EVALUATING NATIONAL SECURITY MEASURES THROUGH THE PRISM OF DEFENSIVE AND OFFENSIVE DEPLOYMENT

Joel Slawotsky*

ABSTRACT

The return of the global governance architecture towards a mercantilist and protectionist era is transformative. From tariffs, outbound investment screening, sanctions, export controls, and counter-measures, an era of weaponized governmental policies has replaced the era of unfettered cross-border investment and trade. The new paradigm is proximately caused by heightened concerns over national security particularly within the context of the China-U.S. hegemonic clash. Restrictive measures are invoked to address an expanded conceptualization of security encompassing economic, technological, and ideological power spheres. Moreover, security is trending towards being understood as retention of dominance and deprivation of a competitor's capabilities raising the potential for abusive invocation. Courts and tribunals will need to balance legitimate security invocation with curbing the slippery slope of unfettered expansion in defining security and impermissible measures. This article endeavors to contribute to the discourse by distinguishing between "defensive" and "offensive" dimensions of national security-based measures. The article concludes that defensive expansion and deployment is more justifiable although some degree of offensive measures may also be linked to legitimate invocation.

* Reichman University, jslawotsky@runi.ac.il.

臺灣大學學術期刊資料庫

KEYWORDS: *national security, defensive measures, offensive measures*

臺灣大學學術期刊資料庫

Table of Contents

I. Introduction 289
II. Defensive and Offensive Expansions of National Security in the U.S., China, and EU 296
A. The Expansion in Defining National Security to Encompass Economic, Technological, and Ideological Power 297
B. Defensive and Offensive Dimensions of U.S., Chinese, and EU Security Expansions 299
1. U.S. Expansion of National Security 299
2. China's Conceptualization of National Security 303
3. EU Conceptualization of National Security 309
III. Defensive and Offensive Conceptualization of Security in the Context of the China-U.S. Rivalry and Frontier Technologies 314
A. China-U.S. Rivalry 314
B. Tribunals Should Evaluate Security-Based Measures Distinguishing Between Defensive and Offensive Conceptualizations 315
C. Recent Arbitral Rulings in the Context of Defensive or Offensive Measures 319
1. Huawei v. Sweden (BIT) (Pending) 319
2. Russia Transit (WTO) 320
3. United States — Certain Measures on Steel and Aluminium Products 321
4. Global Telecom Holding v. Canada 321
D. Suggestions for Tribunals 321
IV. Conclusion 322

I. INTRODUCTION

Far from the halcyon days of cooperation and "win-win" economic partnership, the bipartisan United States (hereinafter "U.S.") perception is that the People's Republic of China (hereinafter "China") seeks regional, if not global dominance.[1] Proximately causing the new age of great power

[1] This Article acknowledges China's claim that this perception is misplaced and that China does not seek to displace the United States [hereinafter U.S.] as the dominant global power. China's Paramount Leader, Xi Jinping, has stated "China will never seek hegemony, expansion or sphere of influence." *See Xi Urges World Political Parties to Shoulder Responsibility for Pursuit of People's Wellbeing, Progress of Mankind*, STATE COUNCIL CHINA (July 7, 2021), https://english.www.gov.cn/news/topnews/202107/07/content_WS60e502a2c6d0df57f98dc82b.html. Yet world history demonstrates that powerful sovereigns do endeavor (or eventually decide) to leverage structural power, project dominance, and seek regional if not global hegemony. *See* Lutz-Christian Wolff, *Legal Responses to China's "Belt and Road" Initiative: Necessary, Possible or Pointless*

臺灣大學學術期刊資料庫

rivalry, the U.S. believes China's ambition constitutes a serious national security threat.[2] However, in contrast to prior eras of strategic rivalry which focused on military power, the China-U.S. hegemonic competition also encompasses economic, technological, and ideological power as these realms of power can degrade and weaken an adversary.[3] Unsurprisingly, the China-U.S. strategic battlefield is defined by both nations as a competitive race to dominate the high-ground in strategic economic, technological, and ideological power spheres (e.g., industrial capacity, frontier technologies, data flows, and social media).[4]

Critically, this paradigm shift in conceptualizing national security has proximately caused a transformational expansion in how nations endeavor to defend national security. No longer limited to armed conflict, commercial

Exercise?, 29(2) TRANSNAT'L L. & CONTEMP. PROBS. 249, 256 (2020) ("It would, in fact, be naive to believe that China is not pursuing its own geopolitical BRI goals.").

[2] The sweeping reconceptualization of the U.S.-China relationship is evinced by comparing U.S. recent National Security Strategy [hereinafter NSS] documents. *Compare* GEORGE W. BUSH, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 27 (2002), https://2009-2017.state.gov/documents/organization/63562.pdf ("In time, [China] will find that social and political freedom is the only source of national greatness."), *and* GEORGE W. BUSH, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 42 (2006), https://history.defense.gov/Portals/70/Documents/nss/nss2006.pdf ("China's leaders . . . cannot let their population increasingly experience the freedoms to buy, sell, and produce, while denying them the rights to assemble, speak, and worship."), *with* DONALD J. TRUMP, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 25 (2017), https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf ("China seeks to displace the United States in the Indo-Pacific region, expand the reaches of its state-driven economic model, and reorder the region in its favor."). *See also infra* notes 39-41 (policy speeches). The realization that China's ascent threatened U.S. hegemony commenced in the mid-2010s. *See* Julien Chaisse, *State Capitalism on the Ascent: Stress, Shock, and Adaptation of the International Law on Foreign Investment*, 27(2) MINN. J. INT'L L. 339, 353 (2018) (Towards the conclusion of Obama's Presidency it became clear that, "China's revival threaten[ed] American power, especially in the Asia-Pacific region. This situation has been clear for some time, at least for observers who know what they are talking about.").

[3] *See generally* Joel Slawotsky, *The Fusion of Ideology, Technology and Economic Power: Implications of the Emerging New United States National Security Conceptualization*, 20(1) CHINESE J. INT'L L. 3 (2021) (discussing the U.S. expansion in defining security). China also has expanded her understanding of security, arguably doing so before the U.S. expansion. *See infra* Part II.B.2. *See also* Sheng Zhang, *Protection of Foreign Investment in China: The Foreign Investment Law and the Changing Landscape*, 23(4) EUR. BUS. ORG. L. REV. 1049, 1066-68 (2022) (China greatly expanded her focus on national security during the era of encouraging foreign investment).

[4] The emphasis on frontier technologies is unsurprising as both nations understand that most technologies have dual uses and some emerging technologies such as Artificial Intelligence [hereinafter AI] and robots will be transformative in the context of armed conflict. *See generally* Basil C. Bitas, *Finding Equilibrium amid the Deep Disruption of the "Geopolitical Metaverse"*, 5(1-4) CHINA & WORLD 1 (2023) (rapid technological transformations impacting the China-U.S. relationship). In addition, nations that dominate these emerging technologies will create vast amounts of new wealth. Indeed, China's Paramount Leader Xi has described the strategic battlefield as a struggle to surpass rivals over technological innovation. *See* Chris Buckley, *What Slowdown? Xi Says China Must Win the Global Tech Race*, N.Y. TIMES (Mar. 11, 2025), https://www.nytimes.com/2025/03/11/world/asia/china-xi-trump.html (China must surpass rivals in emerging technologies. "China [must] forge ahead in advanced technologies including artificial intelligence, biotechnology and new weapons.").

臺灣大學學術期刊資料庫

activity is now inextricably linked to national security. For example, the U.S. Federal government has undertaken measures including tariff imposition, restrictions on Huawei, enhanced inbound and outbound investment review, widespread export controls, potential market de-listings, sanctions impositions, forcing a TikTok sale, and other measures demonstrating that national security is now inextricably linked to commerce.[5] The measures reflect a doctrine explicitly adopted by recent U.S. administrations that economic security (and thus commercial conduct) is inseparable from national security.[6]

Similarly, China has substantially expanded her conceptualization of security beyond military defense and weaponry to encompass a wide swath of economic, political and social interests. China views emerging technologies as crucial in the geo-political strategic battlefield and focuses on surpassing rivals in technological innovation.[7] China has also undertaken measures demonstrating the link between commercial conduct and national security as will be discussed *infra* Part II.B.2.

The emphasis on frontier technologies by both China and the U.S. is logical given that most technologies have dual-uses.[8] Some emerging

[5] These measures encompass Congressional laws as well as Executive Orders which have been increasingly invoked by reliance on the International Emergency Economic Powers Act [hereinafter IEEPA] § 202, 50 U.S.C. § 1701. Pursuant to the IEEPA, a national emergency is declared based on a threat to U.S. national security or foreign policy, and directing Federal agencies such as Treasury, Commerce, and others, to implement rules to defend U.S. national security from the declared threat. *See, e.g.*, Protecting Americans from Foreign Adversary Controlled Applications Act, 15 U.S.C. § 9901 (requires ByteDance, the parent company of TikTok, to sell the app or face a ban in the U.S.); *Outbound Investment Security Program*, U.S. DEP'T TREASURY, https://home.treasury.gov/policy-issues/international/outbound-investment-program (last visited Feb. 28, 2026) (restrictions on U.S. outbound investments in China); *FCC Approves New Safeguards Against Untrustworthy Gear*, FED. COMMC'NS COMM'N (Oct. 28, 2025), https://docs.fcc.gov/public/attachments/DOC-415131A1.pdf (U.S. Federal Communications Commission issues new more expansive restrictions regarding on Huawei and other Chinese devices); *U.S. Export Controls and China: Advanced Semiconductors*, CONGRESS.GOV (Sep. 19, 2025), https://www.congress.gov/crs-product/R48642 (Federal export controls). *See also* Xueji Su, *Reframing Capital Control: Outbound Investment Screening and International Investment Law*, 27(1-2) J. WORLD INV. & TRADE 69 (2026) (reviewing outbound screening mechanisms).

[6] Kathleen Claussen & Timothy Meyer, *Economic Security and the Separation of Powers,* 172(1) U. PA. L. REV. 1955, 1957 (2024) (noting that both the "Trump and Biden administrations have invoked economic security as a justification for action across a wide range of policy issues. They have used tools traditionally viewed as commerce tools to address national security threats and they have deployed national security instruments for threats to commerce."). The trend is not limited to the U.S. *See* Henrique Choer Moraes, *The Changing Logic of International Economic Law*, 27(2) UCLA J. INT'L L. & FOREIGN AFFS. 115, 115 (2024) ("Instead of interdependence, trade liberalization, and market orientation, rules and government decisions are increasingly directed to pursue goals such as reduction of dependence, resilience, autonomy, and even self-reliance.").

[7] *See* Buckley, *supra* note 4 (According to China's Paramount Leader Xi Jinping, "China [must] forge ahead in advanced technologies including artificial intelligence, biotechnology and new weapons."). *See also infra* notes 52-55 (Chinese expansion encompasses political and social stability and other non-traditional notions of national security).

[8] Bitas, *supra* note 4. AI can also be a very powerful tool in legal settings in a wide-array of contexts. *See generally* Hsuan-Lei Shao et al., *Factors Determining Child Custody in Taiwan After*

臺灣大學學術期刊資料庫

technologies, particularly Artificial Intelligence (hereinafter "AI"), will dramatically and consequentially transform the battlefield and nations dominating AI will likely dominate in armed conflict.[9] In addition, nations that lead these emerging technologies will attract global investment and create vast amounts of new wealth. Ideology is another integral component and can be used to weaken an adversary by demoralization; "dumbing-down" a population and reducing critical thinking skills; and shaping public opinion through algorithmic manipulation/AI-generated deep-fakes promoting false or misleading propaganda.[10]

Similar to the U.S. belief, the European Union (hereinafter "EU") perspective is that China seeks to undermine the Western Order and is endeavoring to weaken Western interests and allies.[11] The EU has responded to the perceived threat by establishing stricter EU inbound investment screening (and a possible EU outbound investment program), and restrictions on Chinese economic actors. Similar to the U.S., rising economic nationalism and industrial policy in the EU have replaced the era of

Patriarchy's Decline: Decision Tree Analysis on Family Court Decisions, 18(2) ASIAN J. COMPAR. L. 272 (2023) (innovative decision tree learning study of court decisions and noting the utility of decision tree analysis for lawyers and clients in evaluating likely outcomes to settle disputes extrajudicially).

[9] Daniel Michaels & Dov Lieber, *How AI Is Turbocharging the War in Iran*, WALL ST. J. (Mar. 7, 2026), https://www.wsj.com/tech/ai/how-ai-is-turbocharging-the-war-in-iran-aca59002 ("The U.S. and Israeli attacks on Iran have unfolded at unprecedented speed and precision thanks to months of planning, a massive assemblage of military force and a cutting-edge weapon never before deployed on this scale: artificial intelligence.").

[10] Critical thinking is among the most important skills. *See generally* Lutz-Christian Wolff, *Teaching Legal Creativity: Really*?, ASIAN J. LEGAL EDUC. (forthcoming 2026) https://doi.org/10.1177/2322 0058261468196 (critical thinking more important than creativity). The erosion of critical thinking is a serious danger and states endeavor to weaken an adversary's population's resolve and critical thinking skills through social media propaganda. One example is Roy Singham who operates from Shanghai and funds anti-U.S. activities, protests, and promoting anti-Western narratives. Given China's unique political-economic governance system, it is inconceivable that his activities are not, at a minimum, approved, if not directed or encouraged by the Chinese Communist Party [hereinafter CCP]. *See* Asra Q. Nomani, *Power Couple of Chaos: How a Tycoon and Activist Built a 'Revolutionary Base' at the House of Singham*, FOXNEWS (Mar. 23, 2026), https:// www.foxnews.com/us/power-couple-chaos-how-tycoon-activist-built-revolutionary-base-house-sin gham (discussing calls to investigate U.S. Marxist billionaire Roy Singham who lives in Shanghai with his wife Jodi Evans who founded Code Pink, who are alleged to be funding social media news sites promoting pro-China and anti-U.S. narratives).

[11] *See* FED. GOV'T, ROBUST. RESILIENT. SUSTAINABLE. INTEGRATED SECURITY FOR GERMANY: NATIONAL SECURITY STRATEGY 23 (2023), https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf ("China is trying in various ways to remould the existing rules-based international order, is asserting a regionally dominant position with ever more vigour, acting time and again counter to our interests and values."). *See also* GOV'T OFF. OF SWED., NATIONAL SECURITY STRATEGY 19 (2024), https://government.se/globalassets/governme nt/national-security-strategy.pdf ("China's deepening partnership with Russia and indirect support for Russia's war of aggression against Ukraine contribute to the serious security situation in Europe. China has been moving in an increasingly totalitarian direction.").

臺灣大學學術期刊資料庫

unfettered cross-border investment and trade.[12] Indeed, Huawei and ZTE have been explicitly identified as constituting a national security risk to the EU and might be banned throughout the EU.[13] The EU measures also reflect a doctrine similar to the U.S. that economic security (and thus commercial conduct) is inseparable from national security and is now manifested in the EU security concept.[14]

Chinese economic actors are starting to challenge the restrictive national security-based measures in both international investment tribunals and domestic courts, claiming the measures violate WTO law, investment and trade agreements, or domestic law. For example, TikTok challenged both a Montana state law and a Federal law imposing bans;[15] Huawei has filed an arbitration against Sweden for restrictions allegedly violating the China–Sweden Bilateral Investment Treaty (hereinafter "BIT");[16] Hikvision is considering action pursuant to the China–Canada BIT for Canadian measures targeting Hikvision;[17] FTDI Holding challenged a governmental measure in

[12] *See* TokenRing AI, *Dutch Government Seizes Nexperia Operations amid Intensifying US-Led Semiconductor Scrutiny*, WRAL NEWS (Oct. 14, 2025), https://markets.financialcontent.com/wral/article/tokenring-2025-10-14-dutch-government-seizes-nexperia-operations-amid-intensifying-us-led-semiconductor-scrutiny; Finbarr Bermingham, *China's Wingtech Says Dutch Court Freezes Control of Nexperia amid "National Security" Dispute*, S. CHINA MORNING POST (Oct. 13, 2025), https://www.scmp.com/news/china/diplomacy/article/3328726/chinas-wingtech-says-dutch-court-freezes-control-nexperia-amid-national-security-dispute.

[13] Gian Volpicelli & Jillian Deutsch, *EU Eyes Huawei Ban in Mobile Networks of Member Countries*, BLOOMBERG (Nov. 11, 2025), https://www.bloomberg.com/news/articles/2025-11-10/eu-eyes-banning-huawei-from-mobile-networks-of-member-countries ("The European Commission is exploring ways to force European Union member states to phase out Huawei Technologies Co. and ZTE Corp. from their telecommunications networks, according to people familiar with the matter.").

