure of U.S. policy alignment and the growing risk of economic coercion from China (Suri and Sharma 2023).

The experience of South Korean semiconductor companies such as Samsung Electronics and SK Hynix illustrates this dilemma. The Biden administration has used subsidies to semiconductor companies under the CHIPS and Science Acts as a means to realize its goals of expanding domestic semiconductor manufacturing capacity and slowing Chinese technological innovation. Samsung Electronics has announced a $17 billion investment in Arizona, and SK Hynix has committed to building a semiconductor post-processing facility in the United States. Meanwhile, the U.S. government's provision of subsidies could limit the ability of Samsung and SK Hynix, which already have advanced semiconductor production facilities in China, to expand production. In October 2022, the Biden administration capped the expansion of advanced semiconductor production facilities in China for semiconductor companies receiving U.S.

government subsidies at no more than 5% per year. The example of the semiconductor industry has spurred a shift in economic security strategy.

The limits of the geoeconomic response were also evident in U.S.-China relations. South Korea, which had prioritized expanding its economic ties with China, found itself at odds with Beijing as it sought means to counter the North Korean nuclear threat. When the Park Geun-hye administration decided to deploy THAAD in 2016, bilateral ties, which had just reached a peak, cooled off immediately. Furthermore, the Chinese government banned group tourism to South Korea and implemented de facto economic coercion against the cosmetics, entertainment, and wholesale and retail industries. The economic damage was estimated at 0.5% of South Korea's GDP. The limits of the strategic approach of strengthening security cooperation with the United States and expanding economic ties with China were exposed. This highlighted South Korea needs to incorporate the dual challenges of geopolitics and geoeconomics into its economic security strategy.

## High Technology and South Korea's Economic Security Strategy

### *Counter-Economic Coercive Measures*

South Korea is stepping up efforts to mitigate structural vulnerabilities. It is a proactive response to economic coercion as it remedies the limitations of a reactive strategy. Mitigating vulnerabilities works on two levels. First, South Korea has sought to reduce economic dependence on China. South Korea capitalized on China's economic rise after the 2008 global financial crisis, resulting in a rapid expansion of bilateral trade. The problem, however, is that the bilateral trade relationship is the epitome of asymmetric interdependence, which is the root cause of China's ability to exert economic coercion on South Korea.

Second, South Korea has made a concerted effort to mitigate structural vulnerabilities in its supply chain. South Korea is not the only country to have experienced supply chain disruptions during the US-China strategic competition and the global spread of COVID-19. However, South Korea's expanding economic ties with China since the 2000s have led to the formation of a division of labor between the two countries. It facilitated South Korea has become increasingly dependent on China in upstream of the value chain. According to a supply chain vulnerability analysis conducted by the South Korean government, there are over 600 highly vulnerable items in materials, parts, and equipment, many of which are concentrated in China. The Korean government proposed policies to mitigate structural vulnerabilities in materials, parts, and equipment, not only to prevent another supply chain disruption, but also to respond to economic coercion.

Third, intensifying technology competition between the US and China provided an opportunity for Korea to more actively respond to China's economic coercion by using high technology. As the US high-tech checks on China have strengthened, China's dependence on high-tech cooperation with Korea has increased. Korea has also come to recognize that China's economic coercion has focused on tourism, entertainment, and services and that it could expand its strategic space to respond to China by utilizing high technology.

*Strengthening Tech Sovereignty*

The Korean government highlighted that the triple crisis – the U.S.-China trade war in 2018, Japan's export restrictions in 2019, and supply chain disruption due to the global spread of COVID-19 in 2021 – enormously increased uncertainty in the supply and demand of materials, parts, and equipment in Korea. Defining materials, parts, and equipment as "invisible technology," the Korean government's strategy developed in two directions. First, the Korean government noted that other countries competitively pursue technological innovation as demonstrated in "Manufacturing USA (the US)," "Industry 4.0 (Germany)," and Connected Industries (Japan)." The Korean government realized that it is inevitable to foster a strong manufacturing industry. The Korean government highlighted it is of paramount importance to improve the quality of materials, parts, and equipment to secure the competitiveness of future industries.