[14] *See generally* FRANÇOIS CHIMITS ET AL., EUROPEAN ECONOMIC SECURITY: CURRENT PRACTICES AND FURTHER DEVELOPMENT (2024), https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754449/EXPO_IDA(2024)754449_EN.pdf (European national security depends on European economic security).

[15] Anna Conley, *TikTok v. Montana — State TikTok Ban Blocked by Court Based on Foreign Affairs Preemption*, 28(2) AM. SOC'Y INT'L L. 1, 2 (2024), https://asil.org/insights/volume-28-issue-2/ (suit against state of Montana); Angela Yang & Savannah Sellers, *TikTok Sues U.S. Government, Saying Potential Ban Violates First Amendment*, NBC NEWS (May 8, 2024), https://www.nbcnews.com/tech/tech-news/tiktok-sues-us-government-says-ban-violates-first-amendment-rcna151059 (TikTok sues U.S. Federal Government).

[16] Cosmo Sanderson, *Huawei Brings ICSID Claim Against Sweden over 5G Ban*, GLOB. ARB. REV. (Jan. 24, 2022), https://globalarbitrationreview.com/article/huawei-brings-icsid-claim-against-sweden-over-5g-ban.

[17] *Our Response to the Government of Canada's Order to Shut Down Hikvision Canada Inc.*, HIKVISION, https://www.hikvision.com/ca-en/newsroom/latest-news/2025/our-response-to-the-government-of-canada-s-order-to-shut-down-hi/; Tom Jones, *China's Hikvision Threatens Claim Against Canada over National Security Measures*, GLOB. ARB. REV. (Sep. 24, 2025), https://globalarbitrationreview.com/article/chinas-hikvision-threatens-claim-against-canada-over-national-security-measures.

臺灣大學學術期刊資料庫

UK domestic courts[18]; and Huawei is rumored to be contemplating filing a claim against Poland based on the Energy Charter Treaty (ECT).[19]

This paper's focus is with respect to challenges over measures filed pursuant to international investment and trade agreements (i.e., international economic law). In the context of international economic law, the sovereigns' defense generally relies upon the national or essential security exception found in most agreements which enables the state to override the obligations contained in the agreement in order to defend security. While the security exception has existed for decades, it had not been widely arbitrated until the last few years.[20] However, as national security-based restrictions are increasingly invoked, the likelihood is for economic actors to arbitrate and/or litigate the sovereign's reliance on the security exception and the issue will likely become a significant one for tribunals.[21]

How should tribunals evaluate national security-based measures? Tribunals have rules to guide their evaluation—derived from principles of international law—and legitimate invocations of security have been linked to armed conflict or threats to territorial integrity, requiring a proportional, good-faith invocation demonstrated by necessity.[22] Pursuant to necessity, states must establish the defensive measure was necessary to defend against an imminent and grave peril with no alternative solution.[23]

However, evaluating measures pursuant to the paradigm of armed conflict is problematic for two reasons. One, nations can attack and degrade adversaries through a variety of non-military methods rendering the notion of security being connected solely to physical defense and territorial integrity

---

[18] Joseph Sherlock & Nissim Massarano, *UK High Court Upholds NSIA Order to Divest on National Security Grounds*, CLIFFORD CHANCE (Aug. 4, 2025), https://www.cliffordchance.com/insights/resources/blogs/antitrust-fdi-insights/2025/08/uk-high-court-upholds-nsia-order-to-divest-on-national-security-grounds.html.

[19] Jack Ballantyne, *Huawei Threatens Poland over Cybersecurity Law*, GLOB. ARB. REV. (Oct. 24, 2025), https://globalarbitrationreview.com/article/huawei-threatens-poland-over-cybersecurity-law.

[20] *See* Julien Chaisse, *Demystifying Public Security Exception and* Limitations *on Capital Movement: Hard Law, Soft Law and Sovereign Investments in the EU Internal Market*, 37(2) U. PA. J. INT'L L. 583, 601 (2015) (dearth of rulings on the exception). Indeed, the first WTO ruling on the security exception did not take place until 2019. *See generally* Panel Report, *Russia — Measures Concerning Traffic in Transit*, WTO Doc. WT/DS512/R (adopted Apr. 26, 2019) [hereinafter *Russia — Traffic in Transit* Panel Report]. One of the reasons for the previous relative dearth of rulings (in addition to the reduced relevance of adjudicating security during the boom years of unfettered investment and trade), include a general reluctance to interfere with the decision-making of sovereigns arising from respecting nations' ability to "self-judge". For a comprehensive discussion of self-judging, see generally Tsai-fang Chen, *To Judge the "Self-Judging" Security Exception Under the GATT 1994 – A Systematic Approach*, 12(2) ASIAN J. WTO & INT'L HEALTH L. & POL'Y 311 (2017).

[21] *See generally* Ming Du, *Huawei Strikes Back: Challenging National Security Decisions Before Investment Arbitral Tribunals*, 37(1) EMORY INT'L L. REV. 1 (2022); *supra* notes 15-19.

[22] *See generally* Paul Weidenbaum, *Necessity in International Law*, 24 TRANSACTIONS GROTIUS SOC'Y 105 (1938) (tracing and discussing the development of the necessity principle in light of World War I).

[23] The Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. 7, ¶ 51 (Sep. 25) (principle of necessity has the status of customary international law).

臺灣大學學術期刊資料庫

outmoded. Two, principles of necessity and proportionality, as traditionally understood, are difficult to evaluate in an age of infrastructure hacks, gradual de-industrialization, and AI-generated deep fake propaganda. None of these weapons constitute an easily provable "immediate danger of a grave peril" yet constitute real national security threats. Moreover, the notion of proportionality is unclear given the fact the threat might be either dormant or "a gradual erosion" and therefore the extent of the potential damage unknown rendering the evaluation of a "proportional response" difficult at best. In an age of weaponizing dependencies to deindustrialize a competitor or adversary, emerging technologies embedding viruses or enabling kill switches on Electric Vehicles (hereinafter "EVs") and critical infrastructure (let alone military equipment), data gathering, and algorithmic manipulation of social media, principles of necessity, proportionality, and good-faith are increasingly more complicated and difficult to evaluate.[24]

The issue of national security based measures is of vital import given the ongoing China-U.S. rivalry, a breakdown of traditional alliances, the trend towards unilateralism, and what appears to be an attempt to re-make global governance.[25] Scholars have raised questions regarding the problem of determining under what circumstances invoking national security is legitimate since national security may be invoked for impermissible reasons such as protectionism.[26] This article contributes to the literature by

---

[24] *See generally* Yang Liu, *Proportionality Balancing Under General International Law: The Case of Article 25(1)(b) of ARSIWA*, 21(4) CHINESE J. INT'L L. 647 (2022) (discussing necessity in the context of proportionality).

[25] Wolfgang Alschner, *Recalibration, Shielding and Containment: How the World Trading System De-Risks from China and the United States*, 24(4) WORLD TRADE REV. 498, 498 (2025)

> Trade multilateralism has a problem. The world's largest importer, the United States, and the world's largest exporter, China, are operating outside the rules that govern multilateral trade. China is employing non-market practices that subvert global trading rules and that have fueled an export oriented production overcapacity that threatens deindustrialization abroad. The United States during President Trump's second term has unilaterally barricaded its lucrative consumer market behind tariff walls in clear breach of World Trade Organization (WTO) commitments to tilt the terms of trade in its favor.

see generally Anne van Aaken, *From Cooperation to Anomie and Transaction in the Transatlantic Relationship? A View from Europe on the Trump Administration 2.0*, 119(4) AM. J. INT'L L. 723 (2025) (outlining the fraying U.S.-European alliance and ostensible U.S. efforts to coerce ally conduct); Julien Chaisse & Georgios Dimitropoulos, *Special Economic Zones in International Economic Law: Towards Unilateral Economic Law*, 24(2) J. INT'L ECON. L. 229 (2021) (identifying several forms of economic unilateralism including national security unilateralism); Julien Chaisse & Xueji Su, *Normative Realignment in Domestic Trade Barriers Procedures: Driving Unilateralism in the EU, US, and China*, 24(3) WORLD TRADE REV. 361 (2025) (unilateralism in the U.S., European Union [hereinafter EU], and China).

[26] The issue of evaluating the security exception is vexing and several innovative ideas have been advanced. *See generally* Qianwen Zhang, *Securing National Security in Regulating Cross-Border Data Transfer in Foreign Investment*, 21(1) ASIAN J. WTO & INT'L HEALTH L. & POL'Y 95 (2026) (noting the lack of guidance for both host states and international tribunals with respect to the national

臺灣大學學術期刊資料庫

suggesting a potential method for evaluating the exception by distinguishing measures through the prism of either a "defensive" deployment (intended to defend security) or an "offensive" deployment (designed to degrade and weaken).[27] To be sure, measures may contain aspects of both defensive and offensive deployment. Nevertheless, it may be useful for tribunals to endeavor to differentiate measures, sift through intentions, and determine whether an offensive impact is merely ancillary or the primary intent of a measure. The article concludes that defensive deployment is generally more justifiable although some degree of offensive deployment may be justified as anticipatory self-defense and therefore legitimate.

II. DEFENSIVE AND OFFENSIVE EXPANSIONS OF NATIONAL SECURITY IN THE U.S., CHINA, AND EU

This Part is divided into two main sections. The first section discusses the reasons justifying an expanded security conceptualization which is driven by the ability to degrade an adversary through a variety of non-military means. While national security was traditionally defined in terms of military deterrence and protecting the territorial integrity of a nation, today an enemy

security exception); Ming Du, *International Economic Law in the Era of Great Power Rivalry*, 57(3) VAND. J. TRANSNAT'L L. 723 (2024) (security exception in turmoil); Youyou Jiang, *Defining the Boundaries: WTO National Security Exceptions in the US-China Unilateral Trade Sanctions*, 18(2) J. E. ASIA & INT'L L. 299 (2025). Scholars have made several suggestions. *See generally* Chen, *supra* note 20 (arguing that the abuse of discretion standard might be helpful in evaluating necessity); Tsai-fang Chen, *Forging Trade Rules in the Age of AI: The Case for Special Labor Safeguards*, *in* GEOPOLITICAL RISKS AND GEOECONOMICS IN INTERNATIONAL ECONOMIC LAW 379, 379 (Junji Nakagawa et al. eds., 2026) (noting the transformative nature of AI shocks and suggesting a new WTO instrument to allow members to address employment dislocation linked to trade in AI-intensive products and services); Mao-wei Lo, *Essential Security Creep and WTO Adjudication: Recalibrating Security Exceptions in a Changing Geoeconomic Order*, 57(3) GEO. J. INT'L L. (forthcoming winter 2026) (using U.S. Constitutional law standards); Stratos Pahis, *Can Plurilaterals Solve the WTO's National Security Crisis?*, 26(1-2) J. WORLD INV. & TRADE 189 (2025) (utilizing plurilateral agreements to broaden the current General Agreement on Tariffs and Trade [hereinafter GATT] security exception or by creating a parallel dispute settlement mechanism); Xinyue Li, *Quantizing Geoeconomics: Emerging Geoeconomics in International Economic Law Through a Quantum Worldview*, 17(1) ASIAN J. WTO & INT'L HEALTH L. & POL'Y 5, 9 (2022) (suggesting quantum theory to understand that measures may simultaneously contain various connected (and unconnected) motivations and impacts); Xinyue Li, *A Parallel Narrative: Pluralistic Reconciliation Through Quantizing Geoeconomics in (Cyber) Security Governance in International Economic Law*, 18(1) ASIAN J. WTO & INT'L HEALTH L. & POL'Y 89 (2023).

[27] Similarly, in other contexts the suggestion has been raised of distinguishing between two types of measures. *See* Marko Milanovic, *Revisiting Coercion as an Element of Prohibited Intervention in International Law*, 117(4) AM. J. INT'L L. 601, 601 (2023) (conceptualizing coercive intervention as either "coercion-as-extortion" targeting the victim state's will or decision-making and "coercion-as-control" depriving the victim state of its ability to control its sovereign choices). *See also* Yiying (Gloria) Xiong, *Legality, Legitimacy and Institutionalization: China's Dilemma of Sanctions and Economic Coercion*, 34(152) J. CONTEMP. CHINA 181, 181 (2025) (opining a distinction between defensive anti-sanctions measures and offensive use of original sanctions).

臺灣大學學術期刊資料庫

can "cross the border" and in effect invade and degrade an adversary using economic, technological, and ideological power.

The second section explores the specific expansion of security in the U.S., China and the EU through the prism of distinguishing between defensive and offensive deployment of measures to address security concerns. The defensive prong of expansion encompasses conceptualizing security beyond military power and into new non-military power spheres but deploys measures in a defensive posture, i.e., endeavoring to ensure that sovereigns are resilient and can defend threats in the new power spheres. Examples of defensive measures are traditional export control laws on new dual-use military weapons, preventing cyber-attacks, inbound investment screening to avoid foreign control of strategic sectors, and governmental ownership of publicly-traded corporations in order to protect domestic strategic entities from foreign ownership or influence, ensure domestic resiliency, and to ensure the entities business decisions align with promoting national security.

In contrast to the defensive prong, offensive expansion constitutes a tectonic shift in strategic posture from purely defensive measures to proactive policies evincing an offensive intent to contain or weaken another sovereign. This offensive dimension comports with policies that seek to re-shape the strategic context to ensure long-term dominance and denial of competitive capabilities. The offensive expansion can be exemplified in coercive economic policies, widespread export controls, outbound investment restrictions, forming strategic alliances to deprive adversaries of inputs and technologies, and potentially governmental acquisition of shares in important publicly-traded entities (both domestic and foreign) to be used as offensive instruments (i.e., as a national security agent to weaken adversaries).

A. The Expansion in Defining National Security to Encompass Economic, Technological, and Ideological Power

Historically, military power enabled a nation to physically overwhelm an adversary's defenses, cause destruction, plunder resources, and dominate the enemy. Unsurprisingly, defending the national bastion was focused on defense from armed attack and protecting borders. In the decades following the last era of geostrategic conflict, international law understood legitimate invocation of national or essential security as measures necessary to defend against a physical attack and to preserve territorial integrity.

However, while raw military power remains the ultimate arbiter of strength, nations can now be attacked and undermined through a variety of economic, technological, and ideological power without resorting to military

臺灣大學學術期刊資料庫

conflict.[28] Furthermore, these power spheres can be used to complement an armed attack.

Economic power vests a nation with the financial resources to build both defensive military capabilities as well as providing structural power in global affairs, i.e., the ability to form alliances, leverage power imbalances to extract benefits, wield a global currency, and create the wealth necessary for a strong and politically stable citizenry. Economic power is also related to industrial capacity which translates into employment and the ability to manufacture military equipment and other civilian products necessary to sustain a prolonged military conflict. Domestic economic self-sufficiency and resilience to foreign dependency is therefore also an integral aspect of security.

Technological power enables the creation of vast wealth generated from new industries and the ability to degrade an adversary through non-military means such as election hacking to ensure a favorable candidate is elected, vital infrastructure sabotage, or data theft. Embedded viruses or the ability to hack into a rival's military infrastructure and defense systems during a time of an armed attack would prove invaluable in destroying the adversary's capabilities to defend itself. Similarly, remotely shutting off civilian infrastructure such as power plants, EVs (both civilian and military) and energy facilities would similarly have a devastating impact on the enemy state's ability to defend itself.

In particular, an incredible array of transformational frontier technologies will provide the nation that dominates "Fourth Industrial Revolution" technologies with immense structural and soft power, and economic advantage.[29] Dominating revolutionary frontier technologies such as AI, robotics, quantum, bio-technology, edge computing, digital trust, and space flight, are crucial for national security for three compelling reasons. One, these sectors will create trillions in new wealth that can fund a military. Two, frontier technologies have dual uses either for direct military use or indirect such as intelligence collection and therefore have important relevance to military power. Three, emerging technologies will vest the sovereign with tremendous structural power as other nations seek to buy and

---

[28] *See generally* Slawotsky, *supra* note 3.

[29] *See* TED, *The Next Global Superpower Isn't Who You Think | Ian Bremmer | TED*, at 11:59-12:16 (YouTube, June 14, 2023), https://www.youtube.com/watch?v=uiUPD-z9DTg&t=3s (technology companies and their powerful tools are as important as nations and may, if not regulated properly, rule the future). Technology and digitalization are inextricably linked to national security. *See* Locknie Hsu, *Digitalization and Its Role in International Economic Law*, *in* A RESEARCH AGENDA FOR GLOBAL POWER SHIFTS AND INTERNATIONAL ECONOMIC LAW 127, 127 (Joel Slawotsky ed., 2025) ("[T]he role of technology and increasing digitalization in the public and private spheres have become clearly entwined with considerations of economic strategy (or supremacy to some) and essential national security."). *See also* PAUL B. STEPHAN, THE WORLD CRISIS AND INTERNATIONAL LAW: THE KNOWLEDGE ECONOMY AND THE BATTLE FOR THE FUTURE 276-77 (2023) (discussing the importance of data and how it can be utilized to degrade enemy states).

臺灣大學學術期刊資料庫

incorporate the leader's technologies and standards for their own benefit and development. Both hegemonic rivals, the U.S. and China, understand that *technological dominance* in emerging technologies is the basis of national power.

Ideological power is also vital as ideological warfare can be used to demoralize an enemy and as a vehicle to promote propaganda to shape an adversary's citizens' views. Ideological warfare waged through AI generated deep fakes and algorithmic manipulation of social media and propaganda can weaken adversarial resolve, influence public opinion, and reduce critical thinking abilities which can be leveraged to weaken an adversary. Even "soft-power" and notions of governance and values are considered a component of defending national security.

Furthermore, all three of these power spheres are inextricably linked and the fusion of interests strengthens each sphere collectively. For example, AI, facial recognition, and social media can create powerful new synergistic wealth-creating industries (i.e., economic power), as well as serve as conduits to obtain data, eviscerate privacy, and surveil/control populations (technological and ideological power). AI can help identify the enemy location for drones (and in the future robots) as well as traditional forms of firepower called in instantly to neutralize enemy positions. Accordingly, the cornerstone of national security is no longer solely based upon defending territorial integrity and defense against an armed invasion, but rather encompasses economic, technological, and ideological power.

B. Defensive and Offensive Dimensions of U.S., Chinese, and EU Security Expansions

The following section is divided into three sub-sections which examine U.S., China, and EU invocations of security distinguishing between defensive and offensive deployments. While the importance of discussing the U.S. and China is manifestly clear, including the EU is important because the U.S., EU, and China constitute three enormous economic powers with massive markets and large populations. Moreover, the EU is embedded in investment and trade and has interests within the context of the great power rivalry thereby impacting the emerging re-conceptualization of national security. The EU also represents an economic architecture between the U.S. and China, in a sense, a "Third Way", and other literature on international economic law and governance often reference the EU as an important part of the global economic and legal orders (e.g., when discussing data governance or investment screening mechanisms).

1. U.S. Expansion of National Security —

(a) Defensive Conceptualization and Deployment — Aligning with the expansion in conceptualizing national security, the U.S. has instituted a

臺灣大學學術期刊資料庫

variety of measures related to economic, technological and ideological power. For example, in terms of economic power, in January 2025 the U.S. blocked Nippon Steel's takeover of U.S. Steel ostensibly because U.S. national security demanded avoiding steel production, a critical material for defense, from falling into foreign control.[30] The defensive nature of the measure is evident; critical materials are vital for defense production (comporting with classical notions of security), as well as manufacturing and the industrial base generally (i.e., reflecting the expansion into economic power) triggering a defensive need to avoid steel production from falling into foreign control.[31] While the deal was ultimately approved, on condition the U.S. would receive a Golden Share providing ultimate control, the saga demonstrates the important link between industrial capacity and security and is an exemplar of a defensive deployment of a national security-based measure, i.e., ensuring domestic resilience.

Significantly, the acquisition of the Golden Share is only one example of the trend of the U.S. government to become more involved in the economy and incorporate aspects of state-capitalism as demonstrated by the recent acquisition of stakes in numerous companies. The U.S. move to become a shareholder in strategic entities is not surprising given concerns over national security.[32] The incipient trend of incorporating aspects of state capitalism reflects an expansion in security and may be a harbinger of more states becoming involved in their economies.[33] State acquisition of shares is defensive in nature as the goal is to protect strategic industries and promote resiliency. However, share ownership could potentially be weaponized by leveraging share positions to influence corporation thereby transforming the entities from defensive assets to offensive agents to weaken an adversary by undercutting competition or through cooperation with their home governments.

In a further illustration of a defensive deployment, a 2022 U.S. Presidential Executive Order focused on investment review with respect to the "defense industrial base" noting the national security nexus to "biomanufacturing, quantum computing, advanced clean energy."[34] The

[30] The U.S. Committee on Foreign Investment in the U.S. [hereinafter CFIUS] had raised some objections to the transaction based on national security and former President Biden blocked the deal.
[31] Of course, a "darker" explanation can be that in international relations, even long-term allies may at some point become rivals.
[32] *See generally* Joel Slawotsky, *The Impact of Geo-Economic Rivalry on U.S. Economic Governance: Will the United States Incorporate Aspects of China's State-Centric Governance?*, 16(3) VA. L. & BUS. REV. 559 (2022) (discussing the reasons the U.S. might incorporate tenets of state capitalism).
[33] *See* XINYUE LI, INTERNATIONAL ECONOMIC LAW AND QUANTUM THEORY: QUANTIZING GEOECONOMICS 30-33 (2026) (likelihood that states will become more involved in commercial activity).
[34] Exec. Order No. 14083, 3 C.F.R. 434, 436 (2023) ("The Committee shall consider . . . the covered transaction's effect on supply chain resilience and security, both within and outside of the defense industrial base . . . ."). In recent years, the link between supply chains and national security in the context of the China-U.S. hegemonic rivalry has become manifestly clear. *See* Xuanli Chen & Wei

臺灣大學學術期刊資料庫

Executive Order relates to inbound investment review which comports with a defensive posture, i.e., preventing technological power from being under foreign control.

Demonstrating the expansion in conceptualizing national security into the realm of finance, China's global capital market integration and development of China's central bank digital currency (hereinafter "CBDC") are considered threats to U.S. national security. "China's tightened integration with global financial markets poses distinct economic risks to U.S. investors and national security risks to the United States."[35] "[While] China's digital RMB does not present an immediate challenge to the U.S.-led global financial system, the belief is in the long term it could undermine the status of the U.S. dollar and efficacy of U.S. financial sanctions."[36]

Whether or not the potential measures associated with China's capital market integration and CBDC will be defensive or offensive is more nuanced and would depend upon the specific measure. If for example U.S. financial institutions were blocked from engaging in transactions with a Chinese CBDC it might fall within the ambit of a defensive measure while preventing Chinese institutions from tapping foreign capital or interfering with China's endeavors to build Shanghai into a global financial hub by imposing sanctions might constitute an offensive measure.

Another example of the expansion in defining security beyond the traditional notion of armed conflict, as well as an illustration of how technology and ideology are often fused together, is the U.S. ban on TikTok unless sold to a U.S. entity. Congress passed a law ordering TikTok—currently under the control of a Chinese parent, ByteDance—to be banned unless sold to a U.S. entity based on national security concerns. The claim is that TikTok represents a national security threat based upon data collection and algorithmic manipulation promoting ideological propaganda. The law was upheld by the Supreme Court and a transaction transferring ownership was finalized in early 2026.[37] The measure demonstrates the expansion of the U.S. conceptualization of security to encompass technological and ideological power but constitutes a defensive deployment as the concerns focus on data transfer and algorithmic manipulation with respect to U.S. users.[38]

Shen, *Disputing Supply Chain Security Legislation in the Context of WTO Rules: Litigability, Legitimacy, and Exceptionality*, 16(4) J. INT'L DISP. SETTLEMENT 1, 2 (2025) ("[T]he issue of supply chain security has gradually been linked with international economic and political issues such as national security and geopolitics between major powers").

[35] U.S.-CHINA ECON. & SEC. REV. COMM'N, 117TH CONG., 2021 REPORT TO CONGRESS OF THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION 11 (2021).

[36] *Id.* at 166.

[37] *See generally* TikTok Inc. v. Garland, 604 U.S. 56 (2025). (upholding the measure based upon national security).

[38] Interestingly, while most measures emanate from the U.S. Federal government, U.S. states have also entered the national security paradigm. *See generally* Joel Slawotsky, *The Return of the States:*

臺灣大學學術期刊資料庫

(b) Offensive Conceptualization and Deployment — The second strand of security's expansion ensconces an offensive dimension, an intent to weaken another nation. Significantly, the offensive prong transforms the expansion from "defense" of national resilience and protection of crucial industries to retaining dominance and/or imposing capability denial. Illustrating the conceptual underpinning, former U.S. Attorney General William Barr remarked that China was aiming to surpass the United States *which by itself* represented a threat to U.S. national security.[39]

Former U.S. National Security Advisor Jake Sullivan articulated a particularly expansive notion further exemplifying the foundation of offensive deployment; maintaining dominance is no longer sufficient to defend U.S. security.[40]

> On export controls, we have to revisit the longstanding premise of maintaining "relative" advantages over competitors in certain key technologies. . . . Given the foundational nature of certain technologies, such as advanced logic and memory chips, we must maintain as large of a lead as possible. . . . This has demonstrated that technology export controls can be more than just a preventative tool.[41]

Accordingly, defending U.S. national security is now understood as not merely retaining superiority, but includes depriving a competitor of the means to compete. This is a remarkable conceptualization of national security and comports with an offensive dimension of expansion.

Denial of capabilities measures are increasing as illustrated by export controls and outbound investment restrictions. An example is a 2023 Executive Order instructing the relevant U.S. Federal agencies to develop rules barring persons under U.S. jurisdiction (or requiring notification to U.S. regulators) from investing in businesses, organizations, and governmental/political entities from "countries of concern" (only listing China, the Hong Kong Special Administrative Region (hereinafter

---

Constitutional Dilemmas of State Measures to Defend National and State Security, 34(2) ASIA PAC. L. REV. 247 (2026).

[39] *Attorney General William P. Barr Delivers Remarks on China Policy at the Gerald R. Ford Presidential Museum*, U.S. DEP'T OF JUST. (July 16, 2020), https://www.justice.gov/archives/opa/speech/attorney-general-william-p-barr-delivers-remarks-china-policy-gerald-r-ford-presidential ("The People's Republic of China is now engaged in an economic blitzkrieg—an aggressive, orchestrated, whole-of-government (indeed, whole-of-society) campaign to seize the commanding heights of the global economy and to surpass the United States as the world's preeminent superpower.").

[40] *Remarks by National Security Advisor Jake Sullivan at Special Competitive Studies Project Global Emerging Technologies Summit*, WHITE HOUSE (Sep. 16, 2022), https://www.miragenews.com/remarks-by-national-security-advisor-jake-856536/.

[41] *Id.*

臺灣大學學術期刊資料庫

"HKSAR") and Macau), with regard to activities related to semiconductors and microelectronics, quantum information technologies, and artificial intelligence.[42] Barring U.S. persons from investing in China aligns with an offensive deployment of a national security-based measure.

Recent export controls also demonstrate the stark contrast between defensive and offensive deployment of measures. Export controls on military or dual-use items that identify the risky actors and list them to block transactions comport with a defensive conceptualization and deployment. In contrast, more recent export controls on advanced chips and machines producing chips exemplify the offensive dimension. The October 2025 House Select Committee on the Chinese Communist Party (hereinafter "CCP") report titled *Selling the Forges of the Future*, illustrates the offensive conception as applied to exports.[43] The crux of the report is that the recent export controls on semiconductors are ineffective and are failing to prevent China from achieving success in building its industrial base and technological power. The report illustrates the major shift in understanding export controls, from a defensive preventative posture to the goal of decapitating a competitor's ability to compete particularly in frontier technologies such as AI.

Moreover, the report calls for urgent governmental measures to strictly scrutinize restrictions on licensing policies and controls on both basic technology and advanced tools. A key phrase is the need to deny capabilities to China referred to as a "presumption of denial on a country-wide basis."[44] The report suggests that even basic tools and technology enable China to evade the U.S. containment policy and proposes extensive controls to close the loopholes.[45]

2. China's Conceptualization of National Security —

(a) Defensive Expansion and Deployment — China has also dramatically expanded her conceptualization of national security. The Chinese expansion is not new and arguably, China's expansion pre-dates the U.S. re-conceptualization. [46] Before discussing China's definition of national security, China's political-economic governance model must be understood. China is governed by the CCP which constitutes the omnipresent political authority and wields an overarching role injecting national objectives in the

---

[42] Exec. Order No. 14105, 3 C.F.R. 640, 644 (2023).

[43] *See generally* UNITED STATES CONGRESS, SELLING THE FORGES OF THE FUTURE: HOW THE CCP GETS ITS KEY EQUIPMENT FOR MAKING SEMICONDUCTORS FROM U.S., DUTCH, AND JAPANESE COMPANIES (2025).

[44] *Id.* at 5.

[45] *See generally* Ping Huang & Anton Malkin, *An Innovation Systems Approach to Decoding China's Technological Catch-Up: The Case of the Semiconductor Industry*, 33(4) INDUS. & INNOVATION 431 (2025) (discussing U.S. attempts at containing China's technological advancement).

[46] *See infra* notes 51-56 and accompanying text. *See also* Zhang, *supra* note 3 (discussing China's focus on national security in the 2010s); *see generally* SHEN WEI, CHINA'S FOREIGN INVESTMENT LAW IN THE NEW NORMAL: FRAMING THE TRAJECTORY AND DYNAMICS (2022).

臺灣大學學術期刊資料庫

management of economic priorities, activities, and corporations.[47] In China's model, the economic must always resolutely yield to CCP political interests.[48] Unsurprisingly, China's distinct governance model constitutes a major driver of Western concerns over the motivations of Chinese economic actors.[49]

China's conceptualization of national security is based on Party directives. Paramount Leader Xi Jinping emphasized the importance of "comprehensive national security" (总体国家安全观) which encompasses a whole Party-centric approach: "All party and state organs must improve their efforts to prevent and contain any internal and external threats to China's national security and political system."[50]

China's expansive construction of security beyond military power is illustrated in the 2011 White Paper titled "China's Peaceful Development" which lists China's "core national interests," such as "state sovereignty, national security, territorial integrity and national reunification, the political system established by the Constitution and overall social stability, and the basic safeguards for ensuring sustainable economic and social

[47] *See* Li-Wen Lin & Curtis J. Milhaupt, *We Are the (National) Champions: Understanding the Mechanisms of State Capitalism in China*, 65(4) STAN. L. REV. 697, 754 (2013) (discussing mechanisms of China's model).

[48] Pursuant to China's state-centric capitalist model, the CCP is the ultimate corporate controller whether a company is publicly-traded or ostensibly a private economic actor. *See generally* Slawotsky, *supra* note 32 (Party-state as the controller in both state-linked and private businesses). *See also* Beibei Zhang & Wei Shen, *China's Non-Performing Loans Disposal in Local and Global Contexts: Missing Pieces in International Law Matrix*, 58(3) J. WORLD TRADE 497, 502 (2024) ("The opening of China's financial markets is primarily a domestic policy decision, making it essential to consider political norms…").

[49] *See* HENRY GAO & WENZHOU ZHOU, BETWEEN MARKET ECONOMY AND STATE CAPITALISM: CHINA'S STATE-OWNED ENTERPRISES AND THE WORLD TRADING SYSTEM 1-12 (2022) (inherent conflict between state capitalism and market capitalism proximately causes friction in international investment and trade); Alschner, *supra* note 25, at 500 ("While China possesses a vast and highly dynamic economy with world-class scientists and entrepreneurs, its increasing dominance in industry after industry is attributed not only to comparative advantage, but to WTO-incompatible non-market practices that allow the state to heavily intervene and steer the economy."); Ru Ding, *Interface 2.0 in Rules on State-Owned Enterprises: A Comparative Institutional Approach*, 23(3) J. INT'L ECON. L. 637, 639 (2020) (U.S.-China trade conflict constitutes a manifestation of the tension between two economic models); *see generally* Ming Du, *China's State Capitalism and World Trade Law*, 63(2) INT'L & COMPAR. L.Q. 409 (2014) (discussing China's economic model and the WTO); Julien Chaisse, *State Capitalism on the Ascent: Stress, Shock, and Adaptation of the International Law on Foreign Investment*, 27(2) MINN. J. INT'L L. 339, 353 (2018) ("The rivalry between the two superpowers is also a rivalry between two economic models: market capitalism against state capitalism.").