Second, with the Japanese government's decision to drop Korea from the white list in August 2019, Korea immediately embarked on drafting a strategy to strengthen its competitiveness. In 2020, the Korean government announced the third strategy "Materials/Parts/Equipment 2.0 Strategies for a Leap Forward in High-Tech Industrial Factories" (Relevant Ministries 2020). The Korean government adopted three policy measures in response to Japan's control of three major items – hydrogen fluoride, extreme ultraviolet lithography (EUV), and fluorinated polyimide: (1) increasing domestic production, (2) attracting foreign investment, and (3) diversification to China.

The Korean government's pursuit of technological sovereignty is not limited to reducing damage from Japan. The Korean government designated 100 key strategic items that are deemed essential to high-technology industries. To compile the list of strategic items, the Korean government went through a comprehensive analysis. Out of 4,708 materials, parts, and equipment that were subject to the first-round review, the Korean government conducted the supply chain analysis on 1,194 items of materials, parts, and equipment imported from Japan. For this, the Korean government examined a variety of factors such as the impact of supply chain instability on national security, substitutability, technological level, dependence on a specific country, and linkage with major and next-generation industries (Ministry of Science and ICT 2021). Based on the analysis, the Korean government ultimately came up with a list of items that are eligible for government support.

*Securing the industrial policy-technology innovation nexus*

The 21$^{st}$ century economic security strategy differs from traditional industrial policy in that it explicitly sets out the nature of the challenge or the opponent of competition and seeks specific responses to it. South Korea's economic security strategy in the 21$^{st}$ century showcases the dual nature of continuity and change. While South Korea still relies on an industrial policy in terms of responding to the dual challenges of geopolitics and geoeconomics. Traditional industrial policy possessed the nature of an economic security strategy in that it aimed to protect and nurture domestic industries. Although traditional industrial policy set a mercantilist goal of catching up, the target of catching up was unclear and it did not give high priority to identifying the nature of the challenge. In contrast, the economic coercion of China and Japan, the

nationalism of major countries to strengthen their domestic production capabilities in key high-tech industries such as semiconductors and batteries, and the protectionism that has spread globally in the course of the COVID-19 pandemic emerged as challenges the Korean government should deal with in the 21st century.

Based on the identification of the nature of the challenge, South Korea pursued industrial policies to strengthen supply chain resilience, diversify, and build ecosystems for key high-tech industries. The utilization of advanced technologies is a key element of South Korea's economic and security strategy, as continuously enhancing its technological innovation capabilities not only strengthens international cooperation but also contributes to proactively preparing for uncertainties such as the US-China strategic competition. Again, the geoeconomic nature in South Korea's economic security strategy can be found in an increased reliance on policy measures to strengthen industrial competitiveness and technological innovation capabilities. Integrating technology-industry nexus into the economic security strategy is a priority for the realization of geopolitical goals. The importance of government policies focused on countering competitors at the forefront of high technology becomes even more important. Moving away from an industrial policy that focuses on strengthening industrial competitiveness in a narrow sense and pursuing a strategy that focuses on strengthening technological innovation capabilities and the industrial policy-technology innovation nexus is also a feature of the new economic security strategy. In particular, unlike other countries that tend to focus on strengthening stability and resilience, South Korea's economic security strategy focuses on strengthening the high-tech-industrial nexus, which links high-tech innovation capabilities and industrial competitiveness.

This complements the limitations of reactive economic and security strategies. The importance of strengthening high-tech capabilities in South Korea's economic security strategy is exemplified by the Korean government's decision to select 12 key national strategic technologies for 2021 and provide intensive support. The Korean government recognized that strengthening technological sovereignty is not only a response to high-tech competition, but also a leverage for cooperation with other countries. As the case of semiconductors and batteries illustrates, South Korea's positioning as a country with high-tech innovation and manufacturing capabilities has led to an influx of requests for cooperation from many countries.

*High Technology as a Leverage for International Cooperation*

State-of-the-art technology serves as the nexus of economic and security linkage. The linkage between economy and security without a nexus is likely to turn into a tactical linkage that attempts to secure an edge in negotiations or coerce the target state. Against this backdrop, Korea has explored economic security strategy that takes advantage of its key position in the supply chain of high-tech industries such as semiconductors, batteries, and electric vehicles. Korea's new economic security strategy focused on leveraging its key position in the high-tech supply chain, which aimed to enhance its strategic value, especially in the US-China technology competition.