[50] Xinhua, *Xi Stresses Safeguarding National Security, Social Stability, Peaceful Lives*, CHINA DAILY (Jan. 15, 2022), https://www.chinadaily.com.cn/a/202201/15/WS61e26eeaa310cdd39bc8141 8.html. For a review of Party influence over Chinese political institutions as shaped by Xi Jinping, *see generally* Susan Finder, *The Evolving Relationship Between the National People's Congress and the Supreme People's Court in the Xi Jinping Era*, CHINESE L. & GOV'T (forthcoming 2026).

臺灣大學學術期刊資料庫

development."[51] Social stability, political system stability (retaining CCP leadership which may require the imposition of domestic discipline as well as overseas efforts aimed towards Party stability), and social development are more expansive than classical understandings of security. Arguably, this expansion, at least in conceptualization, is defensive in nature except potentially for what is referred to as "national reunification".

In 2014 Paramount Leader Xi referred to eleven categories of expansive security interests including: political, homeland, military, economic, cultural, social, scientific and technological, information, ecological, resource, and nuclear.[52] Again, political, cultural, social, and ecological security all fall beyond defending the physical territory of China but can be understood as a defensive expansion. Another exemplar is China's 2015 National Security Law (hereinafter "NSL") which corroborated the broader notion of security to encompass the environment, finance, information technology, culture, ideology, education, and religion.[53] China's Export Control Law (hereinafter "ECL") which aims to safeguard national security also incorporates this holistic approach to security.[54] Both the NSL and ECL expand the conceptualization of national security, and while the laws can be understood as a defensive expansion, extraterritorial applicability of these laws may also implicate an offensive dimension depending upon the specific measure.

The expansion beyond the classical conceptualization of physical defense in the context of armed conflict is illustrated by Paramount Leader Xi's focus on conceptualizing security "boldly and innovatively" directing the government to draft comprehensive laws defending Chinese national security from foreign enemies.[55]

> The closer we are to the critical historical moment of realizing the great rejuvenation of the Chinese nation, the more we need to

[51] *See China's Peaceful Development*, STATE COUNCIL INFO. OFF. CHINA (Sep. 6, 2011), http://www.scio.gov.cn/zfbps/ndhf/2011n/202207/t20220704_130065.html.
[52] INST. PARTY HIST. & LITERATURE CENT. COMM. COMMUNIST PARTY CHINA, EXCERPTS OF XI JINPING'S DISCUSSIONS RELATED TO THE COMPREHENSIVE NATIONAL SECURITY CONCEPT 5 (2018).
[53] *See National Security Law*, CHINA L. TRANSLATE (July 1, 2015), https://www.chinalawtranslate.com/en/2015nsl (discussing the preservation of national security).
[54] *See Export Control Law of the People's Republic of China*, art. 3, CHINA L. TRANSLATE (Oct. 19, 2020), https://www.chinalawtranslate.com/en/export-control/. *See also* Shen Wei & Zhang Beibei, *China's Anti-Sanctions Regime: An Initial Assessment*, *in* ECONOMIC SANCTIONS UNDER INTERNATIONAL LAW 191, 195-200 (P. Sean Morris ed., Routledge 2024) (discussing China's anti-sanctions regime and raising the possibility of what this article describes as an offensive deployment of national-security based measures).
[55] *Zhongyang Guojia Anquan Weiyuanhui Di Yi Ci Huiyi Zhaokai Xi Jinping Fabiao Zhongyao Jianghua* (*中央国家安全委员会第一次会议召开 习近平发表重要讲话*) [*The First Meeting of the Central National Security Commission Held; Xi Jinping Delivered an Important Speech*], STATE COUNCIL (Apr. 15, 2014), http://www.gov.cn/xinwen/2014-04/15/content_2659641.htm.

臺灣大學學術期刊資料庫

> make increasing our sense of urgency and be prepared for danger in times of peace as a major principle of governing the party and the country, and the more we need to take national security, which is the foundation of stability and stability, as a top priority. Hold on tight. Hold on tight. *This requires us to boldly innovate the concept of national security*, clearly define the road orientation to achieve national security, *systematically plan new ideas for promoting national security work, and actively explore new ways to safeguard national sovereignty, security and development interests*.[56]

The emphasis on "boldly innovating", planning "new ways", and exploring "new ideas", illustrate the systemic focus on expanding China's security conceptualization.

Furthermore, it is noteworthy that China uses "national security" and "national interests" interchangeably which also can be interpreted as a broader understanding than classical notions of national security. For example, in discussing sanctions against U.S. defense companies selling weapons to Taiwan, the term "national interests" was used which is arguably an expansive conceptualization of national security supporting the deployment of measures either defensively or offensively.[57] Since the sanctions are linked to arms sales, the deployment arguably comports with the classical notions of security (i.e., China opines this is an internal domestic matter) although Taiwan has a different perspective. The U.S. view is that any armed conflict initiated by China aimed at reunification would constitute a violation of the principle of peaceful resolution of disputes which violates the spirit, if not principles, of international law and the sanctions therefore would arguably constitute an offensive deployment.

Demonstrating a regulatory measure that could comport with a defensive or offensive deployment (see *infra* Part II.B.2(b) noting this may also manifest a potentially offensive conceptualization), in March 2025 the U.S. financial titan Blackrock, and its investor consortium, entered into a large transaction with an HKSAR entity, CK Hutchison, for the acquisition of a substantial number of ports including ports located in Panama. The proposed deal would provide Blackrock and its investor group with nearly 10% of

---

[56] Gao Zugui (高祖贵), *Zhongguo Guojia Anquan Lilun Yu Shijian De Zhongda Chuangxin* (*中国国家安全理论与实践的重大创新*) [*Major Innovations in China's National Security Theory and Practice, Research Center for Theoretical System of Socialism with Chinese Characteristics*], QSTHEORY (Feb. 28, 2017), https://www.qstheory.cn/dukan/qs/2017-02/28/c_1120536834.htm (emphasis added).

[57] *Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on October 26, 2020*, MINISTRY OF FOREIGN AFF. PEOPLE'S REPUBLIC OF CHINA (Oct. 26, 2020), https://www.fmprc.gov.cn/eng./xw/fyrbt/lxjzh/202405/t20240530_11346908.html (sanctions will be imposed "*in order to uphold national interests*.").

臺灣大學學術期刊資料庫

global port ownership. China's regulators are reportedly (as this is paper is being finalized) still investigating whether there are potentially harmful effects on China's economy.[58] Measures to defend shipping and port access and prevent harm to domestic economic interests can be understood as defensive in nature (but see below raising the possibility the regulatory investigation is indicative of an offensive measure).

(b) Offensive Conceptualization and Deployment — China's restrictions on rare minerals exports provides an illustration of a potentially offensive deployment or an example of economic coercion. While framed as a measure to ensure domestic supply, the Western consensus is that restrictions were a response to measures against China such as tariffs and restrictions related to investment and trade. The imposition of export controls on critical minerals suggests that China, if empowered to do so, would also engage in the same "denial of capabilities" strategy which aligns with Paramount Leader Xi's recognition that dominance in technology is essential.[59]

Moreover, anecdotal evidence can be inferred that China is incorporating an offensive deployment based upon its regulatory practices. In the context of competition law, and similar to other nations, even when acquisitions are not motivated by profit-seeking in the domestic Chinese market,[60] parties are obligated to file for Chinese regulatory approval due to the potential impact on the Chinese economy.[61] Chinese regulatory enforcement suggests offensive deployments of policy measures in the name of national security.

> [T]here had been instances where the decisions were based on factors that are generally considered irrelevant by international standards. In 2009, for example, [China's] MOFCOM blocked

---

[58] *See* Jeffie Lam & Yuke Xie, *Will Beijing Sink Hutchison-Blackrock Ports Deal with Antitrust Probe?*, S. CHINA MORNING POST (Mar. 29, 2025, 08:00 AM), https://www.scmp.com/news/hong-kong/politics/article/3304384/how-will-beijings-anti-monopoly-probe-hutchison-blackrock-ports-deal-work (Indications that Chinese regulators will investigate anti-competitive impacts for Chinese entities and economy). An interesting question arises whether a People's Republic of China (PRC) shipping company could allege in U.S. courts that Chinese business interests (in the U.S. specifically) might be damaged by the Blackrock transaction. Under U.S. law, a foreign business can file as a private enforcer for violations of antitrust law (i.e., the deal with the Hong Kong (HK) company will be anti-competitive) if harm arises to the foreign entity's U.S. business interests.

[59] *See* Buckley, *supra* note 4 ("China [must] forge ahead in advanced technologies including artificial intelligence, biotechnology and new weapons.").

[60] For a discussion of domestic Chinese mergers and corporate defense mechanisms to thwart takeovers, see generally Robin Hui Huang & Juan Chen, *The Rise of Hostile Takeovers and Defensive Measures in China: Comparative and Empirical Perspectives*, 20(2) EUR. BUS. ORG. L. REV. 363 (2019) (Takeovers are important in China's economic development discussing takeover defenses in comparative context.).

[61] The Antimonopoly Law (AML) extends its jurisdiction to cover anticompetitive conduct outside of China that has the effect of excluding or impeding competition in the Chinese domestic market. *See generally* Wentong Zheng, *The Chinese Antitrust Paradox*, 2(2) U. CHI. BUS. L. REV. 391 (2023).

臺灣大學學術期刊資料庫

> Coca-Cola's proposed acquisition of Huiyuan Juice Group Limited, a Chinese juice manufacturer, despite the fact that Coca-Cola and Huiyuan had non-overlapping businesses and so the merger ought not to have prompted any antitrust concerns. It is widely believed that the desire to protect a famous national brand played an important role in MOFCOM's decision. Moreover, practitioners generally believe that other government agencies directly intervened in the merger review process, *resulting in MOFCOM putting conditions on merger approval for reasons unrelated to antitrust*.[62]

Indeed, China's regulatory context provides several additional potential examples of offensive deployments of measures presumably based upon national security. U.S.-based Intel announced its intention to buy Israel-based Tower Semiconductor, endeavoring to enhance Intel's contract chip-making business to better compete globally. However, the Chinese antitrust regulator refused to approve the merger and the belief is that this was based on strategic factors such as endeavoring to limit Intel's ability to produce advanced chips.[63]

This is similar to the speculation that China's refusal to approve Qualcomm's purchase of NXP Semiconductors was motivated by the same goal.[64] "By effectively blocking Qualcomm Inc.'s forty-four billion U.S. dollar acquisition of NXP Semiconductors Beijing made two points: It showed it has weapons beyond tariffs to use in its trade fight with the U.S., and it checked the advance of a powerful rival in a longer-range battle for tech supremacy."[65]

In another potential example, in September 2025, a Chinese regulator retroactively found Nvidia had violated China's competition law "when it

---

[62] *Id*. at 411. *See also* Will Feuer, *DuPont Scraps Deal to Buy Rogers After Failing to Win Regulatory Clearance*, WALL ST. J. (Nov. 2, 2022), https://www.wsj.com/articles/dupont-scraps-deal-to-buy-rogers-after-failing-to-win-regulatory-clearance-11667403740. *But see* Sandra Marco Colino, *The Internationalization of China's Foreign Direct Investment Laws*, 45(2) FORDHAM INT'L L.J. 275, 288 (2021) (plausible reasons exist to demonstrate protectionism not the proximate cause of the ruling).

[63] *See* Dan Strumpf et al., *China Torpedoes Intel's Bid to Buy Israeli Chip Maker Tower Semiconductor*, WALL ST. J. (Aug. 16, 2023), https://www.wsj.com/business/deals/intel-scraps-tower-acquisition-after-china-fails-to-approve-deal-f59dd70f ("U.S.-China technology tensions are disrupting strategic plans for some major American companies.").

[64] *See* Dan Strumpf, *Scuttled Qualcomm-NXP Deal Is a Win-Win for Beijing*, WALL ST. J. (July 26, 2018), https://www.wsj.com/articles/scuttled-qualcomm-nxp-deal-is-a-win-win-for-beijing-153260 6186 ("By failing to approve Qualcomm's purchase of Dutch chip maker NXP—thus killing the deal—Beijing slowed the San Diego-based company's expansion into new sectors, which could help its own chip companies as they strive to catch up with foreign rivals, analysts say."). *See* Colino, *supra* note 62, at 288 ("In 2018, coinciding with increased tensions in China's trade relationship with the United States, tech giant Qualcomm failed to obtain timely clearance from the SAMR for the purchase of Dutch semiconductor producer NXP").

[65] Strumpf, *supra* note 64.

臺灣大學學術期刊資料庫

acquired Mellanox Technologies, an Israeli-U.S. supplier of networking products, China's State Administration for Market Regulation (SAMR) said . . . . Beijing conditionally approved the US chipmaker's acquisition of Mellanox in 2020."[66]

The investigations and blocked deals suggest an offensive deployment of national security-based measures via regulatory enforcement to deprive the U.S. of competitive capabilities.

As noted below, perceptions of China's weaponization of trade and investment are also of serious concern to the EU and, if true, reflect an increasing willingness to deploy offensive measures.

> China under Xi has frequently resorted to offensive measures against 'misbehaving' partners, or to economic coercion. Beijing often misuses regulatory instruments . . . Beyond outright economic coercion, China often threatens retaliation against countries that go against its economic interests, even when they do so in line with international rules.[67]

Furthermore, as noted above, Chinese regulators are reviewing the Blackrock-CK Hutchison deal. Preventing a corporation based in a competitor jurisdiction from obtaining a 10% global port ownership interest could exemplify an offensive deployment.

Finally, pursuant to China's political-economic governance model, domestic Chinese corporations constitute national security assets.[68] Subsidies and preferential treatment for strategic sectors and national champions constitute integral aspects of China's industrial policy. Leveraging domestic Chinese corporations to promote national interests by undercutting global competition to dominate markets, compelling businesses to cooperate with the government, or promote ideology might also constitute an offensive deployment of national security.

3. EU Conceptualization of National Security — Russia's invasion of Ukraine, China's refusal to condemn Russia for invading Ukraine, and instead

---

[66] Zijing Wu & Cheng Leng, *China Says Nvidia Violated Antitrust Law When It Bought Mellanox*, FIN. TIMES (Sep. 15, 2025), https://www.ft.com/content/fa7a2e35-df03-45a1-bd0b-3f7207a7d84b.

[67] CHIMITS ET AL., *supra* note 14, at 12. *See also* Chien-Huei Wu & Mao-Wei Lo, *The Threat of China's Economic Coercion*, *in* SWITCHING DIPLOMATIC RECOGNITION BETWEEN TAIWAN AND CHINA 14, 14-49 (2024) (discussing weaponizing economic dependencies to exert pressure regarding recognition of Taiwan).

[68] Qingjiang Kong, *Emerging Rules in International Investment Instruments and China's Reform of State-Owned Enterprises*, 3(1) CHINESE J. GLOB. GOVERNANCE 57, 73 (2017) ("SOEs are exactly established to execute national strategic goals."). However, share ownership is not determinative of control so state-linked entities are pervasive. *See* Ru Ding, '*Public Body' or Not: Chinese State-Owned Enterprises,* 48(1) J. WORLD TRADE 167, 179 (2014) (control not defined only by majority share ownership). Moreover, all economic actors even ostensibly private ones are subject to Party direction and the promotion of state interests. *See supra* notes 47-48 and accompanying text.

臺灣大學學術期刊資料庫

offering "friendship without limits", is of particular concern to European nations strengthening the perception that China constitutes a national security risk to the EU.[69] China is perceived be endeavoring to transform, if not overturn, the existing global governance order in which the EU participates.[70] Increasingly, EU policymakers classify China as a systemic rival that employs economic coercion and currency manipulation to advance strategic goals which are inimical to EU interests.[71] The labeling of China as acting counter to Western values, a currency manipulator, and an ally of Russia, implicates a wide-array of alleged threats encompassing economic, technological and ideological power spheres.

In response, European nations are taking measures against Chinese economic actors to address national security threats.[72] The EUs expansion in defining security is evident in stricter investment screening, tariffs, as well as decisions imposing restrictions in an array of commercial contexts that are alleged to pose security risks to the EU.[73] Data is of paramount EU concern; social media, 5G, EVs and AI all generate a large amount of data and are potential conduits of collection and transfer which correlates with measures against Huawei, tariff imposition on Chinese EVs, and EU AI regulations.[74]

(a) Defensive Expansion and Deployment — Conceptualizing security beyond defending territorial integrity, the EU places great emphasis on economic security and promotes incorporating economic defense into national security. With its Economic Security Strategy, the European Commission has specifically linked overall EU security with economic vitality.[75] Trade with China is now viewed as a significant risk particularly the potentially adverse impact on EU industrial capacity.[76] Measures against

[69] *See* GOV'T OFF. OF SWED., *supra* note 11, at 19 (noting "China's deepening partnership with Russia . . . China has been moving in an increasingly totalitarian direction.").
[70] FED. GOV'T, *supra* note 11, at 23 (China endeavoring to re-shape the global order and acting counter to Western values).
[71] *See* Jessie Yin, *Germany Is Finally Waking Up to the China Challenge. And Beijing Is Gearing Up to Respond*, ATLANTIC COUNCIL (July 20, 2026), https://www.atlanticcouncil.org/blogs/econographics/germany-is-finally-waking-up-to-the-china-challenge-and-beijing-is-gearing-up-to-respond/ (German Chancellor Merz arguing that EU-China trade was unfair because China "artificially manipulates its currency").
[72] Volpicelli & Deutsch, *supra* note 13 ("The European Commission is exploring ways to force European Union member states to phase out Huawei Technologies Co. and ZTE Corp. from their telecommunications networks, according to people familiar with the matter.").
[73] Martin Ströder, *Keine chinesischen Komponenten: Bund schließt Verträge mit Netzbetreibern* [*No Chinese Components: Federal Government Concludes Contracts with Network Operators*], JUVE (July 15, 2024), https://www.juve.de/deals/keine-chinesischen-komponenten-bund-schliesst-vertraege-mit-netzbetreibern/.
[74] Friso Bostoen, *Europe's DMA: A Protectionist Weapon?*, CEPA (Mar. 20, 2024), https://cepa.org/article/europes-dma-a-protectionist-weapon/. Data represents complex national security risks. *See generally* Zhang, *supra* note 26 (discussing need to establish standards to avoid abusive regulation).
[75] CHIMITS ET AL., *supra* note 14.
[76] Fredrik Erixon et al., *Securing Europe's Future: Strengthening ICT Competitiveness for Economic and National Security*, EUR. CTR. FOR INT'L POL. ECON. (Dec. 2024), https://ecipe.org/publications/eu-ict-competitiveness-for-economic-national-security/.

臺灣大學學術期刊資料庫

Chinese economic actors to defend EU industrial capacity and supply chain resiliency reflect a defensive expansion.

Technology also constitutes a vital EU national security interest. For example, claims abound alleging Chinese EVs constitute a national security threat due to privacy, cybersecurity, and embedded kill switches:

> Who controls these data flows and software updates is a far from trivial question, the answers to which encroach on matters of national security, cybersecurity, and individual privacy. For these reasons, policymakers have to treat these new vehicles differently from cars as we once knew them. It is concerning that they are yet to fully do so. [77]

Data transfer is of particular concern to EU regulators [78] and is conceptualized as a fundamental right in the EU (and as a national security asset in China, and a financial asset in the U.S. although it is increasingly recognized as a security asset as well). [79] Measures preventing foreign governmental access to EU citizens' data and privacy is defensive in nature.

With respect to ideology, China is perceived to be endeavoring to overturn the existing Western governance order as well as notions of rights and values. In recent decades EU, U.S., and Japanese technological leadership has ensured that these values constituted an integral part of technology.[80] China's refusal to condemn Russia for invading Ukraine is of particular concern to European nations ensconcing perceptions that China is endeavoring to re-shape global governance and acts contrary to Western values.[81] EU Members perceive China moving away from potential reform and embracing a more autocratic world constituting a national security threat.[82] While rights and values do not align with traditional notions of

---

[77] Janka Oertel, *Security Recall: The Risk of Chinese Electric Vehicles in Europe*, EUR. COUNCIL ON FOREIGN REL. (Jan. 25, 2024), https://ecfr.eu/article/security-recall-the-risk-of-chinese-electric-vehicles-in-europe/ ("Chinese brands are leading the way – and pose serious security issues which the European Union and member state governments must quickly address."). *See also* Michael Read, *UK Finds Possible 'Kill Switch' in Chinese Bus Brand Used in Australia*, AUSTL. FIN. REV. (Jan. 19, 2026) https://www.afr.com/policy/foreign-affairs/uk-finds-possible-kill-switch-in-chinese-bus-brand-used-in-australia-20260119-p5nv10 (kill switches on Chinese buses found in United Kingdom).

[78] Bostoen, *supra* note 74.

[79] For an interesting comparison of various conceptualizations of data between the U.S., EU, and China, see generally Raymond Yang Gao, *A Battle of the Big Three?—Competing Conceptualizations of Personal Data Shaping Transnational Data Flows*, 22(4) CHINESE J. INT'L L. 707 (2023).

[80] *See* Anton Malkin, *The Made in China Challenge to US Structural Power: Industrial Policy, Intellectual Property and Multinational Corporations*, 29(2) REV. INT'L POL. ECON. 538, 557 (2020) ("Over the past half-century, technological standard setting was dominated by the U.S., the EU and Japan".).

[81] *See* FED, GOV'T, *supra* note 11, at 23.

[82] Sweden's 2024 National Security Strategy specifically linking China's alliance with Russia as constituting a national security threat to Sweden. *See* GOV'T OFF. OF SWED., *supra* note 11.

臺灣大學學術期刊資料庫

national security, as noted above, given the risks embedded in social media manipulation, measures that seek to protect EU citizens from ideological propaganda or manipulated information would constitute a defensive expansion.

The EUs defensive expansion to defend EU capabilities in the realms of economic, technological, and ideological power include: rules related to foreign ownership of strategic businesses, enhanced screening of inbound investment, tariffs, AI regulations, and anti-subsidy probes on Chinese EVs all manifest a defensive deployment of measures.[83] In another example, the intent of the European Chips Act is for "Europe [to] reinforce its capabilities in semiconductors to ensure future competitiveness and maintain its technological leadership and security of supply".[84] Thus, the law endeavors to lessen non-EU control over chips to bolster European economic resiliency and strength as opposed to weakening China's chip eco-system. EU resilience and de-risking from foreign dependency are measures that are defensive in nature.

In another example of a defensive deployment, China's Huawei is increasingly viewed as a threat capable of greatly damaging the EU.[85] Huawei has been the subject of restrictions and bans[86] as well as corruption probes in the EU.[87] The EU (and U.S.) even warn third countries over alleged risks to national security and foreign investment following 5G rollouts that would enable participation by Huawei.[88] Measures with respect to Huawei's operations in the EU constitute defensive deployments of national security

[83] Jacob Gunter & Grzegorz Stec, *EV Tariffs + EU-China Policy at an Inflection Point + Exports to China*, MERCATOR INST. FOR CHINA STUD. (Oct. 10, 2025), https://merics.org/en/merics-briefs/ev-tariffs-eu-china-policy-inflection-point-exports-china (EU probe led to imposition of tariffs); Gisela Grieger, *EU Anti-Subsidy Probe into Electric Vehicle Imports from China*, EUR. PARL. RSCH. SERV. (Oct. 18, 2023), https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2023)754553.

[84] CHIPS ACT | UPDATES, COMPLIANCE, https://www.european-chips-act.com/ (last visited Feb. 21, 2026).

[85] *See Speech by Commissioner Breton on the Cybersecurity of 5G Networks*, EUR. COMM'N (June 15, 2023), https://ec.europa.eu/commission/presscorner/detail/en/speech_23_3314 ("The situation with 5G should be no different: we cannot afford to maintain critical dependencies that could become a 'weapon' against our interests.").

[86] An EU-wide ban is under consideration. *See* Sam Clark, *EU's Huawei Hardliners Get Top Court Backing*, POLITICO (Mar. 19, 2026) https://www.politico.eu/article/eu-huawei-hardliners-get-top-court-backing/ (discussing the possible shift from a suggestion to ban Huawei to mandatory adherence). Individual nations have already acted with respect to Huawei. For example, in July 2024, Germany ordered the removal of Huawei infrastructure from German communications infrastructure reflecting Germany's greater focus on defending against national security threats. *See* Ströder, *supra* note 73; Hans von der Burchard et al., *Germany Goes Soft on China, Dragging out Huawei Ban Until 2029*, POLITICO (July 10, 2024), https://www.politico.eu/article/germany-china-huawei-ban-2029-5g-networks-government-greens-lawmaker-4g-strand/. *See generally* FED. GOV'T, *supra* note 11.

[87] *Huawei Bribery Scandal: What We Know So Far*, POLITICO (Mar. 17, 2025), https://www.politico.eu/article/huawei-bribery-scandal-eu-chinese-tech-lobby-money-lobbying/.

[88] *EU, US Warn Malaysia of Security Risk in Huawei's Bid for 5G Role, Financial Times Reports*, REUTERS (May 2, 2023), https://www.reuters.com/technology/eu-us-warn-malaysia-national-security-risk-huaweis-bid-5g-role-ft-2023-05-02/.

臺灣大學學術期刊資料庫

as the goals are to protect domestic data and privacy. A more nuanced issue arises when the threat of withholding security cooperation exists, which may, depending upon the circumstances, constitute an effort to coerce compliance implicating an offensive dimension.[89] Of course, if the security threat is legitimate, one would expect allies to warn each other thereby potentially justifying the conduct as defensive in nature.

(b) Offensive Expansion and Deployment — EU national security now includes measures to encourage investments, developing new technologies, and "*fostering the skills needed to sustain Europe's technological edge*."[90] "Retaining an edge" might be understood as retention of dominance, similar to the U.S. understanding of maintaining a lead, if not in fact as big a lead as possible.

> [The EU] approach has largely been to "de-risk" relations with countries like China, by trying to create alternative sources of rare earth magnets, for example, a sector that Beijing dominates. However, alongside this, the EU must ensure it stays ahead in specific technologies where it still has a lead, to provide Brussels with clout when dealing with rival powers. Europe should "maintain and increase other countries' dependencies on the EU for certain key technologies".[91]

The EU's definition of security is arguably now linked to "relative advantage" as a justification for national security grounded measures reflecting a manifestation of offensive expansion. The EU is also considering an outbound rule which would confirm the trend and would constitute another illustration of an offensive national security-based deployment.[92]

---

[89] Charlotte Jee, *The US Threatens to Stop Sharing Intelligence with Allies If They Use Huawei*, MIT TECH. REV. (Feb. 22, 2019), https://www.technologyreview.com/2019/02/22/66068/the-us-threatens-to-stop-sharing-intelligence-with-allies-if-they-use-huawei/ (Allied use of Huawei risks cutting off security cooperation).

[90] Directorate-General for Communication, *Commission Takes Steps to Modernise European Defence and Improve Military Mobility*, EUR. COMM'N (Nov. 19, 2025), https://commission.europa.eu/news-and-media/news/commission-takes-steps-modernise-european-defence-and-improve-military-mobility-2025-11-19_en (emphasis added).

[91] David Matthews, *Europe Needs to Hone Its "Technological Edge" in Areas Where It Leads, Think Tank Fellows Say*, SCI. BUS. (Sep. 19, 2023), https://sciencebusiness.net/news/sovereignty/europe-needs-hone-its-technological-edge-areas-where-it-leads-think-tank-fellows ("The EU must retain its lead in key parts of technology supply chains as a way of gaining geopolitical leverage over other powers like China, according to a new analysis by the European Council on Foreign Relations (ECFR).").

[92] *Commission Calls on Member States to Review Outbound Investments and Assess Risks to Economic Security*, EUR. COMM'N (Jan. 15, 2025), https://ec.europa.eu/commission/presscorner/detail/en/ip_25_261 ("The Recommendation applies to three technology areas of strategic importance as well as the highest risk – semiconductors, artificial intelligence and quantum technologies – and calls on Member States to assess risks to economic security potentially arising from such transactions.").

臺灣大學學術期刊資料庫

Accordingly, the EU is perhaps militating towards more offensive national security deployments.

III. DEFENSIVE AND OFFENSIVE CONCEPTUALIZATION OF SECURITY IN THE CONTEXT OF THE CHINA-U.S. RIVALRY AND FRONTIER TECHNOLOGIES

A. China-U.S. Rivalry

While China's Paramount Leader Xi denies Chinese regional or global ambitions, history and geopolitical realism establish that every nation so empowered, at a minimum, strives to be the regional hegemon, if not exercise dominion globally. Thus logically, China will likely endeavor to leverage its strengths and ascend to the top of the global order. Indeed, the evidence suggests China has already embarked on this course. This is not a critique of China, any nation so empowered would seek to ascend and supplant the existing hegemon. Unsurprisingly, as any hegemonic power would respond when being challenged, retaining U.S. global supremacy constitutes a core U.S. national security interest. Accordingly, the U.S. is endeavoring to leverage its combined economic, technological, and ideological power to both defend these spheres of power, and to contain, reverse, and ultimately weaken China to the degree it no longer poses a challenge to U.S. global hegemony. If the roles were reversed, it is doubtful China would act any differently and would likely also seek to retain global dominance.

An interesting question arises whether Chinese condemnations of U.S export controls and other manifestations of offensive deployments constitute fair criticism. Perhaps an offensive dimension of security measures would be a Chinese policy if empowered to impose such deployments. As China has generally lagged U.S. capabilities in the past, an offensive investment or trade measure would have been difficult or impossible to implement and strategically self-defeating. Therefore, it may be unfair to unduly critique U.S. policy as a comparison with China is unavailable. Indeed, there is no reason to believe that such offensive policies would not be implemented by China to limit U.S. capabilities if empowered to do so and the strategic timing was right. China's export restrictions on rare minerals [93] and regulatory policies [94] suggest that China would also engage in the same

[93] Jon Emont & Raffaele Huang, *China Hatches Plan to Keep U.S. Military from Getting Its Rare-Earth Magnets*, WALL ST. J. (Nov. 10, 2025), https://www.wsj.com/world/china/china-hatches-plan-to-keep-u-s-military-from-getting-its-rare-earth-magnets-f349ee65 ("China plans to ease the flow of rare earths and other restricted materials to the U.S. by designing a system that will exclude companies with ties to the U.S. military while fast-tracking export approvals for other firms, according to people familiar with the plan.") If accurate, an export restriction on U.S. companies and military applicability would militate a finding the measure is defensive.

[94] *See supra* notes 62-66 and accompanying text.

臺灣大學學術期刊資料庫

"denial of capability" strategy and offensive deployment of national security-based measures.

B. Tribunals Should Evaluate Security-Based Measures Distinguishing Between Defensive and Offensive Conceptualizations

International investment law and the legal framework of the General Agreement on Tariffs and Trade (hereinafter "GATT")/WTO enable legitimate governmental measures aimed at securing and protecting the national bastion through the security exception. However, to withstand scrutiny, invoking the exception must be legitimate; i.e., made in good-faith, necessary, and proportional.[95] Thus, given the expanded conceptualization of security, states should be empowered to enact legitimate measures to defend a growing list of non-kinetic threats such as retaining industrial capacity, protecting domestic financial systems, securing data center networks, and ensuring the citizens are not subjected to ideological manipulation.

However, an expansive conceptualization may incentivize improper claims of national security. Protectionism or a motivation to harm another nation might be the real intent of a security-based measure. Moreover, additional dimensions of complexity arise from the fact that principles such as "necessity" and "proportionality" are more difficult to ascertain in an era of embedded backdoors and kill switches, let alone military applications for AI and quantum. In evaluating whether the measure was necessary, it might be an insurmountable challenge for a state to establish that there is an immediate danger of a grave peril without a less restrictive measure available. How can grave and imminent threats be proven in the context of drones, hackable traffic cameras, embedded virus in infrastructure such as power stations, and kill switches in EVs, which might be dormant threats but can be "weaponized" or contain embedded features such as software updates allowing these devices to be remotely and instantly activated thus presenting a potential immediate and grave peril *in the future*. How can a state know that its citizens are being unduly influenced by algorithmic manipulated

[95] *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (International Court of Justice (ICJ) considered the U.S. use of force based on national security interests emphasizing the need for good-faith, necessity and proportionality, when invoking national security measures); *Russia — Traffic in Transit* Panel Report, *supra* note 20, at ¶ 7.5.7 (ruling that Russia's invocation of the national security exception was justified during a "time of war or other emergency in international relations" in the context of armed conflict); Panel Report, *United States — Certain Measures on Steel and Aluminium Products*, WTO Doc. WT/DS551/R (July 11, 2019) (holding purely economic concerns about industrial capacity failed to satisfy the requirements of legitimate national security invocation as these do not constitute a valid "emergency in international relations" and were therefore a violation of WTO obligations).

臺灣大學學術期刊資料庫

propaganda? By the time its citizens have been sufficiently demoralized or bereft of critical thinking skills it might be too late. Similarly, the dangers of de-industrialization and the development of chokepoints might be a slow and intentionally hidden process conducted by an adversary. Accordingly, the threat environment is simply not calculable in terms of the principle of necessity or of a proportionate response. Therefore, the traditional understandings of "necessity" and "proportionality" do not comport with advancements, capabilities, and developments with respect to economic, technological, and ideological power.