The Biden administration has actively promoted reshoring to alleviate supply chain vulnerabilities. It also fosters high-tech cooperation with allies and partners — a policy from which Korea has emerged as a key player. While Korea has been active in expanding and deepening the relationship with the Biden administration, which emphasizes extensive international cooperation, but concerns over the US mercantilist approach have not been removed. Resonating with the Biden

administration's reshoring, Korean companies such as Samsung Electronics, SK Hynix, and Hyundai Auto announced large-scale investments in the US.

## References


Aggarwal, Vinod K. 2013. "U.S. Free Trade Agreements and Linkages." *International Negotiations* 18.

Laskai, Lorand. 2018. "Civil-Military Fusion and the PLA's Pursuit of Dominance in Emerging Technologies," *China Brief* 18-6.

Ministry of Science and ICT (Korea). 2021. "Press Release: In the era of global competition for technological supremacy, national capabilities should be concentrated to secure technological sovereignty." December 22.

Navarro, Peter. 2018. "Economic Security as National Security: A Discussion with Dr. Peter Navarro." November 13.

Relevant Ministries. 2020. Materials/Parts/Equipment 2.0 Strategies to leap forward as a global factory in the high-tech industry - Preemptive future response GVC innovation measures.

The White House. 2017. "National Security Strategy of the United States of America." December 18.

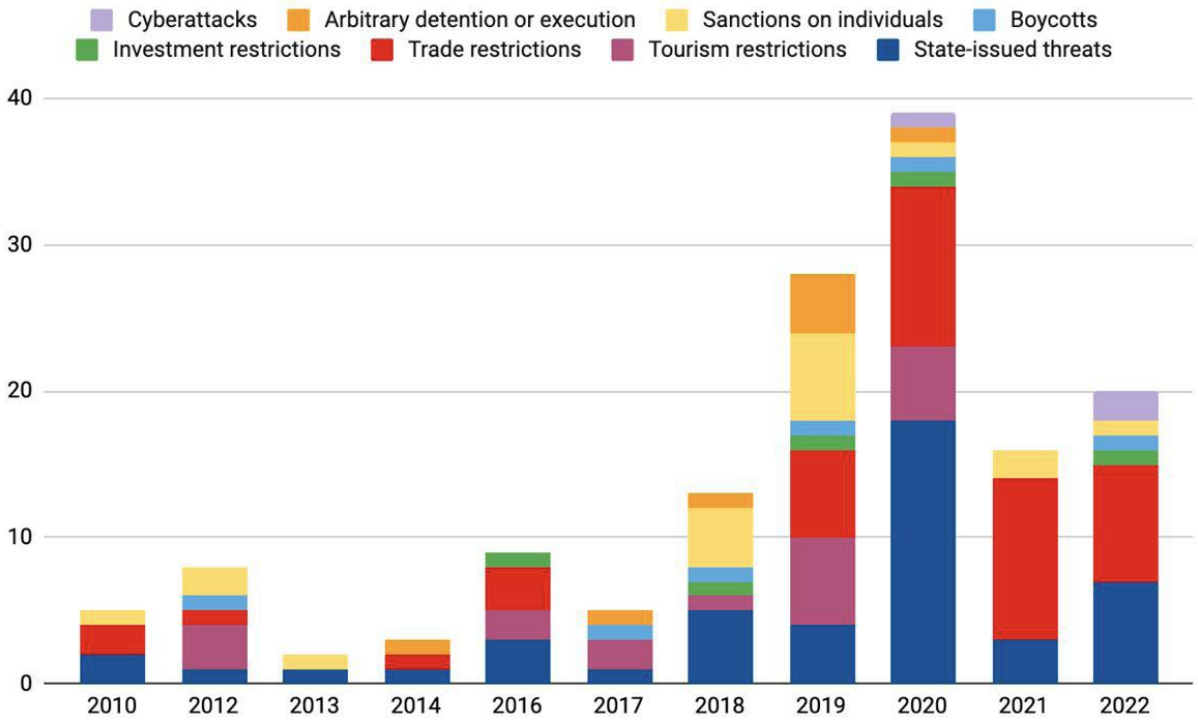
# South Korea's Experiences of Different Economic Coercions from China and Japan and Lessons for Countering Economic Coercion

Yongshin Kim

## I. Introduction

During the Cold War era, China was the recipient of economic sanctions by Western countries. However, as its economic interdependence with the rest of the world deepens, China begins to use economic coercion more frequently to achieve its political and diplomatic goals. China claims it is the biggest trading partner of more than 130 countries and regions, as of 2019, more countries with it than with the U.S. Many studies have come to similar conclusions about when Beijing started to employ economic measures and how often. For example, MERICS identified 123 coercive cases between 2010 and 2022, with a marked increase since Xi's third term. Figure 1, presented by ASPI (Australian Strategic Policy Institute, 2023), shows a similar pattern. (Hunter, Impiombato, Lau, Triggs, Zhang and Deb, 2023)(方炯升 2020) While there are differences in identifying China's economic coercion, Chinese scholars also show an increase in China's economic sanctions since 2010.

**Figure 1. Growing use of coercion—cases of PRC coercion against foreign states, 2010 to 2022**




China's economic coercion does not just affect China and its target countries. China's growing economic coercion has created a vicious spiral spreading globally. Watching Japan, which had experienced rare earth export controls from China, imposing export control on South Korea,

Trent (2019) pointed out that Japan and South Korea learned the wrong lessons from China. The diffusion of economic coercion to achieve political ends could eventually challenge the liberal international order. This study analyzed the case of South Korea, a country with a high level of economic interdependence and which has experienced economic coercions from China and Japan. Economic coercions from China and Japan vary significantly in terms of the form of coercion, the scope and strategic importance of the target industries, and the targeted companies. By analyzing how Seoul's responses to economic coercions from these two countries differed, this study seeks to understand what factors lead target countries by economic coercion to choose different countermeasures.

## II. Economic Coercion and South Korea's Countermeasures to Economic Coercions from China and Japan

While there is no shared definition of economic coercion, its primary characteristic is that it involves using economic means to achieve political goals. Economic means include exploiting economic vulnerabilities and dependencies through trade, investment, and foreign aid measures. While economic sanctions and economic coercion both use economic means for political purposes, economic coercion tends to be more informal and employs "gray zone" strategies. Economic coercion uses economic means to bring about meaningful change in the target country's policy decisions, but it does so implicitly, making it difficult to assess its efficiencies (Drezner 2003).

Target countries also develop countermeasures to coercive measures, Cha (2023) categorized into four categories. First, target countries started to prioritize economic security and developed capabilities to detect disruptions in advance. For example, the Korean government set up the early warning system, which covers nearly four thousand critical industrial materials. Furthermore, to strengthen the function of the control tower for economic security, the Office of the President created the position of secretary to the President for economic security. Second, to respond to disruption caused by economic coercion, target countries usually adopt trade diversification along with strengthening domestic capabilities if possible. When Japan was subjected to rare earth export controls from China in 2010, Japan reduced its dependence of critical minerals on China from 90 percent to 58 percent in a decade by expanding domestic seabed exploration. Third, target countries relocated their core sourcing and production chains away from direct China's influence through reshoring and friend-shoring. Finally, as a mitigation measures, target countries' governments tend to grant ad hoc trade support, monetary assistance, and investments funds to soothe shocks from economic coercion.

Of course, these fours are not exhaustive of what individual target countries are taking, but they do give a sense of the toolkits that respective countries have at their disposal. Among the toolkits possessed by individual countries, countries choose different tools depending on the situation. So why do target countries use different tools as a countermeasure to economic coercion? The answer to this can first be found in different conditions of economic coercion. Table 1 shows the economic coercion exerted by China and Japan on South Korea, categorized by four criteria.

**Table 1. Economic Coercions from China and Japan toward South Korea**

| | **Coercion from China (2016)** | **Coercion from Japan (2019)** |
|---|---|---|
| Formality | Informal | Formal<br>(Export control, exclusion from whitelist) |
| Scope of sanctions | Comprehensive (K-culture products, EV batteries, retail, tourism) | Small yard (fluorine polyamide, etching gas, photoresist) |
| Strategic importance of targeted industries | Low | High |
| Scope of targeted firms | - One firm (Lotte) in the retail industry<br>- Many small and medium enterprise in the tourism industries | The entire value chain of semiconductor and display sector |