The advent of new abilities to weaken competitor states will substantially complicate the already arduous task of evaluating the legitimacy of investment and trade national-security based measures. Both nations and tribunals have few if any ground rules let alone "best practices" to navigate the new realities of economic, technological, and ideological power being used to attack and weaken another sovereign.[96] This article opines measures designed to protect these power spheres should be conceptualized as defensive in nature and understood as legitimate presuming good faith is used in deploying the measures. In contrast, the rise in broad-based export controls, outbound investment restrictions and other measures designed to thwart a competitor's development are manifestations of offensive measures. The offensive dimension of defining national security, deployed to maintain dominance and contain a rival, are arguably less legitimate.

Accordingly, measures evincing a defensive dimension should be easier for a government to justify when using the national security rationale in the context of international economic law. More problematic is the offensive prong which consists of moving from pure defense to maintaining dominance and depriving a competitor of capabilities. Offensive deployment to promote strategic deprivation of a competitor occurs through policies such as cutting off foundational inputs, e.g., lithography machines, chips, or rare Earth minerals. Export controls can be deployed to prevent a rival from getting the specific inputs needed to build frontier technologies thus constituting an offensive coercive choke point.[97] Such measures are intentionally designed to restrict products and services and prevent the ability to innovate and compete and are therefore more problematic in terms of justification. Endeavoring to create a long-term if not unconquerable lead by exercising control over key inputs prevents a competitor not merely from

[96] Moreover, rules establishing the existing governance order did not contemplate transformative technologies such as AI. Tsai-fang Chen, *AI, Job Displacement, and the WTO: Identifying Legal Gaps and Charting a Worker-Centered Path*, YALE J. INT'L L. (Nov. 10, 2025), https://yjil.yale.edu/posts/2025-11-10-ai-job-displacement-and-the-wto-identifying-legal-gaps-and-charting-a-worker (WTO framework not designed to address those dynamics). *See also* Chen, *supra* note 26 (WTO did not contemplate the transformative impacts of AI).

[97] Coercion might certainly be relevant to an economic tribunal. *See, e.g.*, *CME Czech Republic B.V. v. The Czech Republic*, Final Award, ¶ 497 (Mar. 14, 2003), https://jusmundi.com/en/document/decision/en-cme-czech-republic-b-v-v-the-czech-republic-final-award-friday-14th-march-2003.

臺灣大學學術期刊資料庫

ascending but might result in weakening the competitor and degrading their competitive power. The posture is fundamentally different than defensive deployment and reflects a proactive policy rather than merely responding to threats.

However, dividing deployments of measures based on defensive and offensive may not always be simple for two reasons. First, the quantum geoeconomics framework raises the possibility, if not likelihood, that measures may contain elements of both. Similar to a wave function, measures might simultaneously carry both cooperative and competitive probabilities.[98]

In response to a challenge of a measure reflective of an offensive conceptualization, a government can argue the measure is more about risk management and de-risking rather than market-share gain, control, and/or deprivation of competitive opportunities. States can claim that tribunals should recognize today's holistic strategic defensive framework. Various capabilities are interconnected and to avoid domestic degradation, an ostensibly "offensive" measure advancing capability containment is in fact a legitimate "defensive" measure. Accordingly, simply because anti-competitive spillover effect exists should not automatically render a measure unlawful. In one example, with respect to rare earth restrictions, two separate layers of probabilities exist: defensive dimensions cover resource depletion risks and domestic resilience goals; offensive dimensions to ensure global market dominance and weaken a rival.

Second, offensive measures may fall within the ambit of legitimate national defense since emerging technologies have powerful military applications, and therefore, first-mover advantage and dominance are important.[99] Indeed, offensive measures in the context of the China-U.S. rivalry are understandable as both nations believe that a future military conflict is possible and might potentially be understood as anticipatory self-defense.[100] Offensive deployment might therefore constitute legitimate

---

[98] *See* Li, *Quantizing Geoeconomics*, *supra* note 26.

[99] *See, e.g.*, Ali Rogan & Harry Zahn, *How Militaries Are Using Artificial Intelligence on and off the Battlefield*, PBS NEWS WEEKEND (July 9, 2023), https://www.pbs.org/newshour/show/how-militaries-are-using-artificial-intelligence-on-and-off-the-battlefield (explaining the impact of artificial intelligence on modern warfare).

[100] The doctrine of anticipatory self-defense permits a state to deploy measures (traditionally military force) preemptively against an imminent armed attack before it actually occurs. The principle of anticipatory self-defense is controversial and complex but may be legitimate under international law depending on the circumstances. Sienho Yee, *The Potential Impact of the Possible US Responses to the 9–11 Atrocities on the Law Regarding the Use of Force and Self-Defence*, 1(1) CHINESE J. INT'L L. 287, 292-93 (2002) (noting the dilemma and complexity of anticipatory defense but also noting that nations need not be sitting ducks especially in an age of nuclear and biological weapons). *See also* Peter Hilpold, *The Fight Against Terrorism and SC Resolution 2249 (2015): Towards a More Hobbesian or a More Kantian International Society?*, 55(4) IND. J. INT'L L. 535 (2015) (discussing anticipatory defense in the context of terrorism); Peter Hilpold, *Intervening in Iran: Tinkering About Just War, Humanitarian Intervention and Second-Best Solutions for Fundamental Challenges in a Less Than Perfect International Order*, SIDIBLOG (Apr. 1, 2026), http://www.sidiblog.org/2026/04/01/intervening-in-iran-tinkering-about-just-war-humanitarian-intervention-and-second-best-solu

臺灣大學學術期刊資料庫

"anticipatory defense", i.e., measures against an expected conflict.[101] While a claim that preventing an adversary developing advanced capabilities linked to military power clearly comports with historical notions of security, an important question is whether "anticipatory conflict" equates with legitimate defense to a possible future military threat.[102] Anticipatory defense is a complex legal issue and the classical limitation is that anticipatory measures be limited to responding to an imminent threat. However, emerging technologies raise the implication that such limitation may not be as justifiable as in prior eras. In the era of AI and other frontier technologies, preventing an adversary the means to build military-grade AI systems or launch solid-fueled ballistic missiles (let alone nuclear weapons) which are undetectable until immediately before launch (or not until airborne) may, depending on the facts, constitute legitimate anticipatory defensive measures.[103] Another question is the applicability of the doctrine in non-kinetic contexts although given the new pathways to weaken an adversary, and in particular dual-use technologies, the doctrine might very well be applicable to measures relating to economic, technological, and ideological power.

Yet legitimizing measures as anticipatory defense constitutes a slippery slope since denying a competitor's ability to compete is appealing from an

---

tions-for-fundamental-challenges-in-a-less-than-perfect-international-order/ (discussing anticipatory defense in the context of the U.S.-Israeli joint strikes on Iranian nuclear facilities). Today, frontier technologies such as AI perhaps further legitimize anticipatory self-defense. Moreover, nations can be vulnerable to attacks on their infrastructure. *See* Paul B. Stephan, *Big Data as a National Security Issue*, 2024 U. CHI. LEGAL F., 307, 309 (2024)

> Civil aviation, a wide array of public services, the financial system, oil and gas pipelines, and communications networks become more vulnerable. The United States, as one of the most online states in the world, faces grave risks from adversary exploits fueled by big data. . . . Both the United States and its adversaries invade each other's big data both for espionage and to damage or destroy big-data-driven capabilities. All states that have big data consider these assets as something to be defended and attacked.

This vulnerability raises the incentive to preempt such an attack through anticipatory self-defense.

[101] *See generally* Leo Van den hole, *Anticipatory Self-Defence Under International Law*, 19(1) AM. U. INT'L L. REV. 69 (2003).

[102] *See generally* David A. Sadoff, *A Question of Determinacy: The Legal Status of Anticipatory Self-Defense*, 40(2) GEO. J. INT'L L. 523 (2009) (discussing and contrasting the international legal discourse and contrasting the possible justification of "imminent attack" with a more long-term defense).

[103] *See* Yee, *supra* note 100, at 292-93 ("If some forms of anticipatory self-defence are legitimate, then the critical question is how much in advance preemptive measures may be taken. Such a question is not susceptible of precise treatment, and may need to be within the appreciation of the acting State. That can be scary. And yet no State should be required to be a sitting duck waiting for an attack conducted with modern weaponry of a nuclear or biotech nature.") Of course, anticipatory self-defense carries a serious risk. If a state claims it is acting in anticipatory self-defense, but in reality, is launching an offensive strike, the entire system of international law collapses perhaps with catastrophic consequences. However, given the Fourth Revolution technologies that were not available until recently, the legitimacy of anticipatory self-defense is potentially more valid today.

臺灣大學學術期刊資料庫

economic perspective and thus invoking national security might be used as an excuse to block legitimate competition.[104] Policies encompassing an offensive conceptualization may in fact be a cover for protecting domestic economic entities and denying the competitor nations' businesses the ability to compete. In terms of evaluating measures which states may argue constitute legitimate anticipatory defense, tribunals should focus on whether the state can establish: (1) verifiable facts as opposed to conjecture; (2) whether procedurally, the state's findings comport with transparency and good faith; and (3) whether the anti-competitive impact constitute the primary motivation or merely an ancillary impact.

In sum, the question of whether a state's invocation of national security is legitimate is a complicated issue. To help navigate resolving the legitimacy of a measure, courts and tribunals should distinguish between defensive and offensive deployments. Offensive deployments should be reviewed more strictly, and consequently, more difficult to justify under international economic law than a defensive measure as an offensive deployment might be protectionist or constitute economic coercion.[105]

C. Recent Arbitral Rulings in the Context of Defensive or Offensive Measures

1. Huawei v. Sweden (BIT) (Pending) — Huawei has filed a claim against Sweden under the China–Sweden BIT following the ban on Huawei 5G equipment. To justify the measure, Sweden has invoked the national security exception to the BIT while Huawei argues the measure constitutes an impermissible discriminatory measure that violates the "Fair and Equitable Treatment" guarantee contained in the BIT. The ruling of a Swedish court upholding the decision to ban Huawei equipment noted that the decision was based on the Swedish government's determination that Chinese citizens, companies, and organizations, are obligated to cooperate, support, and assist Chinese intelligence and security services. The court held that the decision to ban Huawei is based on a:

---

[104] *See* Gao, *supra* note 79, at 773 ("with the ever-narrowing gap in economic clout and technological strength between these two superpowers, the US has increasingly framed China as a strategic competitor and foreign adversary, which poses growing threats to its dominance, leadership, and security interests.").

[105] *See generally* Sarah Bauerle Danzman, *A Tool Is Not a Strategy: Technology Security Amidst Contested Global Orders*, 28(2) J. INT'L ECON. L. 302 (2025) (noting the complexity of investment and trade issues in the context of coercion. One can argue such measures are deleterious and harmful to global governance but one can also argue that some measures are in fact useful to strengthen a liberal economic order). For an interesting international law perspective, see generally Sienho Yee, *Unilateral Sanctions: Kind and Degree; Long-Arm and Strong-Arm Jurisdiction; Real Intent and "Could-Be" Intent*, 20(4) CHINESE J. INT'L L. 817 (2021) (discussing unilateral sanctions as a potential strong-arm coercive measure).

臺灣大學學術期刊資料庫

> real, current, and sufficiently serious threat against the national security of Sweden. The investigation [by the authority] shows that China already today conducts spying and other security-threatening activities against Sweden, among others, and that the Chinese state could use Huawei to carry out such safety-threatening activities. Cyberattacks also now already occur and a threat against central parts of Sweden's infrastructure must be considered such a serious threat that the restrictions in this case are permissible. It can therefore be assumed that products from Huawei in the 5G network may cause harm to Sweden's security.[106]

The *Huawei v. Sweden* arbitration suggests that the technological context—specifically the "unverifiable" nature of 5G backdoors—will compel tribunals to grapple with the re-conceptualization of security. The case will also challenge traditional principles of necessity since Sweden is not responding to an "immediate and grave" peril, but endeavoring to proactively safeguard against a potential threat. Moreover, the traditional "least restrictive alternative" test is nearly impossible to apply, as the only "safe" alternative in the view of many states is a total exclusion of the "adversary's" technology. However, in contrast to an offensive measure seeking to dominate 5G, let alone containing China's Huawei, the measure appears purely defensive as it relates directly to Sweden's domestic citizens and economy.

2. Russia Transit (WTO) — The arbitration arose out of tensions between Ukraine and Russia wherein Russia imposed measures in 2014 and 2016 banning the transit of goods through Russian territory unless an exception was authorized.[107] The Russian measures were challenged and Russia invoked Article XXI(b) of the GATT 1994 to justify its measures. The WTO panel held that under the essential security exception of Article XXI(b)(iii), the measure would need to be taken in good faith and linked to Russia's essential security.[108] Comporting with the classical understanding, the panel defined "essential security interests" as defending "the quintessential functions of the state, namely, the protection of its territory and its population from external threats, and the maintenance of law and public order internally."[109] In fact, the panel described a very classical context for security—finding that that there was, in fact, an "emergency" situation involving Ukraine and Russia at the time defined as "a situation of armed

[106] Rättsfall från Kammarrätterna [RK] [Court Cases from the Administrative Courts of Appeals], at 33, 2022 case no. 5222-21, https://perma.cc/TQ8Q-9QBM (Swed.).
[107] *Russia — Traffic in Transit* Panel Report, *supra* note 20, ¶ 7.1.
[108] *Id.* ¶ 7.132.
[109] *Id.* ¶ 7.130.

臺灣大學學術期刊資料庫

conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state."[110] The panel found that the measures were legitimate as defensive national security. The Russian measures comport with this article's description of a defensive deployment of security.

3. United States — Certain Measures on Steel and Aluminium Products — The dispute concerned the U.S. imposition of tariffs on steel and aluminum in 2018 against China and other nations (including U.S. allies).[111] The tariffs were part of an "America First" policy seeking to restructure U.S. economic policy away from multilateral partnership to a more individualistic (i.e., unilateralist) approach to trade. The U.S. justified the tariffs by invoking the essential security exception contained in Article XXI(b) of the GATT 1994 alleging the measures were "necessary for the protection of its essential security interests."[112] The WTO panel disagreed finding that U.S. "[did] not purport to identify or address the existence of an 'emergency in international relations' within the meaning of Article XXI(b)(iii) . . . ."[113] The panel rejected what was ostensibly a protectionist measure as the U.S. failed to establish a legitimate defensive invocation. Thus, the panel arguably found the tariffs were—as this article defines—an "offensive" deployment, i.e., intended to ensure U.S. global supply chain dominance.[114]

4. Global Telecom Holding v. Canada — This arbitration related to an inbound investment screening program.[115] A foreign investor (GTH) filed a claim under the Canada–Egypt BIT after Canada blocked a transaction based on national security concerns. The tribunal upheld Canada's right to use security as a justification for the measure. The ruling can be understood as a defensive deployment intended to protect a domestic Canadian industry or entity from foreign influence or control as opposed to a measure intended to dominate a competitor or deprive a foreign sovereign's capabilities.

D. Suggestions for Tribunals

For tribunals, distinguishing between a defensive deployment, i.e., safeguarding, as opposed to an offensive deployment, i.e., dominance retention or denial of capabilities, may prove helpful in evaluating measures.

---

[110] *Id.* ¶ 7.111, 7.125.

[111] *See generally* Panel Report, *United States — Certain Measures on Steel and Aluminium Products*, WTO Doc. WT/DS544/R (Dec. 9, 2022). Numerous nations filed complaints and all reports share the same holding. The Chinese panel report is used here.

[112] *Id.* ¶ 7.102.

[113] *Id.* ¶ 7.143.

[114] Yet, in the context of industrial capacity, it is not so far-fetched to envision a connection between protecting domestic industries particularly in sectors vital for military production doing so would fit a defensive understanding.

[115] *See generally* Global Telecom Holding S.A.E. v. Canada, ICSID Case No. ARB/16/16, Award, (Mar. 27, 2020).

臺灣大學學術期刊資料庫

A defensive deployment where security is used as a shield to protect against for example data transfer (as argued in the ongoing *Huawei v. Sweden* case) should be granted a wider margin of deference but tribunals should ensure the measure was made in good-faith. An offensive deployment where security is used as a sword, for example to deprive a competitor of market access, should be subject to a more rigorous analysis. Given that offensive deployments are similar to classical protectionism and economic nationalism, the measures should be less justifiable and require a more enhanced requirement of demonstrating good-faith as opposed to a defensive measure.