Since the decision to deploy the terminal high-altitude area defense (THAAD) system in South Korea in 2016, China's escalating economic coercion in various ways has been characterized by the following. The most distinctive characteristic of China's economic coercion was informality. While informality is a key feature of economic coercion, China's economic coercion in 2016 was typically conducted "behind the curtains." The state rarely acknowledges the deployment of measures or the links between economic coercive measures and the country's perceived political interests. Second, as the THAAD deployment progressed, the scope of China's coercion also expanded in response, so the extent of economic coercion was very broad. The decision to deploy the THAAD in August 2016 led to the cancellation of K-culture artists' performances in China, and when the South Korean government did not reverse the decision, the coercive measures escalated to include charter flights, cruise ships, and the suspension of selling group tour packages. In addition, after Lotte agreed to provide its golf course as a base for the THAAD deployment, the company was forced to shut down its Lotte Marts and Lotte Department Stores in China, citing domestic regulations. Third, despite the wide range of industries exposed to Chinese economic coercion, the strategic value of individual industries was relatively low. Finally, because the sectors targeted by economic coercion were so comprehensive, the firms targeted by coercion were also very different in each sector. For example, Lotte, the most affected company, was not sanctioned in other sectors such as chemicals but suffered tremendous damage in the retail sector such as supermarkets and department stores. In contrast, in the tourism sector, which was highly dependent on Chinese tourists, many small and medium enterprises (SMEs), rather than just one big conglomerate, suffered damage.

Japan's economic coercion in 2019 refers to a series of economic sanctions implemented following the South Korean Supreme Court's decision to award compensation in the Nippon Steel forced labor lawsuit and order to seize and sell the company's assets. First, on July 4, 2019, Japan switched from comprehensive licenses to individual licenses for exports of hydrogen

fluoride, polyimide fluoride, and photoresist to South Korea. Second, on August 28, 2019, Japan excluded South Korea from its list of trusted whitelists (27 countries) of export destinations. First, Japan's actions consisted primarily of formal rather than informal measures in the form of coercion. While the Japanese government denies any link between the sanctions and political objectives, the economic coercion was more formal than informal. Second, the items affected by the sanctions are also kept in small yards, rather than comprehensive. Despite the significant impact of the three materials on the South Korean semiconductor and display industries, very few items were directly sanctioned. Third, however, the industries targeted by the sanctions were highly strategic in nature. As of 2019, when Japan's economic sanctions were in place, semiconductors accounted for 17.5% of South Korea's major exports, while displays accounted for 3.6%. Given the highly export-dependent nature of South Korea's economy, semiconductors and displays, which are among the top export items, naturally have a high strategic value. Finally, while the number of items sanctioned by Japan is very small, the value chain of the affected industries is extensive. This could have had a devastating impact on the operations of not only large conglomerates like Samsung and SK Hynix, but also many SMEs from both upstream and downstream.

## III. South Korea's Countermeasures to Economic Coercions from China and Japan

### 1) THADD Case

Despite the enormous impact of China's economic coercion on the South Korean economy following the THAAD deployment, the South Korean government has only used mitigation measures to reduce the impact on tourism workers. Local governments have also pledged administrative support, as tourism significantly contributes to the national economy and has a more immediate effect on local economic conditions than the central government. However, because the industry itself is not strategically important, it was difficult for the central government to provide immediate support. In the case of Lotte, which operates a retail chain in China, unlike the tourism industry, it wasn't easy to compensate a single company because it was the primary target. The central government did not explicitly announce any compensation for Lotte, perhaps out of concern that explicitly compensating a single company would escalate Chinese pressure. Even the South Korean media asked, "What did the state do for the companies?" in response to the $2 trillion in damage to South Korean companies.

After the THAAD incident, China's economic coercion had a huge economic impact on Korea. A loss of GDP caused by the THADD was estimated at about 0.5% of nominal GDP. Despite the huge economic impact, the effects of economic coercion are multifaceted. In the short term, China's economic coercion did not reverse the deployment of THAAD. However, to assuage Beijing's concerns, the Moon Jae In administration did issue a three-no declaration: no additional U.S. missile deployments, no participation on the missile defense (MD) system, and no participating in the South Korea-U.S.-Japan military alliance. Additionally, in the long term, we can see that South Korea made significantly different judgments on key issues with the U.S. than other allies. In the end, China's economic coercion measures had an impact on creating strategic ambiguity as the basis of Korea's China policy.