Yet, some offensive deployments might not necessarily constitute an impermissible measure but rather constitute legitimate anticipatory defense. Tribunals need to carefully evaluate the legitimacy of such measures rather than presumptively find them impermissible measures. By ignoring the new methods of attacking an adversary and/or failing to distinguish between defensive and offensive measures, future rulings risk either allowing offensive measures such as protectionism to flourish or striking down legitimate defensive safeguards that are legitimate given that adversarial capabilities reach far beyond traditional notions of war and armed conflict.

IV. CONCLUSION

The rules governing investment and trade were established during a far different and increasingly distant era of unfettered economic liberalization and cross-border investment. However, the strategic context has been transformed and technological advancements render concepts such as “necessity” increasingly outdated and difficult for states to establish. This article suggests defining measures in terms of either a defensive or offensive deployment would be helpful in evaluating whether the measures comport with international economic law. The article opines that measures based upon the defensive expansion are more easily justifiable if challenged than measures based on offensive understanding of security such as maintaining dominance or deprivation of the means to compete. Defensive deployments in the context of an expanded conceptualization are likely legitimate given the expansion in conceptualizing national security. In contrast, offensive deployments fail to comport with traditional notions of "security” inasmuch as these are not required to defend a nation and are similar to protectionism. Yet some offensive deployments might be legitimate particularly, but not exclusively, in the context of anticipatory self-defense.

臺灣大學學術期刊資料庫

REFERENCES

Books

GAO, HENRY & WENZHOU ZHOU (2022), BETWEEN MARKET ECONOMY AND STATE CAPITALISM: CHINA'S STATE-OWNED ENTERPRISES AND THE WORLD TRADING SYSTEM.

INSTITUTE OF PARTY HISTORY AND LITERATURE OF THE CENTRAL COMMITTEE OF THE COMMUNIST PARTY OF CHINA (2018), EXCERPTS OF XI JINPING'S DISCUSSIONS RELATED TO THE COMPREHENSIVE NATIONAL SECURITY CONCEPT.

LI, XINYUE (2026), INTERNATIONAL ECONOMIC LAW AND QUANTUM THEORY: QUANTIZING GEOECONOMICS.

STEPHAN, PAUL B. (2023), THE WORLD CRISIS AND INTERNATIONAL LAW: THE KNOWLEDGE ECONOMY AND THE BATTLE FOR THE FUTURE.

WEI, SHEN (2022), CHINA'S FOREIGN INVESTMENT LAW IN THE NEW NORMAL: FRAMING THE TRAJECTORY AND DYNAMICS.

Articles

Alschner, Wolfgang (2025), *Recalibration, Shielding and Containment: How the World Trading System De-Risks from China and the United States*, 24(4) WORLD TRADE REVIEW 498.

Bauerle Danzman, Sarah (2025), *A Tool Is Not a Strategy: Technology Security Amidst Contested Global Orders*, 28(2) JOURNAL OF INTERNATIONAL ECONOMIC LAW 302.

Bitas, Basil C. (2023), *Finding Equilibrium amid the Deep Disruption of the "Geopolitical Metaverse"*, 5(1-4) CHINA AND THE WORLD 1.

Chaisse, Julien & Georgios Dimitropoulos (2021), *Special Economic Zones in International Economic Law: Towards Unilateral Economic Law*, 24(2) JOURNAL OF INTERNATIONAL ECONOMIC LAW 229.

Chaisse, Julien & Xueji Su (2025), *Normative Realignment in Domestic Trade Barriers Procedures: Driving Unilateralism in the EU, US, and China*, 24(3) WORLD TRADE REVIEW 361.

Chaisse, Julien (2015), *Demystifying Public Security Exception and* Limitations *on Capital Movement: Hard Law, Soft Law and Sovereign Investments in the EU Internal Market*, 37(2) UNIVERSITY OF PENNSYLVANIA JOURNAL OF INTERNATIONAL LAW 583.

Chaisse, Julien (2018), *State Capitalism on the Ascent: Stress, Shock, and Adaptation of the International Law on Foreign Investment*, 27(2) MINNESOTA JOURNAL OF INTERNATIONAL LAW 339.

Chen, Tsai-fang (2017), *To Judge the "Self-Judging" Security Exception Under the GATT 1994 – A Systematic Approach*, 12(2) ASIAN JOURNAL OF WTO & INTERNATIONAL HEALTH LAW AND POLICY 311.

臺灣大學學術期刊資料庫

Chen, Tsai-fang (2026), *Forging Trade Rules in the Age of AI: The Case for Special Labor Safeguards*, *in* GEOPOLITICAL RISKS AND GEOECONOMICS IN INTERNATIONAL ECONOMIC LAW 379 (Junji Nakagawa et al. eds.).

Chen, Xuanli & Wei Shen (2025), *Disputing Supply Chain Security Legislation in the Context of WTO Rules: Litigability, Legitimacy, and Exceptionality*, 16(4) JOURNAL OF INTERNATIONAL DISPUTE SETTLEMENT 1.

Claussen, Kathleen & Timothy Meyer (2024), *Economic Security and the Separation of Powers*, 172(1) UNIVERSITY OF PENNSYLVANIA LAW REVIEW 1955.

Conley, Anna (2024), *TikTok v. Montana – State TikTok Ban Blocked by Court Based on Foreign Affairs Preemption*, 28(2) AMERICAN SOCIETY OF INTERNATIONAL LAW 1, https://asil.org/insights/volume-28-issue-2/.

Ding, Ru (2014), *'Public Body' or Not: Chinese State-Owned Enterprises*, 48(1) JOURNAL OF WORLD TRADE 167.

Ding, Ru (2020), *Interface 2.0 in Rules on State-Owned Enterprises: A Comparative Institutional Approach*, 23(3) JOURNAL OF INTERNATIONAL ECONOMIC LAW 637.

Du, Ming (2014), *China's State Capitalism and World Trade Law*, 63(2) INTERNATIONAL & COMPARATIVE LAW QUARTERLY 409.

Du, Ming (2022), *Huawei Strikes Back: Challenging National Security Decisions Before Investment Arbitral Tribunals*, 37(1) EMORY INTERNATIONAL LAW REVIEW 1.

Du, Ming (2024), *International Economic Law in the Era of Great Power Rivalry*, 57(3) VANDERBILT JOURNAL OF TRANSNATIONAL LAW 723.

Finder, Susan (forthcoming 2026), *The Evolving Relationship Between the National People's Congress and the Supreme People's Court in the Xi Jinping Era*, CHINESE LAW AND GOVERNMENT.

Gao, Raymond Yang (2023), *A Battle of the Big Three?—Competing Conceptualizations of Personal Data Shaping Transnational Data Flows*, 22(4) CHINESE JOURNAL OF INTERNATIONAL LAW 707.

Hilpold, Peter (2015), *The Fight Against Terrorism and SC Resolution 2249 (2015): Towards a More Hobbesian or a More Kantian International Society?*, 55(4) INDIAN JOURNAL OF INTERNATIONAL LAW 535.

Hsu, Locknie (2025), *Digitalization and Its Role in International Economic Law*, *in* A RESEARCH AGENDA FOR GLOBAL POWER SHIFTS AND INTERNATIONAL ECONOMIC LAW 127 (Joel Slawotsky ed.).

Huang, Ping & Anton Malkin (2025), *An Innovation Systems Approach to Decoding China's Technological Catch-Up: The Case of the Semiconductor Industry*, 33(4) INDUSTRY AND INNOVATION 431.

Huang, Robin Hui & Juan Chen (2019), *The Rise of Hostile Takeovers and Defensive Measures in China: Comparative and Empirical Perspectives*, 20(2) EUROPEAN BUSINESS ORGANIZATION LAW REVIEW 363.

臺灣大學學術期刊資料庫

Jiang, Youyou (2025), *Defining the Boundaries: WTO National Security Exceptions in the US-China Unilateral Trade Sanctions*, 18(2) JOURNAL OF EAST ASIA AND INTERNATIONAL LAW 299.

Kong, Qingjiang (2017), *Emerging Rules in International Investment Instruments and China's Reform of State-Owned Enterprises*, 3(1) THE CHINESE JOURNAL OF GLOBAL GOVERNANCE 57.

Li, Xinyue (2022), *Quantizing Geoeconomics: Emerging Geoeconomics in International Economic Law Through a Quantum Worldview*, 17(1) ASIAN JOURNAL OF WTO & INTERNATIONAL HEALTH LAW AND POLICY 5.

Li, Xinyue (2023), *A Parallel Narrative: Pluralistic Reconciliation Through Quantizing Geoeconomics in (Cyber) Security Governance in International Economic Law*, 18(1) ASIAN JOURNAL OF WTO & INTERNATIONAL HEALTH LAW AND POLICY 89.

Lin, Li-Wen & Curtis J. Milhaupt (2013), *We Are the (National) Champions: Understanding the Mechanisms of State Capitalism in China*, 65(4) STANFORD LAW REVIEW 697.

Liu, Yang (2022), *Proportionality Balancing Under General International Law: The Case of Article 25(1)(b) of ARSIWA*, 21(4) CHINESE JOURNAL OF INTERNATIONAL LAW 647.

Lo, Mao-wei (forthcoming winter 2026), *Essential Security Creep and WTO Adjudication: Recalibrating Security Exceptions in a Changing Geoeconomic Order*, 57(3) GEORGETOWN JOURNAL OF INTERNATIONAL LAW.

Malkin, Anton (2020), *The Made in China Challenge to US Structural Power: Industrial Policy, Intellectual Property and Multinational Corporations*, 29(21) REVIEW OF INTERNATIONAL POLITICAL ECONOMY 538.

Marco Colino, Sandra (2021), *The Internationalization of China's Foreign Direct Investment Laws*, 45(2) FORDHAM INTERNATIONAL LAW JOURNAL 275.

Milanovic, Marko (2023), *Revisiting Coercion as an Element of Prohibited Intervention in International Law*, 117(4) AMERICAN JOURNAL OF INTERNATIONAL LAW 601.

Moraes, Henrique Choer (2024), *The Changing Logic of International Economic Law*, 27(2) UCLA JOURNAL OF INTERNATIONAL LAW AND FOREIGN AFFAIRS 115.

Pahis, Stratos (2025), *Can Plurilaterals Solve the WTO's National Security Crisis?*, 26 JOURNAL OF WORLD INVESTMENT & TRADE 189.

Sadoff, David A. (2009), *A Question of Determinacy: The Legal Status of Anticipatory Self-Defense*, 40(2) GEORGETOWN JOURNAL OF INTERNATIONAL LAW 523.

臺灣大學學術期刊資料庫

Shao, Hsuan-Lei et al. (2023), *Factors Determining Child Custody in Taiwan After Patriarchy's Decline: Decision Tree Analysis on Family Court Decisions*, 18(2) ASIAN JOURNAL OF COMPARATIVE LAW 272.

Slawotsky, Joel (2021), *The Fusion of Ideology, Technology and Economic Power: Implications of the Emerging New United States National Security Conceptualization*, 20(1) CHINESE JOURNAL OF INTERNATIONAL LAW 3.

Slawotsky, Joel (2022), *The Impact of Geo-Economic Rivalry on U.S. Economic Governance: Will the United States Incorporate Aspects of China's State-Centric Governance?*, 16(3) VIRGINIA LAW & BUSINESS REVIEW 559.

Slawotsky, Joel (2026), *The Return of the States: Constitutional Dilemmas of State Measures to Defend National and State Security*, 34(2) ASIA PACIFIC LAW REVIEW 247.

Stephan, Paul B. (2024), *Big Data as a National Security Issue*, 2024 UNIVERSITY OF CHICAGO LEGAL FORUM 307.

Su, Xueji (2026), *Reframing Capital Control: Outbound Investment Screening and International Investment Law*, 27(1-2) THE JOURNAL OF WORLD INVESTMENT & TRADE 69.

van Aaken, Anne (2025), *From Cooperation to Anomie and Transaction in the Transatlantic Relationship? A View from Europe on the Trump Administration 2.0*, 119(4) AMERICAN JOURNAL OF INTERNATIONAL LAW 723.

Van den hole, Leo (2003), *Anticipatory Self-Defence Under International Law*, 19(1) AMERICAN UNIVERSITY INTERNATIONAL LAW REVIEW 69.

Wei, Shen & Zhang Beibei (2024), *China's Anti-Sanctions Regime: An Initial Assessment*, *in* ECONOMIC SANCTIONS UNDER INTERNATIONAL LAW 191 (P. Sean Morris ed., Routledge).

Weidenbaum, Paul (1938), *Necessity in International Law*, 24 TRANSACTIONS OF THE GROTIUS SOCIETY 105.

Wolff, Lutz-Christian (2020), *Legal Responses to China's "Belt and Road" Initiative: Necessary, Possible or Pointless Exercise?*, 29(2) TRANSNATIONAL LAW AND CONTEMPORARY PROBLEMS 249.

Wolff, Lutz-Christian (forthcoming 2026), *Teaching Legal Creativity: Really?*, ASIAN JOURNAL OF LEGAL EDUCATION, https://doi.org/10.1177/23220058261468196.

Wu, Chien-Huei & Mao-wei Lo (2024), *The Threat of China's Economic Coercion*, *in* SWITCHING DIPLOMATIC RECOGNITION BETWEEN TAIWAN AND CHINA 14.

Xiong, Yiying (2025), *Legality, Legitimacy and Institutionalization: China's Dilemma of Sanctions and Economic Coercion*, 34(152) JOURNAL OF CONTEMPORARY CHINA 181.

臺灣大學學術期刊資料庫

Yee, Sienho (2002), *The Potential Impact of the Possible US Responses to the 9–11 Atrocities on the Law Regarding the Use of Force and Self-Defence*, 1(1) CHINESE JOURNAL OF INTERNATIONAL LAW 287.

Yee, Sienho (2021), *Unilateral Sanctions: Kind and Degree; Long-Arm and Strong-Arm Jurisdiction; Real Intent and "Could-Be" Intent*, 20(4) CHINESE JOURNAL OF INTERNATIONAL LAW 817.

Zhang, Beibei & Wei Shen (2024), *China's Non-Performing Loans Disposal in Local and Global Contexts: Missing Pieces in International Law Matrix*, 58(3) JOURNAL OF WORLD TRADE 497.

Zhang, Qianwen (2026), *Securing National Security in Regulating Cross-Border Data Transfer in Foreign Investment*, 21(1) ASIAN JOURNAL OF WTO & INTERNATIONAL HEALTH LAW AND POLICY 95.

Zhang, Sheng (2022), *Protection of Foreign Investment in China: The Foreign Investment Law and the Changing Landscape*, 23(4) EUROPEAN BUSINESS ORGANIZATION LAW REVIEW 1049.

Zheng, Wentong (2023), *The Chinese Antitrust Paradox*, 2(2) THE UNIVERSITY OF CHICAGO BUSINESS LAW REVIEW 391.

Cases

CME Czech Republic B.V. v. The Czech Republic, Final Award, (March 14, 2003) https://jusmundi.com/en/document/decision/en-cme-czech-republic-b-v-v-the-czech-republic-final-award-friday-14th-march-2003.

Global Telecom Holding S.A.E. v. Canada, ICSID Case No. ARB/16/16, Award, (March 27, 2020).

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Judgment, 1986 I.C.J 14.

Panel Report, *Russia — Measures Concerning Traffic in Transit*, WTO Doc. WT/DS512/R (adopted April 26, 2019).

Panel Report, *United States — Certain Measures on Steel and Aluminium Products*, WTO Doc. WT/DS551/R (July 11, 2019).

Panel Report, *United States — Certain Measures on Steel and Aluminium Products*, WTO Doc. WT/DS544/R (December 9, 2022).

Rättsfall från Kammarrätterna [RK] [Court Cases from the Administrative Courts of Appeals], 2022 case no. 5222-21, https://perma.cc/TQ8Q-9QBM (Sweden).

The Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. 7 (September 25).

TikTok Inc. v. Merrick B. Garland, 604 U.S. 56 (2025).

Statutes

Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern, Executive. Order No. 14105, 3 C.F.R. 640, 88 Fed. Reg. 54867 (August 11, 2023).

臺灣大學學術期刊資料庫

Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States, Executive. Order No. 14083, 3 C.F.R. 434 (2023).
International Emergency Economic Powers Act, 50 U.S.C. § 1701.
Protecting Americans from Foreign Adversary Controlled Applications Act, 15 U.S.C. § 9901, https://www.congress.gov/bill/118th-congress/house-bill/7521/text.

Internet Sources

Attorney General William P. Barr Delivers Remarks on China Policy at the Gerald R. Ford Presidential Museum, U.S. DEPARTMENT OF JUSTICE (July 16, 2020), https://www.justice.gov/archives/opa/speech/attorney-general-william-p-barr-delivers-remarks-china-policy-gerald-r-ford-presidential.
Ballantyne, Jack, *Huawei Threatens Poland over Cybersecurity Law*, Global Arbitration Review (October 24, 2025), https://globalarbitrationreview.com/article/huawei-threatens-poland-over-cybersecurity-law.
Bermingham, Finbarr, *China's Wingtech Says Dutch Court Freezes Control of Nexperia amid "National Security" Dispute*, South China Morning Post (October 13, 2025), https://www.scmp.com/news/china/diplomacy/article/3328726/chinas-wingtech-says-dutch-court-freezes-control-nexperia-amid-national-security-dispute.
Bostoen, Friso, *Europe's DMA: A Protectionist Weapon?*, CENTER FOR EUROPEAN POLICY ANALYSIS (March 20, 2024), https://cepa.org/article/europes-dma-a-protectionist-weapon/.
Buckley, Chris, *What Slowdown? Xi Says China Must Win the Global Tech Race*, THE NEW YORK TIMES (March 11, 2025), https://www.nytimes.com/2025/03/11/world/asia/china-xi-trump.html.
Chen, Tsai-fang, *AI, Job Displacement, and the WTO: Identifying Legal Gaps and Charting a Worker-Centered Path*, YALE JOURNAL OF INTERNATIONAL LAW (November 10, 2025), https://yjil.yale.edu/posts/2025-11-10-ai-job-displacement-and-the-wto-identifying-legal-gaps-and-charting-a-worker.
China's Peaceful Development, THE STATE COUNCIL INFORMATION OFFICE OF THE PEOPLE'S REPUBLIC OF CHINA (September 6, 2011), http://www.scio.gov.cn/zfbps/ndhf/2011n/202207/t20220704_130065.html.
Chips Act | Updates, COMPLIANCE, https://www.european-chips-act.com/ (last visited February 21, 2026).
Clark, Sam, *EU's Huawei Hardliners Get Top Court Backing*, POLITICO (March 19, 2026) https://www.politico.eu/article/eu-huawei-hardliners-get-top-court-backing/.
Commission Calls on Member States to Review Outbound Investments and Assess Risks to Economic Security, EUROPEAN COMMISSION (January

臺灣大學學術期刊資料庫

15, 2025), https://ec.europa.eu/commission/presscorner/detail/en/ip_25_261.

Directorate-General for Communication, *Commission Takes Steps to Modernise European Defence and Improve Military Mobility*, EUROPEAN COMMISSION (November 19, 2025), https://commission.europa.eu/news-and-media/news/commission-takes-steps-modernise-european-defence-and-improve-military-mobility-2025-11-19_en.

Emont, Jon & Raffaele Huang, *China Hatches Plan to Keep U.S. Military from Getting Its Rare-Earth Magnets*, THE WALL STREET JOURNAL (November 10, 2025), https://www.wsj.com/world/china/ china-hatches-plan-to-keep-u-s-military-from-getting-its-rare-earth-magnets-f349ee65.

Erixon, Fredrik et al., *Securing Europe's Future: Strengthening ICT Competitiveness for Economic and National Security*, EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY (December 2024), https://ecipe.org/publications/eu-ict-competitiveness-for-economic-national-security/.

EU, US Warn Malaysia of Security Risk in Huawei's Bid for 5G Role, Financial Times Reports, REUTERS (May 2, 2023), https://www.reuters.com/technology/eu-us-warn-malaysia-national-security-risk-huaweis-bid-5g-role-ft-2023-05-02/.

Export Control Law of the People's Republic of China, CHINA LAW TRANSLATE (October 19, 2020), https://www.chinalawtranslate.com/en/export-control/.

FCC Approves New Safeguards Against Untrustworthy Gear, Federal COMMUNICATIONS COMMISSION (October 28, 2025), https://docs.fcc.gov/public/attachments/DOC-415131A1.pdf.

Feuer, Will, *DuPont Scraps Deal to Buy Rogers After Failing to Win Regulatory Clearance*, THE WALL STREET JOURNAL (November 2, 2022), https://www.wsj.com/articles/dupont-scraps-deal-to-buy-rogers-after-failing-to-win-regulatory-clearance-11667403740.

Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on October 26, 2020, MINISTRY OF FOREIGN AFFAIRS PEOPLE'S REPUBLIC OF CHINA (October 26, 2020), https://www.fmprc.gov.cn/eng./xw/fyrbt/lxjzh/202405/t20240530_11346908.html.

Grieger, Gisela, *EU Anti-Subsidy Probe into Electric Vehicle Imports from China*, EUROPEAN PARLIAMENTARY RESEARCH SERVICE (October 18, 2023), https://www.europarl.europa.eu/thinktank/en/document/EPRSATA(2023)754553.

Gunter, Jacob & Grzegorz Stec, *EV Tariffs + EU-China Policy at an Inflection Point + Exports to China*, MERCATOR INSTITUTE FOR CHINA STUDIES (October 10, 2025), https://merics.org/en/merics-briefs/ev-tariffs-eu-china-policy-inflection-point-exports-china.

臺灣大學學術期刊資料庫

Hilpold, Peter, *Intervening in Iran: Tinkering About Just War, Humanitarian Intervention and Second-Best Solutions for Fundamental Challenges in a Less Than Perfect International Order*, SIDIBLOG (April 1, 2026), http://www.sidiblog.org/2026/04/01/intervening-in-iran-tinkering-about-just-war-humanitarian-intervention-and-second-best-solutions-for-fundamental-challenges-in-a-less-than-perfect-international-order/.

Huawei Bribery Scandal: What We Know So Far, POLITICO (March 17, 2025), https://www.politico.eu/article/huawei-bribery-scandal-eu-chinese-tech-lobby-money-lobbying/.

Jee, Charlotte, *The US Threatens to Stop Sharing Intelligence with Allies If They Use Huawei*, MIT TECHNOLOGY REVIEW (February 22, 2019), https://www.technologyreview.com/2019/02/22/66068/the-us-threatens-to-stop-sharing-intelligence-with-allies-if-they-use-huawei/.

Jones, Tom, *China's Hikvision Threatens Claim Against Canada over National Security Measures*, GLOBAL ARBITRATION REVIEW (September 24, 2025), https://globalarbitrationreview.com/article/chinas-hikvision-threatens-claim-against-canada-over-national-security-measures.

Lam, Jeffie & Yuke Xie, *Will Beijing Sink Hutchison-Blackrock Ports Deal with Antitrust Probe?*, SOUTH CHINA MORNING POST (March 29, 2025), https://www.scmp.com/news/hong-kong/politics/article/3304384/how-will-beijings-anti-monopoly-probe-hutchison-blackrock-ports-deal-work.

Matthews, David, *Europe Needs to Hone Its "Technological Edge" in Areas Where It Leads, Think Tank Fellows Say*, SCIENCE | BUSINESS (September 19, 2023), https://sciencebusiness.net/news/sovereignty/europe-needs-hone-its-technological-edge-areas-where-it-leads-think-tank-fellows.

Michaels, Daniel & Dov Lieber, *How AI Is Turbocharging the War in Iran*, THE WALL STREET JOURNAL (March 7, 2026), https://www.wsj.com/tech/ai/how-ai-is-turbocharging-the-war-in-iran-aca59002.

National Security Law, CHINA LAW TRANSLATE (July 1, 2015), https://www.chinalawtranslate.com/en/2015nsl.

Nomani, Asra Q., *Power Couple of Chaos: How a Tycoon and Activist Built a 'Revolutionary Base' at the House of Singham*, FOXNEWS (March 23, 2026), https://www.foxnews.com/us/power-couple-chaos-how-tycoon-activist-built-revolutionary-base-house-singham.

Oertel, Janka, *Security Recall: The Risk of Chinese Electric Vehicles in Europe*, EUROPE COUNCIL ON FOREIGN RELATION (January 25, 2024), https://ecfr.eu/article/security-recall-the-risk-of-chinese-electric-vehicles-in-europe/.

Our Response to the Government of Canada's Order to Shut Down Hikvision Canada Inc., HIKVISION, https://www.hikvision.com/ca-en/newsroom/

臺灣大學學術期刊資料庫

latest-news/2025/our-response-to-the-government-of-canada-s-order-to-shut-down-hi/.

Outbound Investment Security Program, U.S. DEPARTMENT OF THE TREASURY, https://home.treasury.gov/policy-issues/international/outbound-investment-program.

Read, Michael, *UK finds possible 'kill switch' in Chinese bus brand used in Australia*, AUSTRALIAN FINANCIAL REVIEW (January 19, 2026) https://www.afr.com/policy/foreign-affairs/uk-finds-possible-kill-switch-in-chinese-bus-bran d-used-in-australia-20260119-p5nv10.

Remarks by National Security Advisor Jake Sullivan at Special Competitive Studies Project Global Emerging Technologies Summit, THE WHITE HOUSE (September 16, 2022), https://www.miragenews.com/remarks-by-national-security-advisor-jake-856536/.

Rogan, Ali & Harry Zahn, *How Militaries Are Using Artificial Intelligence on and off the Battlefield*, PBS NEWS WEEKEND (July 9, 2023), https://www.pbs.org/newshour/show/how-militaries-are-using-artificial-intelligence-on-and-off-the-battlefield.

Sanderson, Cosmo, *Huawei Brings ICSID Claim against Sweden over 5G Ban*, GLOBAL ARBITRATION REVIEW (January 24, 2022), https://globalarbitrationreview.com/article/huawei-brings-icsid-claim-against-sweden-over-5g-ban.

Sherlock, Joseph & Nissim Massarano, *UK High Court Upholds NSIA Order to Divest on National Security Grounds*, CLIFFORD CHANCE (August 4, 2025), https://www.cliffordchance.com/insights/resources/blogs/antitrust-fdi-insights/2025/08/uk-high-court-upholds-nsia-order-to-divest-on-national-security-grounds.html.

Speech by Commissioner Breton on the Cybersecurity of 5G Networks, EUROPEAN COMMISSION (June 15, 2023), https://ec.europa.eu/commission/presscorner/detail/en/speech_23_3314.

Ströder, Martin, *Keine chinesischen Komponenten: Bund schließt Verträge mit Netzbetreibern* [*No Chinese Components: Federal Government Concludes Contracts with Network Operators*], JUVE (July 15, 2024,), https://www.juve.de/deals/keine-chinesischen-komponenten-bund-schliesst-vertraege-mit-netzbetreibern/.

Strumpf, Dan et al., *China Torpedoes Intel's Bid to Buy Israeli Chip Maker Tower Semiconductor*, THE WALL STREET JOURNAL (August 16, 2023), https://www.wsj.com/business/deals/intel-scraps-tower-acquisition-after-china-fails-to-approve-deal-f59dd70f.

Strumpf, Dan, *Scuttled Qualcomm-NXP Deal Is a Win-Win for Beijing*, THE WALL STREET JOURNAL (July 26, 2018), https://www.wsj.com/articles/scuttled-qualcomm-nxp-deal-is-a-win-win-for-beijing-1532606186.

臺灣大學學術期刊資料庫

TED, *The Next Global Superpower Isn't Who You Think | Ian Bremmer | TED*, YOUTUBE (June 14, 2023), https://www.youtube.com/watch?v=uiUPD-z9DTg&t=3s.

TokenRing AI, *Dutch Government Seizes Nexperia Operations amid Intensifying US-Led Semiconductor Scrutiny*, WRAL NEWS (October 14, 2025), https://markets.financialcontent.com/wral/article/tokenring-2025-10-14-dutch-government-seizes-nexperia-operations-amid-intensifying-us-led-semiconductor-scrutiny.

U.S. Export Controls and China: Advanced Semiconductors, CONGRESS.GOV (September 19, 2025), https://www.congress.gov/ crs-product/R48642.

Volpicelli, Gian & Jillian Deutsch, *EU Eyes Huawei Ban in Mobile Networks of Member Countries*, BLOOMBERG (November 11, 2025), https://www.bloomberg.com/news/articles/2025-11-10/eu-eyes-banning-huawei-from-mobile-networks-of-member-countries.

Von der Burchard, Hans et al., *Germany Goes Soft on China, Dragging out Huawei Ban Until 2029*, POLITICO (July 10, 2024), https://www.politico.eu/article/germany-china-huawei-ban-2029-5g-networks-government-greens-lawmaker-4g-strand/.

Wu, Zijing & Cheng Leng, *China Says Nvidia Violated Antitrust Law When It Bought Mellanox*, FINANCE TIMES (September 15, 2025), https://www.ft.com/content/fa7a2e35-df03-45a1-bd0b-3f7207a7d84b.

Xi Urges World Political Parties to Shoulder Responsibility for Pursuit of People's Wellbeing, Progress of Mankind, STATE COUNCIL OF CHINA (July 7, 2021), https://english.www.gov.cn/news/topnews/202107/07/content_WS60e502a2c6d0df57f98dc82b.html.

Xinhua, *Xi Stresses Safeguarding National Security, Social Stability, Peaceful Lives*, CHINA DAILY (January 15, 2022), https://www.chinadaily.com.cn/a/202201/15/WS61e26eeaa310cdd39bc81418.html.

Yang, Angela & Savannah Sellers, *TikTok Sues U.S. Government, Saying Potential Ban Violates First Amendment*, NBC NEWS (May 8, 2024), https://www.nbcnews.com/tech/tech-news/tiktok-sues-us-government-says-ban-violates-first-amendment-rcna151059.

Yin, Jessie, *Germany Is Finally Waking Up to the China Challenge. And Beijing Is Gearing Up to Respond*, ATLANTIC COUNCIL (July 20, 2026), https://www.atlanticcouncil.org/blogs/econographics/germany-is-finally-waking-up-to-the-china-challenge-and-beijing-is-gearing-up-to-respond/.

Zhongyang Guojia Anquan Weiyuanhui Di Yi Ci Huiyi Zhaokai Xi Jinping Fabiao Zhongyao Jianghua (中央国家安全委员会第一次会议召开 习近平发表重要讲话) [*The First Meeting of The Central National Security Commission Held; Xi Jinping Delivered an Important Speech*],

臺灣大學學術期刊資料庫

STATE COUNCIL (April 15, 2014), http://www.gov.cn/xinwen/2014–04/15/content_2659641.htm.

Zugui, Gao (高祖贵), *Zhongguo Guojia Anquan Lilun Yu Shijian De Zhongda Chuangxin (中国国家安全理论与实践的重大创新)* [*Major Innovations in China's National Security Theory and Practice, Research Center for Theoretical System of Socialism with Chinese Characteristics*], QSTHEORY (February 28, 2017), https://www.qstheory.cn/dukan/qs/2017-02/28/c_1120536834.htm.

Other Sources

BUSH, GEORGE WALKER (2002), THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA, https://2009-2017.state.gov/documents/organization/63562.pdf.

BUSH, GEORGE WALKER (2006), THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA, https://history.defense.gov/Portals/70/Documents/nss/nss2006.pdf.

CHIMITS, FRANÇOIS ET AL. (2024), EUROPEAN ECONOMIC SECURITY: CURRENT PRACTICES AND FURTHER DEVELOPMENT, https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754449/EXPO_IDA(2024)754449_EN.pdf.

FEDERAL GOVERNMENT (2023), ROBUST. RESILIENT. SUSTAINABLE. INTEGRATED SECURITY FOR GERMANY: NATIONAL SECURITY STRATEGY, https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf.

GOVERNMENT OFFICES OF SWEDEN (2024), NATIONAL SECURITY STRATEGY, https://government.se/globalassets/government/national-secu rity-strategy.pdf.

TRUMP, DONALD JOHN (2017), THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

UNITED STATES CONGRESS (2025), SELLING THE FORGES OF THE FUTURE: HOW THE CCP GETS ITS KEY EQUIPMENT FOR MAKING SEMICONDUCTORS FROM U.S., DUTCH, AND JAPANESE COMPANIES, https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/selling-the-forges-of-the-future.pdf.

UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 117TH CONGRESS (2021), 2021 REPORT TO CONGRESS OF THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. U.S. GOVERNMENT PUBLISHING OFFICE, 2021 REPORT TO CONGRESS OF THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION 11 (2021), https://www.uscc.gov/sites/default/files/2021-11/2021_Annual_Report_to_Congress.pdf.

臺灣大學學術期刊資料庫