**Table 2. Allied Positions on Key Issues**

| | Australia | France | Germany | Italy | Japan | Poland | South Korea | U.K. | U.S. |
|---|---|---|---|---|---|---|---|---|---|
| Hong Kong: Signed statement to U.N. opposing Hong Kong National Security Law? | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| Xinjiang: Signed statement to U.N. opposing China's policies? | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| 5G: New restrictions on vendors? | Yes* | Yes† | Yes‡ | Yes§ | Yes** | Yes†† | No | Yes | Yes |
| South China Sea: Refuted legality of China's nine-dash line claim? | Yes | Yes | Yes | No | Yes | No | No | Yes | Yes |
| Belt and Road Initiative agreement? | No | No | No | Yes | No | Yes | No | No | No |
| Chinese Investments: Established new foreign investment screening rules? | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Taiwan: Support for Taiwan's participation in the WHO? | Yes | No | Yes | No | Yes | No | No | No | Yes |

* In order to protect critical infrastructure, Australia has banned Huawei from providing 5G equipment.
† New restrictions in France amount to a de facto ban on Huawei within the next eight years: telecoms operators who have purchased 5G equipment from Huawei will be prevented from renewing their licences after the equipment expires, causing a phase-out.
‡ The German government has tightened scrutiny over equipment vendors but has not formally banned Huawei from its 5G networks.
§ Huawei is working with Telecom Italia despite having been excluded from a tender to supply 5G technology.
** While Japan has not explicitly banned Huawei from its networks, the company is effectively excluded from public procurement.
†† South Korea is using Huawei and has called restrictions on semiconductor sales to Huawei and other Chinese companies "unacceptable."

*Sources: Available from authors upon request*

BROOKINGS

Source: https://www.brookings.edu/articles/retooling-americas-alliances-to-manage-the-china-challenge/

**2) Economic Coercion from Japan in 2019**

In response to Japan's economic pressure, the Korean central government has been actively supporting the localization of three key semiconductor and display materials as well as investment and supply chain diversification since July 2019. In addition, by announcing the "Measures to Strengthen Competitiveness of Materials, Parts, and Equipment," the government has prepared special measures to invest national resources and capabilities fully in the materials, parts, and equipment industry. Using budget, finance, taxation, and regulatory incentives, the measure aims to resolve the high dependence on Japan, ultimately turning them into opportunities for Korean manufacturing to innovate and leap forward. Compared to the THAAD situation, the Korean government's intervention was very immediate and extensive. The target of Japan's sanctions is official and clear, and the damage to the semiconductor and display industries is too obvious. In addition, the strategic position of the semiconductor and display industry is also very important.

Japan's economic coercion has not solved the short-term goal of reversing the South Korean Supreme Court's decision. However, since South Korea's new president took office, the country has been actively working on new ways to resolve the issue, such as "third-party reparations," to improve bilateral relations. South Korea's reliance on Japan for materials, parts,

and equipment has also declined. The share of imports of Japanese materials and parts peaked at 28.0% in 2003 and gradually declined to 18.2% in 2014. Since then, it has hovered around 17% and dropped to 15.9% in 2019. On the other hand, the share of imports from Taiwan increased from 8.3% last year to 9.3% this year, and the share of imports from China increased from 29.1% to 30.1%.

## VI. Conclusions

This study shows how difficult it is for economic coercion to achieve its targeted political goals despite the different conditions of economic coercion through the cases of China's economic coercion against Korea in 2016 and Japan's economic coercion against Korea in 2019. This paper first provides a comparative analysis of the two cases, focusing on the form of economic coercion, scope of sanctions, strategic importance of targeted industries, and scope of targeted firms.

These two cases illustrate how one country, South Korea, can react differently when faced with extremely different conditions across these four variables. In the case of THAAD, which was an informal, carpet-bombing style coercion against an industry that was not of high strategic importance, the government intervened by supporting small and medium-sized enterprises affected by the sanctions rather than responding immediately. However, China's economic coercion was large enough to cause a loss of 0.5% of Korea's GDP. It affected a wide range of sectors, including the performing arts, EV batteries, tourism, and retail, so it was perceived as bullying beyond its original political objectives. Ultimately, it failed to change the target country's behavior and left deep scars in the bilateral relationship that are difficult to repair.

Japan's economic coercion, on the other hand, had a clear official means of coercion and a limited scope. Tokyo effectively chose three materials that selectively hit industries of strategic importance to South Korea without significantly impacting the Japanese economy. However, for South Korea, the strategic importance of the affected industries and the clear direction and scope of the attack made it easier to centralize its response. As a result, Japan failed to achieve its initially intended short-term goal of influencing the Korean Supreme Court ruling, but it resulted in Japan's demands being actively reflected when Korea's Yoon Seok-yeol government came into power.

The above two cases give the following two implications. First, as seen in the two cases of economic coercion from China and Japan, it is not easy to achieve the political purpose of economic coercion in the short term. In situations of economic coercion, the target country tends to prepare countermeasures appropriate to the situation and is not willing to easily compromise with the political demands of the coercer country. Ultimately, considering the difficulties in discussing building collective resilience based on deterrence by punishment amid various discussions on China's economic coercion, an approach based on deterrence by denial also needs to be actively considered. Ultimately, given the difficulties of building collective resilience based on deterrence by punishment, an approach based on deterrence by denial should also be actively considered. According to Reynolds and Goodman (2023), "Deterrence by denial aims to prevent an adversary from taking an unwanted action not through fear of punishment but rather through fear of failure." Hence, making public China's economic coercion has a poor track record of succeed and maximizing reputational and economic costs of maneuvering economic coercion is not perfect, but a low-cost deterrence strategy.

Second, in the long run, policy change in the target country is only possible through the operation of internal interest groups. The Hirschmanesque logic that increased economic interdependence can create new interest groups in the other country that can exert political pressure on the government is equally applicable to the situation of weaponization of economic interdependence. (Kirshner 2008) From a long-term perspective, it is advantageous for economic coercion to be targeted rather than carpet-bombed to expect interest groups to play a role in the target country. After all, in order to win the hearts and minds of interest groups in a target country, disciplined, formalized, and precise coercion can have some effect in the long run.

**References**


方炯升. 2020. “有限的回击: 2010 年以来中国的经济制裁行为.” *外交评论: 外交学院学报* 37(1):65-87.

Cha, Victor D. 2023. “Collective Resilience: Deterring China’s Weaponization of Economic Interdependence.” *International Security* 48(1):91-124.

Drezner, Daniel W. 2003. “The hidden hand of economic coercion.” *International Organization* 57(3):643-59.

Hunter, Fergus, Daria Impiombato, Yvonne Lau, Adam Triggs, Albert Zhang, and Urmika Deb. 2023. “Countering China’s coercive diplomacy.” International Cyber Policy Centre, ASPI, Canberra.

Lim, Darren J, and Victor A Ferguson. 2022. “Informal economic sanctions: the political economy of Chinese coercion during the THAAD dispute.” *Review of International Political Economy* 29(5):1525-48.

Reynolds, Matthew, and Matthew P Goodman. 2023. “Deny, Deflect, Deter: Countering China’s Economic Coercion.” Center for Strategic and International Studies (CSIS) March:1-110.

Trent, Mercedes. 2019. “Japan and South Korea are Learning the Wrong Lessons from China.” *The Diplomat*.

# Memo

# Memo

# Memo

# Memo


East Asia Institute (EAI) is a non-profit, independent, private think tank founded in 2002 with the mission of seeking to establish a regional community based on democracy and a market economy. EAI strives to produce and promulgate realistic policy ideas and suggestions through interdisciplinary research in the social science fields and the use of its domestic and international knowledge network. EAI seeks to become "Korea's leading think tank" and develop into "a globally recognized think tank" by doing its outmost to create "a knowledge net for a better world."

Mission

- Promote democracies that respect civil rights and human dignity with an emphasis on liberal values such as tolerance, accountability, transparency, and equal opportunity.
- Contribute to the peace and prosperity of the international community, based on liberal democracy, a market-oriented economy, and an open society.
- Propose policy recommendations to construct a democratic community and realize a peaceful East Asia.
- Provide good ideas for South Korea's domestic and foreign affairs through the Peace and Security, Economy and Technology, Democratic Cooperation, and Innovative Future programs.
- Nurture future leaders through Education and Human Development program.
- Construct a knowledge-net for a better world in the belief that good ideas can change the world.


EAI
EAST ASIA INSTITUTE